ЦИФРОВЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ: ГЕНЕЗИС И ПЕРСПЕКТИВЫ

Материалы I Международной межвузовской научно-практической конференции (28 февраля 2020 года)

Министерство науки и высшего образования РФ

ФГАО ВО «Национальный исследовательский университет
«Московский институт электронной техники»

Министерство сельского хозяйства РФ

ФГБОУ ВО «Красноярский государственный аграрный университет»

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ: ГЕНЕЗИС И ПЕРСПЕКТИВЫ

**Материалы I Международной межвузовской
научно-практической конференции
28 февраля 2020 года**

Электронное издание

Красноярск 2020

ББК 32.973.2
Ц 75

Ц75 Цифровые технологии в юриспруденции: генезис и перспективы [Электронный ресурс]: материалы I Международной межвузовской научно-практической конференции (28 февраля 2020 г., Москва) / НИУ МИЭТ, Краснояр. гос. аграр. ун-т, 2020. – 262 с.

Представлены материалы I Международной межвузовской научно-практической конференции «Цифровые технологии в юриспруденции: генезис и перспективы», которая проходила 28 февраля 2020 года в Москве и соорганизаторами которой стали Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники» и Федеральное государственное бюджетное образовательное учреждение высшего образования «Красноярский государственный аграрный университет».

Предназначено для ученых и специалистов образовательных и научно-исследовательских учреждений, представителей органов государственной и муниципальной власти, адвокатуры, иных организаций и учреждений, а также лиц, интересующихся вопросами цифровых технологий.

ББК 32.973.2

Статьи публикуются в авторской редакции, авторы несут полную ответственность за подбор и изложение информации.

УДК 316.3.4

ИДЕОЛОГИЯ ЦИФРОВИЗАЦИИ В ДИСКУРСЕ СОВРЕМЕННОГО СОЦИАЛЬНО-ГУМАНИТАРНОГО ЗНАНИЯ

Айснер Лариса Юрьевна, Наумов Олег Дмитриевич
Красноярский государственный аграрный университет, Красноярск, Россия

Анализируются идеологические аспекты процесса цифровизации, рассматриваемого в качестве одного из ключевых социально-культурных процессов, характеризующих облик современности. Обобщая дискурсивные практики социально-гуманитарных наук, затрагивающих рассматриваемый феномен в качестве одного из главных объектов своего изучения, проблема цифровизации ставится и решается в антропологическом ключе.

***Ключевые слова**: цифровизация, наука, идеология, человек, общество, техника, дискурс.*

THE IDEOLOGY OF DIGITALIZATION IN THE DISCOURSE OF MODERN SOCIO-HUMANITARIAN KNOWLEDGE

Aisner Larisa Yurievna, Naumov Oleg Dmitrievich
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The ideological aspects of the digitalization process, which is considered as one of the key socio-cultural processes that characterize the face of modernity, are analyzed. Summarizing the discursive practices of the social sciences and humanities, affecting the phenomenon under consideration as one of the main objects of their study, the problem of digitalization is posed and solved in an anthropological manner.

***Keywords**: digitalization, science, ideology, man, society, technology, discourse.*

Одна из ключевых тенденций, характеризующих развитие современного общества, как в России, так и за ее пределами, определяется в качестве стремительно охватывающего все сферы общественной жизни процесса цифровизации, в том числе и сферу образования, учитывая то, что именно она «порождает» цифровые кадры [5, 6]. В связи с этим, информационное пространство, а также дискуссии экспертов, разворачивающееся вокруг описываемого тренда социальной реальности, определяются созданием специфической идеологической установки, согласно которой обращение к цифре: от искусственного интеллекта до криптовалюты – ассоциируется с единственно возможным способом успешного развития государства. Именно эта ситуация является объектом пристального интереса социально-гуманитарных наук, стремящихся к всестороннему описанию разнообразных аспектов современного этапа развития общества. В этом смысле, анализ перспектив развития цифрового общества, а

также оценка долгосрочных последствий развития процесса цифровизации – одна из ключевых задач гуманитаристики XXI века.

На сегодняшний день под «цифрой», или цифровизацией принято понимать совокупность технологий обработки больших данных, необходимых для достижения поставленных производственных, социальных и управленческих целей. В тоже самое время, практика показывает, что ключевую роль в принятии административных решений любого уровня продолжает играть человек, что свидетельствует не столько о кризисе цифровизации, сколько о ситуации в рамках которой общество не до конца осознает перспективы цифровизации, а также не видит большой отдачи от практического применения новейших технологий. Таким образом, один из альтернативных вариантов развития преобладающей сегодня технократической идеологии заключается в разработке актуального проекта социогуманиатрного содержания, продуцирующего и обосновывающего возможность эффективного сосуществования и взаимодействия человека и искусственного интеллекта, реализующих себя в пространстве высоких технологий [4, с. 354]. Это позволило бы не только оптимизировать и увеличить эффективность процессов коммуникации и поиска новых образовательных практик, но и стимулировать развитие бизнеса, выводя его на новый виток развития посредством создания и апробации алгоритмов для выработки обоснованных прогнозов на долгосрочное будущее.

Однако идеологические аспекты цифровизации, заключающиеся в стремительной погоней за «цифрой», а также установки на прогресс ради прогресса, сулящего лишь увеличение прибыли оставляет без должного внимания вопросы, связанные со смысловым пластом реализуемых преобразований. Заметим, что в данной социокультурной ситуации практически полностью выносится за скобки вопрос о влиянии описываемого процесса на человека и общество, что свидетельствует не столько о кризисе современной философии техники, сколько об экономической ангажированности всеобщей цифровизации. Таким образом, вопрос о границах и потребности современного общества в цифре остается открытым, что позволяет социально-гуманитарному знанию предлагать и развивать в своем дискурсе широкий диапазон сценариев развития общественных отношений: от общества знания до гиперреальности цифровых муляжей, приуменьшающей интерес к живым людям и их насущим проблемам, подменяя его псевдоинформационным пустословием.

С другой стороны, современный истеблишмент все больше рассматривает цифру в качестве пути, ведущему к реально возможному обществу всеобщего благоденствия. В это же время, путь к этому идеалу социально-политического развития, оборачивается ситуацией доминации цифровых фантомов, выносящих подлинную реальность за скобки и лишь усиливая противостояние между различными онтологическими модусами бытия человека и общества. В результате действий государства и чиновников, составляющих большинство его бюрократического аппарата, осуществляющего функцию оперативного управления, большинство обычных людей вместе с их проблемами остаются за границами фокуса восприятия власти. Вместе с тем, цифровое отчуждение власти от общества способствует процессу формирования подпольного интернета

[2, с. 27], являющегося в действительности не только пространством криминальных отношений в информационном мире, но и площадкой освобождения большого количества пользователей от тотального и общедоступного Интернета, перегруженного фантомными и риторическими программами типа «Цифровой экономики».

По замыслу своих создателей, данный документ, призванный направить действующих в данной сфере акторов к формированию последовательной и целенаправленной политики вдумчивых преобразований, обернулся маркетинговым хайпом, а также малопродуктивной полемикой, носящей преимущественно идеологический, а не рационально-научный характер. Таким образом, современный этап развития высоких технологий характеризуется не столько качественными достижениями, сколько количественными, воплощающихся в росте спроса со стороны власти на инновации, а также действительной оценки революционных изменений в самой архитектоники общества, пребывающего в поиски новых реальных векторов своего развития.

Нельзя не согласиться с Г. Клейнером в том, что в данной ситуации разработка стратегии развития государства должна начинаться «снизу». При этом стратегия развития отдельно взятого индивида (физического или юридического лица – не суть важно) должна рассматриваться в контексте тотальной сетевой структуры стратегии в масштабах всего государства. В этом смысле, даже в условиях развития «цифровой экономики» движущей силой ее развития продолжает оставаться сумма личных мотиваций к работе, а также личностное стремление к творчеству и самостановлению.

Отрицание данного факта – причина многочисленных проблем, характеризующих облик современности, отличительная черта которых сводится к концептуальной неоднозначности. В частности, современный этап цифровизации обусловлен размытием понятия личности, а также ее статуса в сетевом пространстве. Кроме того, перенос большой доли социальных и межличностных взаимоотношений в сетевое пространство позволяет рассматривать последнее в качестве площадки для взаимных столкновений субъектов, а также роста криминальных отношений. Одним из результатов данного процесса является «упрощение» общества: «мы все больше похожи друг на друга, в нас все меньше креативности, индивидуальности, независимости», а также усиление существующих в нем проблем: от обеднения и принципиальной конфликтности разрешения имущественных споров до защиты биометрических данных. Описываемые проблемы красноречиво указывают на кризис и фактическое свертывание идеи естественного права, трактующей закон в качестве специфического регулятора общественной жизни, берущего свое начало в «природе разума человеческого» [3, с. 49]. Таким образом, основополагающая задача государства в описываемой ситуации заключается не в том, чтобы плодить очередные цифровые фантомы, а в том, чтобы способствовать реальной защите интересов, прав и свобод разнообразных представителей общества с целью собственной легитимации. Принимая во внимание еще одну атрибутивную характеристику современного общества, согласно которой маркер, определяющий современность сводится к обществу всеобщего потребления, несложно сформулировать клю-

чевую дилемму современного этапа развития. Она, в духе кьеркегорвской дихотомии может быть определена следующим образом: или обретение общества знания и свободы духа, или общество потребления и окончательное порабощение цифрой, тотальность которой в настоящее время не предполагает альтернативных сценариев развития общественных отношений.

На сегодняшний день высокие технологии закабалили людей, в то же самое время, позволив сэкономить им колоссальный ресурс свободного времени, расходуемого на удовлетворение потребности в комфорте, а также потреблении. Вместе с тем, цифра сегодня – один из наиболее востребованных и эффективных способов контроля и управления над людьми. Сказанное, не может не поставить вопроса сугубо антропологической направленности [1, с. 12], заключающегося в возможности такого преобразования мира, когда станет возможно реальное возвращение человека к самому себе и своеобразному очеловечиванию природы.

Иными словами, оценка феномена цифровизации современности, не столько обнажает свой очевидно амбивалентный характер, сколько ставит вопрос о преобразовании мира, который не только выстроит диалогичные отношения с цифрой, но и определит положение человека в качестве субъекта, пребывающего среди своих [1, с. 14].

Библиографический список

1. Айснер, Л. Ю. Генеалогия личностно-социального события человека: экзистенциальный аспект / Л. Ю. Айснер, О. Д. Наумов, М. Э. Червяков // Контекст и рефлексия: философия о мире и человеке. – 2019. – Т. 8, № 4 А. – С. 11–19.
2. Бартлетт, Дж. Подпольный Интернет: темная сторона мировой паутины / Дж. Бартлетт. – М.: Эксмо, 2017. – 352 с.
3. Куницын, А. П. Право естественное / А. П. Куницын. – М.: ЛКИ, 2011. – 162 с.
4. Лепский, В. Е. Социогуманитарная эргономика стратегического проектирования российского развития / В. Е. Лепский // Актуальные проблемы психологии труда, инженерной психологии и эргономики. – Вып. 4. – М.: Издательство Института психологии РАН, 2012. – С. 351–358.
5. Трашкова, С. М. Некоторые теоретико-правовые аспекты по использованию информационных технологий в образовании / С. М. Трашкова // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. научно-практич. конф. / отв. за выпуск В. Л. Бопп. – Красноярск, 2016. – С. 82–84.
6. Трашкова, С.М. Основы правового регулирования использования информационных технологий в образовании / С.М. Трашкова // Инновационные тенденции развития российской науки: мат-лы IX междунар. науч.-практ. конф. / отв. за выпуск В. Л. Бопп. – Красноярск, 2016. – С. 27–30.

УДК 004.9:35

ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ ЦИФРОВЫХ ГОСУДАРСТВ: КОПИЯ ФИЗИЧЕСКОГО ГОСУДАРСТВА В ИНТЕРНЕТ-СРЕДЕ

Белов Никита Сергеевич
Национальный исследовательский университет «МИЭТ», Москва, Россия

Физическое государство XXI века имеет множество нерешенных и сложно решаемых проблем из-за недостатка высококвалифицированных людей на постах первостепенной важности. На помощь в решении данной проблемы может прийти цифровое государство, созданное в интернет-среде и имеющее некоторое преимущество в сфере государственного аппарата. Цифровое государство имеет шансы помочь в решении некоторых проблем физического государства, но из-за сложностей в создании подобного государства требуется гораздо глубже окунуться в исследования среды интернет и ее особенностей.

***Ключевые слова**: цифровое государство, Big Data, Блокчейн.*

PROSPECTS FOR THE FORMATION OF DIGITAL STATES: A COPY OF THE PHYSICAL STATE IN THE INTERNET ENVIRONMENT

Belov Nikita Sergeevich
National Research University MIET, Moscow, Russia

The physical state of the XXI century has many unsolved and difficult to solve problems due to the lack of highly qualified people in positions of primary importance. To help solve this problem, a digital state created in the Internet environment and having some advantage in the sphere of state apparatus can come. The digital state has a chance to help solve some of the problems of the physical state, but due to the difficulties in creating such a state, it is necessary to plunge much deeper into the research of the environment-the Internet and its features.

***Keywords**: digital state, Big Data, Blockchain.*

В XXI веке – веке высоких технологий прогресс окутывает все сферы жизни человека, не удивительно, что высокие технологии проникли и в государственную среду. В настоящее время каждое государство непременно старается использовать высокие технологии для автоматизации деятельности государственного аппарата и улучшения его как такого в принципе.

На данный момент правительства используют такие средства как: Big Data (структурированные и неструктурированные данные огромных объемов и разнообразия, а также методы их обработки, которые позволяют распределённо анализировать информацию) – для большого спектра таких задач, как: видеонаблюдение, прогнозирование преступлений и заблаговременное распределение ресурсов.

Используются технологии распознавания лиц – для быстрого нахождения граждан, которые могут быть разносчиками различных заболеваний. Применяется цифровизация повседневных услуг: электронные очереди и предоставление онлайн услуг на государственных ресурсах по типу «Госуслуги». В последнее время очень остро встал вопрос об использовании искусственного интеллекта, который может перевернуть весь государственный аппарат и автоматизировать большой объём рабочих процессов.

Но это лишь малый потенциал использования всех раннее указанных технологий. Среди главных нерешенных задач перехода государства в «цифру» является:

1. Недостаточное понимание устройства цифровых технологий, что означает недостаточное количество высококвалифицированных специалистов;

2. Отсутствие надлежащего контроля за реализацией новых идей;

3. Недостаточное количество оцифрованных данных (Big Data не будет работать, если нет базы от которой стоит отталкиваться);

4. Отсутствует надлежащая система защиты персональных данных.

Подобные проблемы в цифровизации государства поднимаются и в работах А.И. Овчинникова [2], С.Б. Халиды [3], А.И. Чучаева, Ю.В. Грачёвой, С.В. Маликова [1].

Очевидно, что подобные изъяны не могут быть решены в ближайшие годы, быть может даже в десятилетия, так как переход к новому всегда был самым трудным этапом в истории любого государства. Но я бы хотел обратить внимание на новый способ для ускорения данного перехода, а в перспективе развития и полного доминирования за счет определенных «ресурсов» на мировой «цифровой» арене.

Речь пойдет о Цифровом государстве. Чтобы внести ясность – то, что мы наблюдаем сейчас, это «цифровизация» государства – то есть уже существующее государство, которое впитывает в себя цифровые технологии и пытается использовать их надлежащим и наиболее целесообразным способом что, естественно, очень проблематично. Под «цифровым государством» следует понимать создание нового, ранее не существовавшего государства, чьи основные проблемы – это вопрос территориального характера и отстаивания суверенитета.

Начнем с простого определения – что есть государство? Государство – это организация власти, направляющая жизнь людей в определенное русло. Рассмотрим признаки, при которых государство является государством.

В первую очередь, это территория. Это пространственная основа государства. Она включает сушу, недра, водное и воздушное пространство и др. Этот признак является одним из двух проблемных, так как невозможно обозначить территорию в кибер-государстве.

Вторым признаком государства является его население. Население в «цифровом государстве» будет одновременно и его главным ресурсом. Для получения гражданства в таком государстве будет необходимо доказать свою значимость для общества при помощи своих знаний и умений, далеко не каждый сможет стать гражданином такой страны.

Власть в таком государстве будет принадлежать парламенту как источнику обновления законов, но, чтобы принять закон будет необходимо поддержка большей части населения, так как в ней будет принимать участие система блокчейн, которая не даст возможности в изменении государственного аппарата по желанию только определенного круга лиц.

Право в цифровом государстве будет крайне скудно из-за отсутствия как таковой возможности физического контакта. По сравнению с нынешним законодательством будет сильно сокращен свод уголовного кодекса и упростится судебная система, однако придется отдать большое внимание гражданским правам.

Налоговая система в таком государстве будет функционировать за счет его ресурсов – то есть буквально за счет его населения. Государство будет использовать знания и умения для своих граждан для пополнения бюджета за счет торговли информации и/или силами граждан.

Суверенитет – проблемный признак государства, так как независимость внутренней политики с использованием системы блокчейн противоречит самому понятию власти из-за того, что эта власть находится в руках всего населения без возможности полного контроля со стороны государства. Независимость внешнего характера ограничивается его уникальностью и одновременным «отсутствием», и «присутствием» соседних стран.

Таким образом, цифровое государство – это государство без определенной территориальной основы, в котором государственная власть вместе с гражданами решает все законотворческие вопросы, население страны используется для поддержания экономической стабильности.

Очевидно, что с подобным количеством недочетов идея не кажется достаточно хорошей, но что, если создать подобное цифровое государство под покровительством уже существующего – схожего по отношениям сюзерена (тип крупного феодального правителя, власть которого основана на вассальном подчинении ему более мелких феодалов, получавших от сюзерена право на часть земли (феод) в его владениях).

В этом случае решится огромное количество проблем. Территория будет являться общей для обеих стран, финансовая поддержка даст больше возможностей, а население цифрового государства будет больше за счет не только идейного ключа, но и с учетом добавления привилегий гражданам цифрового государства на территории его физического. Также благодаря наличию физического государства возможности понести наказание за несоблюдение прав цифрового государства не будет ограничена только исключением из общества, но и реальным гонением со стороны физического государства.

Но выгоду получит не только государство цифровое, но и физическое – неограниченный доступ к людям, чьи способности и знания могут предопределить будущее обеих стран и быть может всего мира довольно неплохое предложение.

Если обратиться к истории, то можно заметить, как происходят изменения в государстве в зависимости от общественных взглядов: при революцион-

ной направленности происходит резкая смена векторов политических взглядов, что влечет расцвет и следом резкий спад в стране. В случае консервативных взглядов почти невозможно создать даже малейшие изменения в политическом устройстве, что негативно сказывается на общем темпе развития. Если же использовать устоявшуюся демократическую систему взглядов, то можно отметить, что скорость в изменении и принятии новых решений достаточно низка, что влияет на продуктивность всего государственного аппарата и страны в целом.

На наш взгляд создание подобного общества поможет обоим государствам по средствам взаимовыгодного обмена ресурсами на пути процветанию, а также изменит устоявшуюся концепцию мира и понятия «страны» как таковой. Равно как будет большим скачком в цифровой сфере вообще.

Библиографический список

1. Грачева, Ю. В. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения / Ю. В. Грачева, А. И. Коробеев, С. В. Маликов [и др.] // LEX RUSSICA. – 2020. – № 1 (158). – С. 145–159.

2. Овчинников, А. И. Риски в процессах цифровизации права / А. И. Овчинников // Юридическая техника. – 2019. – № 13. – С. 257–261.

3. Халида, С. Б. О цифровизации экономики в Российской Федерации / С. Б. Халида // Образование. Наука. Научные кадры. – 2019. – № 3. – С. 82–84.

УДК 343.1:343.3

ОСОБЕННОСТИ СУДОПРОИЗВОДСТВА ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ В СФЕРЕ ЭНЕРГЕТИКИ

Бертовский Лев Владимирович
доктор юридических наук, профессор
ФГАОУ ВО «Российский университет дружбы народов», Москва, Россия

В статье показана общественная опасность совершаемых преступлений в сфере энергетики и обосновывается необходимость создания в Российской Федерации цифрового судопроизводства, определены основные направления развития цифрового судопроизводства.

***Ключевые слова**: преступления в сфере энергетики, цифровое судопроизводство, уголовное судопроизводство, искусственный интеллект, технологии распределенного реестра, коррупционные преступления, технология блокчейн.*

FEATURES OF LEGAL PROCEEDINGS IN CASES OF CRIMES COMMITTED IN THE ENERGY SECTOR

Bertovsky Lev Vladimirovich
Doctor of law, Professor
Peoples' Friendship University of Russia, Moscow, Russia

The article shows the public danger of crimes committed in the field of energy and substantiates the need to create a digital court system in the Russian Federation, and defines the main directions for the development of digital justice.

***Keywords**: crimes in the energy sector, digital legal proceedings, criminal proceedings, artificial intelligence, distributed registry technologies, corruption crimes, blockchain technology.*

Количество различных видов преступлений, совершаемых в сфере энергетики огромно. К таким уголовно-наказуемым деяниям можно отнести и кражи, и уклонение от уплаты налогов, и превышение должностных полномочий, и террористические акты, и многое другое. В ряде случаев эти преступления носят международный характер. При этом наиболее опасными по своим последствиям являются преступления, совершаемые с использованием высоких технологий. В последнее время по миру прокатилась целая волна таких происшествий.

В сентябре 2010 года в Иране около 30 тыс. компьютерных систем промышленных объектов были заражены вирусом Stuxnet. Взлом привел к остановке работы более 1,3 тыс. центрифуг по обогащению урана в Натанзе и переносу сроков запуска АЭС «Бушер». По словам экспертов, кибератака отбросила

ядерную программу страны на два года. Власти Ирана обвинили во взломе спецслужбы США.

В декабре 2014 года в Южной Корее хакеры получили доступ к внутренней сети оператора Hydro and Nuclear Power Co Ltd. Проникнуть в сеть удалось после рассылки сотрудникам компании более 5,9 тыс. зараженных писем. В дальнейшем злоумышленники требовали остановки реакторов на АЭС «Кори» и «Вольсон», а также публиковали схемы, внутренние инструкции и данные о сотрудниках. Представители компании заявляли, что похищенная информация не является конфиденциальной и не представляет угрозы. Власти страны обвинили во взломе КНДР [5].

Не так давно The Wall Street Journal опубликовала материал, в котором содержались сенсационные данные о диверсиях российских хакеров, якобы имевших место в 2016–2017 гг. Издание сообщило, что они проводили целенаправленные атаки на сотни подрядчиков в США, Канаде и Великобритании, подготавливая плацдарм для масштабной диверсии с целью вывода из строя энергетической системы США. Это далеко не первая попытка «скрестить» Россию с киберпреступлениями и энергообъектами Соединенных Штатов. Летом 2017 г. Bloomberg сообщал, что хакеры проникли в компьютерные системы 12 электростанций США, включая ядерный объект The Wolf Greek в Канзасе. Уже тогда агентство со ссылкой на свои источники распространило информацию, что подозрение в связи с потенциальным взломом падает на Россию.

Самое масштабное отключение электроэнергии в истории Венесуэлы произошло 7 марта 2019 г. и затронуло 21 штат из 23. Почти сутки жители Венесуэлы были без света, а также телефонной связи и интернета. В Каракасе остановилось метро, в больницах города Матурин из-за блэкаута скончались 15 детей. Власти обвинили в энергетической диверсии хакеров США.

Но хакеры есть во всем мире. Они успешно работают и в Америке, и в Индии, Израиле, Китае, Великобритании, Франции, Мексике, в странах Африки и т.д. Часть работает на правительство, а часть на себя. Причем мотив последних чаще всего или корыстный или месть.

Так как предупредить такие преступления? Кто реально их совершил? Как это установить?

Термин «потенциальный взлом» весьма размыт. Доказать, был ли данный инцидент на самом деле или нет, носит ли он криминальный характер, могут только специалисты, доступ которых на энергообъекты любой страны ограничен. Привлечь к ответственности за подобные преступления, как показывает практика, оказывается очень непростым делом. Еще сложнее, когда хакеры объединяются в международные сообщества. В этом случае пресечь их деятельность или хотя бы минимизировать причиненный ими ущерб становиться крайне затруднительно, при этом не менее проблемным становится последующее расследование таких преступлений.

В целях оптимизации деятельности по противодействия вышеуказанных преступных проявлений был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Россий-

ской Федерации». Данный нормативный акт регулирует отношения в области обеспечения безопасности объектов информационной инфраструктуры РФ, функционирование которых критически важно для экономики государства. Такие объекты в законе называются объектами критической информационной инфраструктуры. А к субъектам критической информационной инфраструктуры отнесены, в том числе, государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере энергетики, топливно-энергетического комплекса, в области атомной энергии, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Согласно закону, субъекты критической информационной инфраструктуры должны провести категорирование находящихся в их распоряжении объектов, обеспечить интеграцию в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и принять организационные и технические меры по обеспечению безопасности объектов КИИ.

Принятие этого и ряда других нормативно-правовых актов положительно повлияло на организацию обеспечения безопасности указанных объектов.

Менее оптимистично выглядит ситуация с расследованием вышеуказанных противоправных деяний в рамках уголовного судопроизводства. У практикующих сотрудников правоохранительных органов возникает множество проблем, связанных с их недостаточной компьютерной грамотности, отсутствием современной нормативно-правовой базы, нехваткой соответствующего материально-технического обеспечения, и др. Преодоление существующих проблем возможно только после проведения ряда мероприятий на государственном уровне.

В своем обращении к Федеральному Собранию в конце 2016 г. Президент России Владимир Путин заявил о нуждаемости в собственных передовых разработках и научных решениях, направленных на развитие экономики и социальных отраслей. Было сказано о необходимости сосредоточиться на, так называемых, «сквозных» технологиях – цифровых технологиях, с мощным технологическим потенциалом, которые сегодня определяют облик всех сфер жизни [1].

В целях реализации своего послания 9 мая 2017 г. Президент РФ В.В. Путин подписал указ № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», в котором в качестве одной из важнейших задач, стоящих перед государством, определил обеспечение использования российских информационных и коммуникационных технологий в органах государственной власти Российской Федерации, компаниях с государственным участием, органах местного самоуправления.

Существует тесная связь между социально-экономическими преобразованиями в обществе и судьбой институтов государственной власти, в частности

судебных органов. Без коренной модификации судопроизводства, без внедрения информационных технологий, стандартизации процессуальных документов, использование алгоритмов в процессе доказывания, включение всех или большинства судебных актов в единую аналитическую систему, расследование высокотехнологичных преступлений представляется крайне затруднительным, если вообще возможным. Перефразируя одного из первых воров-сыщиков Э.Ф. Видока, можно сказать, что высокотехнологичных преступников могут поймать только высокотехнологичные полицейские. Таким образом время и сама жизнь диктуют необходимость создания цифрового судопроизводства.

«Цифровое судопроизводство – урегулированная нормами процессуального права деятельность суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел, в которой ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность» [2, с. 23].

Оно развивается в нескольких направлениях: нормативное правовое регулирование цифрового судопроизводства, кадровое обеспечение данной сферы, образовательная деятельность, информационная инфраструктура, технические аспекты, информационная безопасность.

При этом хотелось бы особенно выделить значимость первого направления, так как оно требует не только разработки специализированных нормативных правовых актов, касающихся цифрового судопроизводства как такового, но и внесения существенных изменений и дополнений в законодательство вообще, в том числе в УПК РФ, ГПК РФ, АПК РФ, «О судебной системе Российской Федерации», «О прокуратуре Российской Федерации» и др.

Необходимо и четкое и конкретное формирование политики государства, которая бы находила отражение в соответствующих документах, в частности, нужны планы мероприятий («дорожная карта»), сформированных в рамках системы управления реализацией указа Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Также насущной проблемой является вопрос кадрового обеспечения. Он предопределяется низким уровнем технической подготовленности кадров на современном этапе, что не отвечает ожиданиям и потребностям рынка труда в такого рода работниках. Так, если обратиться к сфере уголовного судопроизводства и проанализировать правоприменительную деятельность по расследованию преступлений в сфере технологий, то можно сделать вывод, что у практических работников повсеместно имеются пробелы в данной области, что свидетельствует об одном: необходимо проведение дополнительного обучения должностных лиц правоохранительных органов современным информационным технологиям не только как продвинутых пользователей офисных программ, но и как лиц, осведомленных в стандартах и новациях IT в целом и в юридических аспектах обеспечения функционирования IT в том числе.

С этой точки зрения неподдельный интерес вызывает реализуемая Федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский университет «Московский институт электронной техники» в рамках специальности 40.05.01 «Правовое обеспечение национальной безопасности» первая в Российской Федерации учебная программа, в которой 60 процентов учебных дисциплин традиционны для юридического образования (уголовное, гражданское, административное право, криминалистика и т. д.), а 40 процентов учебных дисциплин носят технический характер (конструирование программного обеспечения; управление программными проектами; программирование на языке высокого уровня; объектно-ориентированное программирование и др.). Представляется, что специалисты именно такого уровня смогут эффективно решать вопросы, возникающие при переходе на цифровое судопроизводство.

Основными сквозными цифровыми технологиями, используемыми в рамках цифрового судопроизводства, могут стать:

– большие данные (англ. big data – обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами), появившиеся в конце 2000-х гг. и ставшие альтернативными традиционным системам управления базами данных и решениям класса Business Intelligence [4]. Так, большой объем сведений, имеющих криминалистическое значение, на сегодняшний день поступает в различные базы данных, причем они могут поступать из внутренней информации организаций, в сфере энергетики, которая генерируется в информационных средах, но ранее не сохранялась и, соответственно, не анализировалась.

– нейротехнологии и искусственный интеллект (например, в делах по нарушению прав человека в Страсбургском суде (ЕСПЧ) широко применяется искусственный интеллект, который с вероятностью 79 % предсказывает судебные решения. Это позволит спрогнозировать вероятностное решение судов по расследуемым уголовным делам, что, в свою очередь, поможет определить дополнительные мероприятия, необходимые для повышения качества материалов по уголовным делам о преступлениях в сфере энергетики, предоставляемых в суд);

– системы распределенного реестра, в том числе и при расследовании уголовных дел о преступлениях в сфере энергетики [3, с. 34];

– квантовые технологии (например, возможность обеспечения кибербезопасности и сверхбезопасный обмен данными на длинных расстояниях является одной из возможностей компьютеров на основе квантовых технологий, что применяется в системах в сфере энергетики);

– компоненты робототехники и сенсорика (применяемые в сфере энергетики);

– технологии беспроводной связи (оперативное использование различных банков данных, учетов в сфере энергетики, проведение онлайн процессуальных действий и пр.);

– технологии виртуальной и дополненной реальностей (представление доказательств в суде по уголовным делам о преступлениях в сфере энергетики, моделирование исследуемых в судебном процессе событий, имеющих значение для установления обстоятельств, подлежащих доказыванию, и иных, имеющих значение для уголовных дел о преступлениях в сфере энергетики) и др.

Рассматриваемые технологии позволят вывести процессы расследования и рассмотрения уголовных дел о преступлениях, совершаемых в сфере энергетики, на совершенно иной уровень, что, с одной стороны, будет направлено на повышение эффективности в установлении виновных лиц, в определении размера причиненного ущерба и т.п., а с другой стороны, будет содействовать повышению уровня гласности при минимальной угрозе потери конфиденциальности данных следствия, уменьшению волокиты, сокращению сроков следствия; в оперативном порядке станут решаться вопросы, связанные с процедурами при осуществлении судебного контроля и прокурорского надзора, повысится качество расследования, и пр.

Таким образом, решение вопросов, связанных с цифровизацией уголовного судопроизводства, имеет прямое значение для повышения качества и эффективности производства по уголовным делам в сфере энергетики и обеспечения стабильности функционирования энергетических систем.

Библиографический список

1. Послание Президента Федеральному Собранию // Президент России. – URL: http://kremlin.ru/events/president/news/53379.

2. Бертовский, Л. В. Цифровое судопроизводство как фактор повышения качества расследования преступлений экономической направленности / Л. В. Бертовский // Мат-лы VI междунар. науч.-практ. конф. – Краснодар: Краснодарский университет МВД России, 2018. – С. 23.

3. Бертовский, Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства / Л. В. Бертовский // Проблемы экономики и юридической практики. – 2017. – № 6. – С. 34.

4. Большие данные: как извлечь из них информацию / А. Моррисон [и др.] // Технологический прогноз. – 2010. – Вып. 3.

5. Федуненко, Е. В. Кибератаки на ядерные объекты: история вопроса / Е. В. Федуненко, Е. А. Чернышева // Коммерсантъ. – 2017. – 20 янв.

УДК 343.14

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ ИСПОЛЬЗОВАНИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Бурмистрова Наталья Сергеевна
старший преподаватель кафедры уголовно-правовых дисциплин и судебно-экспертной деятельности
Пятигорский государственный университет, Пятигорск, Россия

В статье изложены некоторые аспекты использования новых методов цифровой криминалистики, а также тенденции ее развития и применения в будущем. Основное внимание уделено направлению «цифровой двойник», а также методам фиксации и использования «цифровых» доказательств.

Ключевые слова: *цифровая криминалистика, преступления, совершенные в киберпространстве; цифровой двойник преступника, компьютерная информация; электронно-цифровые следы.*

ABOUT SOME DIRECTIONS OF USING DIGITAL CRIMINALISM **N.S.**

Burmistrova Natalya Sergeevna
Senior lecturer of the Department of criminal law and forensic science
Pyatigorsk state University, Pyatigorsk, Russia

The article outlines some aspects of the use of new methods of digital forensics, as well as trends in its development and application in the future. The main attention is paid to the direction of the «digital double», as well as to the methods of fixing and using «digital» evidence.

Keywords*: digital forensics; crimes committed in cyberspace; digital criminal double, computer information; electronic digital tracks.*

Как в физическом мире, мы оставляем следы самих себя – отпечатки пальцев, волосы, волокна одежды, ДНК и так далее в тот момент, когда мы двигаемся и взаимодействуем с людьми, местами и объектами, так и в цифровой сфере любые действия пользователей оставляют следы или отголоски о себе. Эти виртуальные или цифровые следы – фрагменты файлов, журналы активности, метки времени, метаданные и т. д. – могут рассматриваться как полезная, а иногда и ключевая информация, имеющая значение по уголовному делу.

Такая информация может иметь доказательственное значение при установлении происхождения документа или программного обеспечения, в юридических целях при определении действий сторон, участвующих в уголовном деле, или даже в качестве ресурса для киберпреступления, как например кража персональных данных. Какой бы ни была мотивация, выявления и фиксации таких следов, исследование, интерпретация или реконструкция доказательств (следов) в вычислительной среде относится к сфере цифровой криминалистики [1].

Цифровая криминалистика (также называемая компьютерной криминалистикой или кибер-криминалистикой) – это практика сбора, анализа и составле-

ния отчетов об информации, найденной на компьютерах и в сетях, таким образом, что этот процесс считается допустимым в правовом контексте в качестве доказательства в уголовном или гражданском расследовании [2].

Цифровые криминалистические операции могут применяться как в правоохранительных органах в ходе расследований преступлений, так и в коммерческих, частных проектах, а также в контексте кибербезопасности.

Действия, проводимые в отдельных компьютерных системах и сетях, обычно оставляют своего рода «цифровой отпечаток» – электронно-цифровые следы [3]. Они могут варьироваться от кэшей истории веб-браузера и файлов «cookie» до фрагментов удаленных файлов, заголовков электронной почты, метаданных документов, журналов процессов и файлов резервных копий.

Для специалистов по безопасности, защищающих предприятие, или для следователей, работающих над расследованием преступления, любой или все эти аспекты криминалистических цифровых доказательств могут быть ключевыми при документировании инцидента, формулировании ответа или разработке стратегии для будущих операций.

С научной точки зрения изучение деятельности и методологии хакеров и киберпреступников вместе с цифровым криминалистическим анализом инструментов и методов, которые они используют, может дать представление о преобладающих или будущих направлениях атак, действиях киберпреступников, сетях и возникающих штаммах вредоносных программ.

С точки зрения безопасности предприятия, доказательства, полученные с применением цифрового криминалистического анализа, помогают быстро отреагировать на инциденты и предпринять меры по исправлению ситуации, при обнаружении кибератак или краже данных. Информация может быть получена по направлениям атак, новым или специализированным формам вредоносного программного обеспечения. Такой тип устойчивых и скрытых кибератак могут происходить незамеченными, в течение нескольких месяцев или даже лет, когда злоумышленники применяют ряд различных методов для получения доступа к сети, распространения через систему, а затем воплощают преступные цели.

В ходе расследований киберпреступлений следует проявлять осторожность при сборе цифровой криминалистической информации, которая впоследствии может приобрести доказательственное значение, для этого необходимо гарантировать, что данные, собираемые для криминалистического цифрового анализа, являются достоверными, насколько это возможно.

Принимая во внимание, что файлы на компьютере изменяются каким-либо образом, даже если просто открыть их в связанных приложениях, не сохраняя их, система, которая предположительно хранит судебные доказательства, имеющие отношение к делу, должна оставаться неизменной до тех пор, пока эта информация не будет извлечена в неразрушающем режиме. Это также относится к случаям, когда необходимо установить аутентификацию определенных файлов, способы доступа к ним или их использования, а также сроки проверяемых событий [4].

Поскольку компьютеры, мобильные телефоны и Интернет представляют собой крупнейший растущий ресурс для преступников, цифровая криминалистика имеет ключевое значение в правоохранительном секторе. Киберпреступления предлагают возможность совершать преступные действия, приносящие

высокий доход, при этом они имеют относительно низкий риск и не требуют физического насилия. Задача правоохранительных органов в настоящее время постоянно улучшать качество криминалистической деятельности, направленной на пресечение подлогов мошенников, кражи личных данных, вымогательств и других преступных действий в цифровом пространстве [5].

Для раскрытия сложных корпоративных преступлений требуется соответствующие технические условия и технически подкованные специалисты, а цифровая криминалистика делает именно это. Она широко охватывает идентификацию, оценку, проверку и рецензирование артефактов, связанных с компьютером или мобильными устройствами. Однако охват продолжает развиваться с появлением платформ и поддержкой искусственного интеллекта «AI» мобильных устройств с высокой степенью защиты и других всеобъемлющих тенденций в мире технологий.

По сравнению с классическими видами экспертиз, компьютерная экспертиза и ее научная база, в последние годы демонстрирует весьма привлекательные возможности. Хотя цифровая криминалистика занимала лидирующее положение последние несколько лет, во всем мире наблюдается впечатляющий всплеск использования мобильных устройств, что делает компьютерную экспертизу мобильных устройств наиболее предпочтительным выбором среди исследований в области цифровой криминалистики.

Компьютерная экспертиза мобильных устройств в рамках уголовного дела может извлечь криминалистически значимую информацию в различных случаях: например в случаях автомобильной аварии можно легко извлечь информацию о действиях водителя в точное время аварии. В мобильных устройствах также имеется множество данных, которые могут быть использованы по ходу расследования преступления, например, истории разговоров или данные о физическом местоположении и т.п.

Хотя тесная связь между физическим и технологическим миром открыла такие возможности, как разрешение уголовных дел с помощью оцифровки, она также несет в себе ряд потенциальных угроз, которые всегда связаны с его использованием.

Наиболее распространенные кибератаки включают атаки на DDoS, интеллектуальные транспортные средства и устройства VoIP, явно указывают на масштабы разработки для цифровой криминалистики в течение ближайших лет. Однако, для специалистов по цифровой криминалистике по-прежнему остается серьезной проблемой инвестировать в разработку новых методов и инструментов, которые могут удовлетворить потребности в анализе больших объемов данных, а также в составлении отчетов о потенциальных цифровых подсказках, которые могут направить дальнейшее расследование [6].

Кроме того, они подчеркивают особое внимание к постоянно развивающейся способности критического мышления человека, которая, несомненно, останется частью систем искусственного интеллекта, используемых в цифровой криминалистике, и она все еще находится на начальной стадии.

Ещё одним направлением развития цифровой криминалистики и автоматизации процесса составления психологического портрета преступника является концепция «Цифрового двойника».

Концепция «Цифровых двойников» впервые была представлена в 2002 году профессором Мичиганского университета Майклом Гривзом. В своем докладе, посвященном управлению жизненным циклом продукта (PLM), он рассказал о возможностях, открывающихся при создании виртуального пространства, которое дублировало бы реальное пространство и обменивалось с ним информацией.

Базовая концепция заключается в следующем: цифровой двойник – это цифровая копия физического объекта или процесса. В направлении реализации потребностей криминалистики «цифрового двойника» это виртуальная модель преступника, воссозданная по информации, полученной в ходе исследования материалов уголовного дела, после создания которой ее можно использовать в связке со своим физическим двойником на протяжении всего жизненного цикла: на этапах сокрытия преступления, планирования поведения в ходе расследования, социального поведения преступника. Важное свойство цифрового двойника заключается в том, что он должен быть постоянно обновляемым представлением реального физического объекта. Используемый в целях криминалистики «Цифровой двойник» – это динамическая, а не статическая модель реального человека. Ответом из виртуального пространства в реальное, становятся различные прогнозы и оценки поведения преступника, которые могут быть использованы в целях раскрытия преступления.

Библиографический список

1. Ищенко, Е. П. У истоков цифровой криминалистики / Е. П. Ищенко // Вестник Университета имени О.Е. Кутафина. – М., 2019. – С. 11.

2. Пастухов, П. С. Использование информационных технологий для обеспечения безопасности личности, общества и государства / П. С. Пастухов, М. Лосавио // Вестник Пермского университета. Юридические науки. – 2017. – Вып. 36. – С. 231–236.

3. Лушин, Е.А. О термине «электронно-цифровые следы» / Е.А. Лушин // Расследование преступлений: проблемы и пути их решения. – 2017. – № 4. – С. 161–163.

4. Вехов, В. Б. Криминалистическое значение сведений о компьютерных сетях и образующихся в них дорожках электронно-цифровых следов / В. Б. Вехов // Информационное обеспечение раскрытия и расследования преступлений. В 3 ч. Ч. 1. – Луганск: ЛГУВД, 2008. – С. 78–85.

5. Мещеряков, В. А. Криминалистика в цифровой век / В. А. Мещеряков // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сб. ст. междунар. науч.-практ. конф. – М., 2018. – С. 182–183.

6. Бахтеев, Д. В. Криминалистическая классификация цифровой доказательственной информации / Д. В. Бахтеев // Криминалистика в условиях информационного сообщества (59-е ежегодные криминалистические чтения): сб. ст. междунар. науч.-практ. конф. – М., 2018. – С. 44–49.

УДК 336.1/5

ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ ЮРИДИЧЕСКИХ ЛИЦ

Галахтин Михаил Геннадьевич
кандидат философских наук, доцент
Национальный исследовательский университет «МИЭТ», Москва, Россия

Статья посвящена правовым аспектам электронной регистрации юридических лиц. Рассмотрены особенности правоприменительной практики налоговых органов и ответственности при электронной регистрации юридических лиц.

Ключевые слова: *государственная регистрация юридических лиц, наименование и адрес юридического лица, электронная цифровая подпись, ответственность при регистрации юридических лиц.*

ELECTRONIC REGISTRATION OF LEGAL ENTITIES

Galakhtin Mikhail Gennadievich
candidate of philosophy, associate Professor
National Research University of Electronic Technology (MIET), Moscow, Russia

This paper outlines the juridical aspects of legal entities electronic registration. We have contemplated some particular questions of the law application and responsibility of the tax authorities during the legal entities registration procedures.

Keywords*: state registration of legal authorities, identification and address of a legal entity, electronic digital signature legal responsibility of the registration of legal entities.*

Одним из ключевых факторов создания благоприятной среды для бизнеса является возможность беспрепятственного выхода на рынок субъектов хозяйственной деятельности. Поддерживающая среда развития хозяйственной и инвестиционной деятельности, минимализация административных барьеров выступает своеобразным драйвером многих процессов в сфере предпринимательства, первоочередным из которых является создание юридического лица и его государственная регистрация.

Новеллы федерального законодательства в области государственной регистрации юридических лиц, закрепивших возможность удаленного направления документов в электронной форме в регистрирующий орган, практика ФНС России, активно внедряющей электронные сервисы в процедуры государственной регистрации, значительно упростили и удешевили процесс государственной регистрации юридических лиц, вывели доступность выхода на рынок для хозяйствующих субъектов на уровень стандартов самых развитых и либеральных экономик мира.

В настоящий момент ФНС России (далее ФНС) уже внедрен электронный сервис по государственной регистрации юридических лиц с полным циклом электронного документооборота, размещенный на официальном сайте ФНС (URL: https://service.nalog.ru/gosreg/#ul), который распространяется на общества с ограниченной ответственностью с единственным участником физическим лицом и типовым уставом. В отношении других юридических лиц электронный документооборот при регистрации юридических лиц носит фрагментарный характер.

Указанный сервис обладает рядом преимуществ перед традиционным способом подачи документов для государственной регистрации. Прежде всего, существенно сокращаются сроки подготовки и направления документов. Если верить информации, размещенной на сайте ФНС, процедура подготовки и передачи документов заявителем должна занимать не более 15 минут. При этом сам процесс осуществляется фактически не выходя из дома (офиса). При требуемом законом трехдневном сроке регистрации новых юридических лиц процедуры электронной регистрации могут быть сокращены до одних суток.

Электронная регистрация позволяет, кроме того, существенно снизить затраты на регистрационные процедуры. В частности, не требуется нотариальное удостоверение подписи заявителя на заявлении о регистрации. Личность в этом заявлении, как и в других документах, предоставляемых при регистрации, удостоверяется электронной цифровой подписью (ЭЦП). Сервис ФНС предоставляет заявителю возможность выбора из перечня аккредитованных удостоверяющих центров наиболее для него удобные для получения ЭЦП. С 1 января 2019 г. использование электронной регистрации юридического лица дает возможность не оплачивать государственную пошлину.

Электронные сервисы ФНС позволяют лицу, начинающему создавать свой бизнес, избежать возможных нарушений, влекущих как прямые финансовые потери, так и различные меры юридической ответственности. В частности, сервис «прозрачный бизнес» проверки контрагента на сайте ФНС (URL: https://pb.nalog.ru/about.html) позволяет выявить повторяемость фирменного наименования юридического лица и сферу его деятельности. Согласно требованиям п.1 ст. 1473 Гражданского кодекса Российской Федерации (далее ГК РФ) право на фирменное наименование как средство индивидуализации коммерческой организации возникает с момента государственной регистрации. Следовательно, все юридические лица, зарегистрированные под аналогичным наименованием позже даты регистрации правообладателя и осуществляющие сходные виды деятельности, несут риск предъявления иска о понуждении к прекращению использования чужого фирменного наименования и возмещении убытков в связи нарушением прав правообладателя (п. 4 ст. 1474 ГК РФ).

Электронные сервисы ФНС позволяют пользователям осуществлять корректный выбор адреса юридического лица в соответствии с требованиями п. 3 ст. 54 ГК РФ. В частности, пользователь имеет возможность получить информацию об адресах так называемой массовой регистрации юридических лиц. По указанным адресам по сложившейся практике ФНС юридические лица регистрироваться не могут, поскольку не предполагают возможности осуществления

связи с юридическим лицом. Данная позиция закреплена в п. 2 Постановления Пленума ВАС РФ от 30.07.2013 № 61 «О некоторых вопросах практики рассмотрения споров, связанных с достоверностью адреса юридического лица» (далее Пленум ВАС).

В указанном постановлении, в частности, указывается, что недостоверным может считаться адрес, указанный в документах, представленных при государственной регистрации, согласно сведениям ЕГРЮЛ обозначен как адрес большого количества иных юридических лиц, в отношении всех или значительной части которых имеются сведения о том, что связь с ними по этому адресу невозможна (представители юридического лица по данному адресу не располагаются и корреспонденция возвращается с пометкой «организация выбыла», «за истечением срока хранения» и т. п.). Согласно п. 1 ст. 23 федерального закона «О государственной регистрации юридических лиц и индивидуальных предпринимателей» от 08.08.2001 № 129-ФЗ (далее Закон о регистрации) недостоверность сведений об адресе юридического лица влечет отказ в его государственной регистрации.

Практика регистрации юридических лиц некоторыми инспекциями ФНС возлагает обязанности подтверждения достоверности адреса юридического лица на самих инициаторов его создания. В комплекте документов для государственной регистрации территориальные органы ФНС нередко требуют предоставления различного рода предварительных договоров аренды, гарантийных писем от собственников нежилых помещений и т. п. Данная практика полностью расходится с требованиями действующего законодательства в сфере регистрации юридических лиц. В частности, в перечне документов, предоставляемых для государственной регистрации, установленном ст. 12 Закона о регистрации подобные документы не значатся. Согласно правилам п. 4 ст. 9 Закона о регистрации регистрирующий орган не вправе требовать представление других документов кроме документов, установленных этим законом. Аналогичная позиция подтверждена в постановлении Пленума ВАС, который отметил, что регистрирующий орган не вправе возлагать на лицо, обратившееся с соответствующим заявлением о государственной регистрации, бремя подтверждения достоверности представленных сведений об адресе юридического лица, в том числе путем представления дополнительных документов помимо предусмотренных законом.

Применение электронного формата регистрации юридических лиц порождает определенные особенности юридической ответственности за правонарушения в этой сфере. В частности, в ст. 25 Закона о регистрации предусмотрена ответственность за непредставление или несвоевременное представление необходимых для включения в государственные реестры сведений, а также за предоставление недостоверных сведений. При существенных (неустранимых) нарушениях действующего законодательства при создании юридического лица оно может быть ликвидировано в судебном порядке по иску регистрирующего органа. К таким нарушениям при электронной регистрации юридических лиц можно отнести, например, использование электронной цифровой подписи, выданной с нарушением правил выдачи квалифицированных сертификатов.

Более сложный механизм ответственности за преступления в сфере регистрации юридических лиц предусмотрен уголовным законом. В ст. 173.1 Уголовного кодекса Российской Федерации (далее УК РФ) установлена уголовная ответственность за регистрацию юридических лиц через так называемых подставных лиц. Под подставными лицами в отмеченной статье УК РФ понимаются лица, которые являются учредителями (участниками) юридического лица или органами управления юридического лица и путем введения в заблуждение либо без ведома которых были внесены данные о них в единый государственный реестр юридических лиц, а также лица, которые являются органами управления юридического лица, у которых отсутствует цель управления юридическим лицом. Применительно к формату электронной регистрации юридических лиц объективная сторона преступления будет характеризоваться, прежде всего, использованием чужой ЭЦП без ведома ее обладателя, либо посредством введения его в заблуждение, либо посредством неправомерного завладения. В этом случае именно ЭЦП, выступающее единственным механизмом идентификации заявителя, является предметом преступного умысла. Вместе с тем ст. 173.2 УК РФ предусматривает уголовную ответственность лишь за незаконное использование документов, удостоверяющих личность, повлекшее внесение в единый государственный реестр юридических лиц сведений о подставных лицах. Таким образом, лица, неправомерно в преступных целях использующие ЭЦП не подпадают под действие указанной статьи УК РФ. Ситуация проблематичности доведения ответственности до конкретных лиц усугубляется тем, что законодательство об использовании ЭЦП не содержит однозначного запрета на передачу использования ЭЦП третьим лицам. Не предусмотрена в этом случае уголовная ответственность и в статьях главы 28 УК РФ «Преступления в сфере компьютерной информации». Законодатель предусмотрел лишь административную ответственность аккредитованного удостоверяющего центра за правонарушения при выдаче квалифицированного сертификата ключа проверки ЭЦП, содержащего заведомо недостоверную информацию о его владельце. При этом сотрудники этих центров за неправомерные действия при выдаче сертификатов ни административной, ни уголовной ответственности не несут. С учетом того, что использование ЭЦП все больше становится нормой имущественного и документального оборота усиление ответственности за ее незаконные выдачу и использование становятся важной задачей обеспечения кибербезопасности в Российской Федерации.

УДК 651

ПРАВОВЫЕ АСПЕКТЫ ПРИ ВНЕДРЕНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ПРЕДПРИЯТИИ

Галахтина Екатерина Михайловна
Национальный исследовательский университет «МИЭТ», Москва, Россия

В работе анализируются правовые аспекты при внедрении системы электронного документооборота на предприятии, а также обосновывается необходимость внедрения данных систем.

Ключевые слова: *электронный документооборот, бумажный документооборот, информационная сфера, информационное право, внедрение, электронная подпись, электронный документ.*

LEGAL ASPECTS IN THE IMPLEMENTATION OF ELECTRONIC DOCUMENT MANAGEMENT AT THE ENTERPRISE

Galakhtina Ekaterina Mikhailovna
National Research University of Electronic Technology (MIET), Moscow, Russia

The paper analyzes the legal aspects of the implementation of the electronic document management system in the enterprise, and justifies the need for the introduction of these systems.

Keywords*: electronic document management; paper document management; information sphere; information law; implementation; electronic signature; electronic document.*

Делопроизводство красной линией проходит через всю деятельность современной компании, охватывая основу работы предприятия. Ведение документооборота вручную способствует огромного количеству ошибок, связанных с человеческим фактором, потере данных и связей между документами. В связи с подобными проблемами процесс согласования неоправданно затягивается, а реализационная деятельность предприятия страдает от не вовремя оформленных счетов, договоров и при работе с контрагентами.

Внедрение системы управления документооборотом имеет решающее значение для обеспечения бесперебойной работы предприятия. С помощью СЭД компании могут значительно облегчить управление потоком информации во всей организации.

На сегодняшний день активно развивается информационное общество, где знание и информация становятся одним из условий успешного ведения бизнеса. Информация превратилась в фактор, существенным образом влияющий практически на все сферы общественной жизни. В данном разрезе, развитие электронного документооборота следует по пути глобализации.

Производилось много различных исследований по темам правового обеспечения, внедрения, сопровождения, ведения, возникновения электронного документооборота. Отдельные аспекты электронного документооборота проанализированы в различных диссертационных работах и статьях, стоит отметить статью «Актуальные аспекты формирования и применения систем электронного документооборота в управлении» П.В. Глущенко [1], в которой автор поставил своей задачей изучение проблем взаимодействия права и информационных процессов.

Любая солидная компания с целью поддержания своего имиджа и авторитета, будучи участником товарно-денежных отношений, обладающая экономической самостоятельностью, соответственно, отвечающая за итоги своей хозяйственной деятельности, обязана создать у себя такую модель управления, которая гарантировала бы эффективность её деятельности, конкурентоспособность, внедряя инновационные технологии, обеспечивающие стабильное место на рынке.

При внедрении электронного документооборота проявляются правовые аспекты, затрагивающие важные части делопроизводства, к которым компания должна адаптироваться.

Возникает работа в области информационного права, характеризующиеся быстрым темпом внедрения инновационных технологий в практику работы различных процессов предприятий, формируя информационную сферу и её процессы - создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации [2].

При создании информационной сферы на предприятии возникают общественные отношения, подлежащие правовому регулированию, при выполнении информационных процессов. Эти общественные отношения составляют основной предмет информационного права, предмет его правового регулирования и аспектов [3].

В любой стране правовые аспекты являются неотъемлемой частью успешной бизнес-среды. Они гарантируют, что каждая компания функционирует в соответствии с законодательными рамками страны. Каждое предприятие должно принимать во внимание эту правовую структуру при определении основных целей и задач своей компании. Это необходимо для эффективного и здорового функционирования организации и помогает ей узнать о правах, обязанностях, а также проблемах, с которыми она может столкнуться.

Ведение делопроизводства является важной частью управления организацией. Формирующиеся внутри компании информационная сфера подталкивает предприятия ведущие «бумажный документооборот» внедрять инновационные технологии в виде системы электронного документооборота (СЭД).

После анализа различных источник, в особенности работы П.В. Глущенко, выведенных аспектов формирования и применения СЭД, были выделены основные цели внедрение системы электронного документооборота – это обеспечение поддержки делопроизводства, регламентация и контроль процесса движения внешних и внутренних документов на предприятии, формирование единого информационного пространства, упрощение процессов поиска и хранения документации, сокращение бумажного документооборота, обеспечение сохранности информации и отслеживание взаимоотношений с контрагентами [1].

Внедрение электронного документооборота — это шаг к современному управлению информационными потоками. По данным CNews Analytics, отечественный рынок СЭД — один из наиболее активно развивающихся сегментов IT-индустрии [4]. Это объясняется тем, что основным потребителем программ является государство.

После появления электронных документов (ЭД) в законодательстве были определены стандарты оформления бумаг. Они записаны в ГОСТ Р 6.30-2003 [5]. После этого многое в документообороте изменилось: появились электронные документы, подписи и прочее. Это привело к необходимости создания нового государственного стандарта. Результатом стал ГОСТ Р 7.0.97-2016. В новом ГОСТ закрепляются основные требования к оформлению бумажных и электронных документов [6].

Несмотря на удобство и современность, немногие российские компании внедряют электронный документооборот. С точки зрения права и регулирование делопроизводства предприятия, появление СЭД означало возникновение таких проблем и вопросов, как: условия определения юридической значимости ЭД, проблема законодательного регулирования электронного документооборота, проблема хранения электронных материалов, проблемы внедрения систем электронного документооборота, электронная подпись, электронные платежи, сбор, учет, защита персональных данных, документов с коммерческой тайной в электронном пространстве и прочее.

Недостаточное акцентирование внимания государства к внедрению СЭД проявляется в малом интересе к составлению законодательно-нормативной базы, которая позволила бы обширнее применять электронные материалы и современные технологии как в государственном управлении, так и в коммерческой деятельности [7].

В будущем возможность составлять и получать первичные документы только в электронном виде, а также принимать эти документы для бухгалтерского и налогового учета, способствует налаженному информационному потоку между государственными структурами и коммерческими организациями. На данный момент для формирования потока электронных документов между организациями необходимо заключение сторонами Соглашения об обмене электронными документами [8].

Договор об обмене электронными документами должен быть заключен в письменной форме, данный аспект зафиксирован в ГК РФ статье 434. Форма договора. Кроме того, законодательство позволяет заключать его в электронной форме с использованием электронной подписи. Однако во избежание недоразумений с контрагентом со стороны инспекционных органов и аудиторских проверок, используют бумажный вид.

Подобные аспекты ставят под сомнения использование доступных, в рамках внедренной СЭД, преимуществ. Невозможность предприятия перейти на электронный документооборот полноценно, заставляют постоянно метаться из стороны в стороны, частично дублируя работу и усложняя процессы.

Большинство СЭД имеет возможность использовать цифровую подпись в рамках системы, однако правовых нюансов и упущений при использовании электронной подписи так много, что российский предприниматель предпочитает не

пользоваться данной функцией вовсе. О данных правовых аспектах пишет в своей статье «Электронная подпись: опыт комплексного изучения» Роман Туркин, как решение Туркин предлагает, что в законодательство и практику работы с электронными документами должны быть внесены целый ряд новшеств, создавая условия для популяризации электронной подписи, что впоследствии создаст благоприятную среду для работы с информационными продуктами в целом.

Несмотря на молодость отрасли информационного права, и темпы перехода современных предприятий в информационную сферу, фокусировка внимания на безбумажные технологии давно назрела в экономике и предпринимательстве. Внедрение электронного документооборота позволит автоматизировать процессы делопроизводства предприятия и вести единую информационную среду по работе с документами, позволит исключить потерю документов, учет документов, обеспечить прозрачную версионность, а также поможет отследить неоправданное затягивание согласования, что позволит каждый раз оптимизировать процессы.

Библиографический список

1. Актуальные аспекты формирования и применения систем электронного документооборота в управлении // URL: https://cyberleninka.ru (дата обращения: 22.02.2020).
2. Костылев, А. К. Информационное право / А. К. Костылев. – 3-е изд. Тюмень: Издательство Тюменского государственного университета, 2010. 29 с.
3. Костылев А. К. Информационное право / А. К. Костылев. – 3-е изд. Тюмень: Издательство Тюменского государственного университета, 2010. 34 с.
4. Российские ИТ-компании выходят из стагнации и возобновляют рост [Электронный ресурс]. – URL: https://www.cnews.ru/reviews/rynok_it_itogi_2018/articles/rossijskie_itkompanii_vyhodyat_iz_stagnatsii_i_vozobnovlyayut_rost (дата обращения: 22.02.2020).
5. ГОСТ Р 6.30-2003. Унифицированные системы документации. Требования к оформлению документов [Электронный ресурс] – URL: https://base.garant.ru/185891/ (дата обращения: 22.02.2020).
6. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов [Электронный ресурс] – URL: http://www.consultant.ru/document/cons_doc_LAW_216461/ (дата обращения: 22.02.2020).
7. Артеменко, А. А. Актуальные вопросы информационного права / А. А. Артеменко // Молодой ученый. – 2018. – № 11. – С. 742–744.
8. Соглашение об электронном документообороте между юридическими лицами. – URL: https://assistentus.ru/forma/soglashenie-ob-ehlektronnom-dokumentooborote-mezhdu-yuridicheskimi-licami (дата обращения: 22.02.2020).

УДК 343.98:004

ПРОТИВОДЕЙСТВИЕ УГОЛОВНОМУ ПРЕСЛЕДОВАНИЮ ПО УГОЛОВНЫМ ДЕЛАМ О КИБЕРПРЕСТУПЛЕНИЯХ И СРЕДСТВА ЕГО ПРЕОДОЛЕНИЯ: ПРОБЛЕМЫ ТЕОРИИ И ДИДАКТИКИ

Гармаев Юрий Петрович
доктор юридических наук, профессор,
Кубанский государственный аграрный университет, Краснодар, Россия

В статье рассматривается проект учебной программы Московского института электронной техники по подготовке специалистов в области расследования киберпреступлений и инцидентов. Вносятся предложения по поводу спецкурса «Преодоление противодействия уголовному преследованию по уголовным делам о киберпреступлениях», концепция которого существенно отличается от традиционных взглядов на соответствующую частную криминалистическую теорию.

***Ключевые слова**: противодействие уголовному преследованию, преодоление противодействия уголовному преследованию, частная криминалистическая теория, расследование киберпреступлений, криминалистика.*

COUNTERING THE PROSECUTION OF CRIMINAL CASES ABOUT CYBERCRIMES AND MEANS TO OVERCOME IT: PROBLEMS OF THEORY AND DIDACTICS

Garmaev Yuri Petrovich
Doctor of Law, Professor,
Kuban State Agrarian University, Krasnodar, Russia

The article discusses the draft curriculum of the Moscow Institute of Electronic Technology for the training of specialists in the investigation of cybercrimes and incidents. Suggestions are being made about the special course «Overcoming the Counteraction to Criminal Prosecution in Criminal Cases of Cybercrime», the concept of which differs significantly from traditional views on the corresponding private forensic theory.

***Keywords**: opposition to criminal prosecution, overcoming opposition to criminal prosecution, private forensic theory, investigation of cybercrime, MIET, forensic science.*

Уже не требует каких-либо дополнительных обоснований тезис об актуальности повышения эффективности мер противодействия киберпреступлениям и, соответственно, инициативы Московского института электронной техники (далее – МИЭТ) по подготовке специалистов по программе, обеспечивающей получение обучающимися компетенций, необходимых для расследования киберпреступлений и инцидентов. Действительно такая инициатива не имеет аналогов в стране и перспективы ее реализации представляются весьма плодотворными. Прежде всего, для самих обучаемых.

Предложенная программа, проект учебного плана, составленные в институте и представленные заранее участникам конференции, также заслуживают высокой оценки. По тематике дисциплин антикриминального цикла проект включает такие уникальные предметы, как:

– расследование преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

– расследование преступлений, связанных с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных компьютерных программ;

– квалификация преступлений в сфере высоких технологий;

– криминалистическое исследование виртуальных следов и др.

В проекте учебного плана есть и иные, не менее актуальные и притом нечасто встречающиеся в других юридических вузах (во всяком случае, в «гражданских») дисциплины:

– «Методика расследования преступлений коррупционной направленности»;

– «Основы оперативно-розыскной деятельности»;

– «Организация следственной деятельности» и др.

Поскольку от оргкомитета конференции еще в прошлом году поступила просьба высказать частное мнение по вопросам оптимизации учебного плана, сформулируем некоторые предложения по его дополнению и уточнению.

Первое предложение касается введения дисциплины под названием: «Противодействие уголовному преследованию и средства его преодоления (по уголовным делам о киберпреступлениях)». Как известно присутствующим на конференции коллегам – ведущим ученым-криминалистам России, соответствующая криминалистическая частная теория уже многие десятилетия привлекает внимание ученых и практиков. В литературе ее название чаще выглядит следующим образом: «Преодоление противодействия уголовному преследованию» или «Преодоление противодействия предварительному расследованию».

На наш взгляд, становление и развитие теории прошло три этапа [5]. В частности, начало исследованию проблемы положили такие авторитетные ученые, как О.Я. Баев, Р.С. Белкин, Г.Г. Зуйков, В.Н. Карагодин, В.П. Лавров, И.М. Лузгин, В.А. Овечкин и другие [2, 4, 8, 9]. Формирование данной частной криминалистической теории послужило основой и драйвером дальнейшего совершенствования криминалистической тактики и криминалистической методики.

Так, начало третьего тысячелетия характеризуется разработкой и внедрением целого ряда монографических работ по преодолению противодействия применительно к отдельным видам преступлений (В.А. Ищенко, А.Б. Петрунина, И.В. Тишутина и др.) [7, 10, 12]. В настоящее время происходит активное развитие частной криминалистической теории преодоления противодействия уголовному преследованию именно по этому направлению, которое условно можно обозначить как частно-методическое или «направление пополнения криминалистических методик».

Одной из последних крупных работ по данной тематике является учебник под общей редакцией Б.Я. Гаврилова, В.П. Лаврова [11]. Хотелось бы подчеркнуть, что издание предназначено, прежде всего, для изучения одноименной

дисциплины в вузах системы МВД России. К сожалению, этот предмет изучается на обязательной основе только в вузах министерства, что не соответствует уровню ее актуальности, востребованности для всех будущих и действующих юристов. Обобщая личный многолетний опыт проведения занятий по этому спецкурсу в классическом вузе и занятий по повышению квалификации для следователей, адвокатов и прокуроров (вводная лекция автора на эту тему по ссылке: https://youtu.be/_gs0x_PucPE), отмечу, что результаты анкетирования и интервьюирования более 500 респондентов из обоих групп (студенты и правоприменители) показали их 100%-ую заинтересованность в этом предмете, высокий уровень мотивации к его изучению по причинам, излагаемым ниже.

Дальнейшее изучение проблем преодоления противодействия уголовному преследованию на научном, дидактическом и практическом уровне имеет самые широкие перспективы для гражданских вузов в целом, и для МИЭТ в частности. Но при условии не изменения, а некоторого уточнения как методологических основ этой частной теории, так и методики преподавания соответствующего предмета.

Начнем с первого – с методологии. Рассмотрим проблемы предмета теории (учебной дисциплины) и ее понятийного аппарата. Авторы упомянутого учебника определяют противодействие расследованию преступлений как совокупность умышленных противоправных и иных действий преступников (а также связанных с ними лиц), направленных на воспрепятствование деятельности правоохранительных органов по выявлению, раскрытию и расследованию преступных деяний [11, с. 9]. В целом соглашаясь с определением, отметим, что в нем и в целом – в авторской концепции, заложена некая, условно говоря, обвинительная правовая позиция. Не следует путать ее с пресловутым обвинительным уклоном. Обвинительная позиция – это всегда позиция, основанная на законе. Обвинительный же уклон – это порой преступное игнорирование сведений, свидетельствующих о невиновности либо о меньшей степени виновности привлекаемого лица. Исходя из нее всякое противодействие, хоть и определяемое как «противоправное *или иное*», все же рассматривается как некий негативный феномен. Такое допущение - а точнее эта часть парадигмы всей науки криминалистики - безусловно, имеет право на жизнь. Но можно использовать и иной подход. Далее по тексту адаптируем этот подход к упомянутому учебному плану МИЭТ.

Во-первых, можно было бы шире подходить к оценке целей и мотивов субъектов противодействия по уголовным делам о киберпреступлениях и расследования инцидентов. В реальной практике таковыми далеко не всегда являются лишь «воспрепятствование выявлению, раскрытию и расследованию преступлений (и инцидентов)». В реальности существуют и иные цели, мотивы противодействия.

Цели:

– изменение меры пресечения в виде заключения под стражу на иную, более мягкую;

– если человек арестован, то добиться тех или иных преимуществ в местах содержания под стражей;

– смягчение обвинения и иное: переквалификация деяния на менее тяжкие статьи УК РФ, исключение из объема обвинения отдельных эпизодов, иные

обстоятельства уголовно-правового, уголовно-процессуального и иного характера, правомерно улучшающие положение подозреваемого (обвиняемого).

Мотивы:

– субъективная уверенность противодействующего лица в полной или частичной невиновности подозреваемого (обвиняемого);

– субъективная уверенность противодействующего лица в том, что доказательства вины подозреваемого (обвиняемого) получены с нарушениями закона, а потому не могут быть признаны допустимыми;

– иная незаконная, неэффективная и/или аморальная, по мнению субъекта противодействия, деятельность отдельных сотрудников правоохранительных органов и суда.

Например, программист в организации, совершивший по неосторожности деяния с признаками преступления – нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) субъективно уверен, что в его действиях нет состава преступления. Он недавно был принят на работу, не имел наставника, не был ознакомлен с инструкциями, обеспечивающими безопасность компьютерной информации в организации. В результате неустановленные лица – хакеры (следует обратить внимание на многозначность этого термина в области вычислительной техники и программирования. В том числе, как позитивную, так и негативную правовую и эмоциональную его окраску. См.: URL: https://goo-gl.su/pWfILpO4) получили к ней неправомерный доступ. Кроме того, в рамках опроса оперативный сотрудник вел себя грубо, угрожал лишением свободы, требовал дать компрометирующую информацию на руководство организации. При таких обстоятельствах программист наверняка будет противодействовать уголовному преследованию. Например, он откажется от дачи показаний или будет отрицать свою вину, с помощью адвоката потребует производства экспертиз и т. п. Все это – акты противодействия. Но они законные и их мотив – субъективная уверенность противодействующего в своей полной невиновности, а также в незаконности и аморальности действий сотрудника правоохранительного органа.

Исходя из изложенного, предлагаем следующее определение противодействия. Противодействие уголовному преследованию — это противоправная или законная деятельность заподозренных, подозреваемых или обвиняемых, а также содействующих им лиц, сопровождающаяся созданием препятствий для реализации представителями стороны обвинения поставленных ими задач на досудебных и судебных стадиях уголовного судопроизводства.

В данном определении, прежде всего, акцентируется внимание на следующем:

– противодействие может быть не только противоправным, но и законным. Как верно отметила Э.У. Бабаева, отказ обвиняемого от дачи показаний, дача им заведомо ложных показаний не являются уголовно наказуемыми, поскольку это вытекает из необходимости права на защиту [1, с. 154]. А такого рода правомерных актов противодействия, как показывает практика, великое множество;

– противодействие создает некие препятствия для реализации представителями стороны обвинения, поставленных ими перед собой задач, некоторые из

которых, а также средства их решения, могут быть и ошибочными, неправомерными и даже преступными.

Уже в дидактическом и практическом (а не в научном) контексте данной проблематики, обратим внимание на следующие закономерности. Какая-то часть, а может и большинство обучаемых по названной программе в МИЭТ, по его окончании не будет работать в правоохранительных органах или поработает в них недолго. А вот защищаться самим и защищать своих родных и близких от уголовного преследования, а значит зачастую и противодействовать ему, придется очень и очень многим, если не всем, в том числе и законопослушным, добросовестным гражданам. К сожалению, практика показывает, что защищать и защищаться от клеветы и обвинений (в том числе и ложных) в преступной и иной противоправной деятельности придется буквально всем следователям, оперативным сотрудникам и иным правоохранителям.

Упомянутое выше и регулярно проводимое анкетирование студентов показало, что из двух компонентов спецкурса 83 % обучаемых больше заинтересовалась первым – актами противодействия уголовному преследованию, нежели вторым – их преодолением. По первому компоненту задается более 70 % всех вопросов на занятиях. Студенты просят дополнительных консультаций по конкретным жизненных ситуациям, где они или их близкие могут быть привлечены или привлекаются к уголовной ответственности.

По ситуациям, связанным с киберпреступлениями, усматривается особая закономерность. Рассуждая по аналогии, скажем так: редко кто из обучаемых в юридическом вузе может представить себя в роли террориста, насильника или убийцы и, соответственно, проявлять нездоровый интерес к актам противодействия по уголовным делам об этих преступлениях. Между тем, представить себя в ситуации начала уголовного преследования (в том числе, незаконного) по подозрению в неправомерном доступе к компьютерной информации (ст. 272 УК РФ и сопутствующие) может, вероятно, каждый из обучаемых по названной учебной программе.

Осознание этих обстоятельств может дать обучаемым в МИЭТ и практическим работникам (на курсах повышения квалификации в том же вузе) глубокую и устойчивую личную мотивацию к изучению данной частной теории и учебной дисциплины.

Следует обратить внимание, что в проекте учебного плана заложена важная компетенция: «Способность соблюдать и защищать права и свободы человека и гражданина». Традиционно она обеспечивается такими дисциплинами как «Конституционное право России» и другие. В МИЭТ закладывается еще и такой предмет как «Информационная культура». При всей полезности этих знаний, полагаем, что они не носят в полной мере прикладного характера. Вместе с тем нет и не может быть в учебном плане такого предмета, как «Защита от уголовного преследования по делам о …». Учить такому категорически не следует.

Однако в рамках предлагаемого и притом уже апробированного в течение многих лет спецкурса, на основе предложенной методологии, в ходе занятий обучаемые могут многократно обсуждать следующие тезисы, носящие принципиальный характер:

1. Противодействовать уголовному преследованию можно, в том числе и по уголовным делам (материалам, в иных ситуациях наличия подозрений) о признаках киберпреступлений и в рамках расследования инцидентов. Но ТОЛЬКО законными и этически допустимыми средствами.

2. Недопустимо распространять знания о том, как совершать киберпреступления и уходить от ответственности за них, пусть даже законными средствами.

3. Нужно внедрять рекомендации по выбору доверителем адвоката и взаимодействию с ним.

4. Нужно защищать, в том числе, следователей и оперативных сотрудников от клеветы и незаконного обвинения.

5. Следует использовать самые современные информационные ресурсы и программные средства, а также криминалистические рекомендации, направленные на защиту собственных персональных данных, гарантированных Конституцией России прав на тайну переписки, телефонных и иных переговоров, и т. д. Все это, в том числе, для правомерной защиты от уголовного преследования, а также от деятельности ОПГ, ОПС, направленных на преступное собирание и использование указанных персональных данных и иной информации.

Названные подходы должны быть отражены в УМКД предлагаемой дисциплины. И это только некоторые подходы. Весь их комплекс должен обсуждаться дополнительно.

Следующее предложение носит характер уточнения по поводу уже имеющихся в учебном плане предметов. Материалы предлагаемого спецкурса могут и должны использоваться в рамках занятий по другим упомянутым выше дисциплинам. Например, по курсу «Квалификация преступлений в сфере высоких технологий» считаем возможным, после дополнительных консультаций между преподавателями, предусмотреть рассмотрение проблем необоснованных уголовно-правовых рисков, включая незаконное привлечение к уголовной ответственности и средства защиты от такового.

По курсу «Методика расследования преступлений коррупционной направленности» в обязательном порядке следует указывать на широко распространенную (увы, это так!) практику незаконного привлечения к уголовной ответственности различных категорий лиц, особенно «взяткодателей» (широко распространена провокация преступлений). Рассматривая закономерности высоких коррупционных рисков целого ряда профессий и должностей, сфер деятельности, можно раскрывать типичные акты противодействия по делам данной категории и наиболее эффективные средства их преодоления, включая: уголовно-правовые, уголовно-процессуальные, оперативно-розыскные, а также технико-, тактико- и методико-криминалистические. Особое внимание – к средствам преодоления противодействия с использованием новейших информационных технологий.

При реализации подобных подходов можно добиться впечатляющих результатов в плане качества подготовки юристов данной специализации, высокой мотивации их как к учебе, так и к работе по специальности, а также эффективного продвижения высококачественного «образовательного продукта» в сфере высшего образования, повышения рейтинга МИЭТ как ведущего вуза страны.

Библиографический список

1. Бабаева, Э. У. Проблема теории и практики преодоления противодействия уголовному преследованию / Э. У. Бабаева. – М.: Юрлитинформ, 2006.
2. Баев, О. Я. Конфликты в деятельности следователя (вопросы теории). / О.Я. Баев. – Воронеж, 1981.
3. Баев, О. Я. Криминалистическая адвокатология как подсистема науки криминалистики / О. Я. Баев // Профессиональная деятельность адвоката как объект криминалистического исследования. – Екатеринбург, 2002.
4. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике / Р. С. Белкин. – М., 1988.
5. Гармаев, Ю. П. Преодоление противодействия уголовному преследованию в следственных изоляторах / Ю.П. Гармаев, Б. А. Поликарпов. – М.: Юрлитинформ, 2019. – 232 с.
6. Зашляпин, Л. А. Основные компоненты теории адвокатского мастерства в уголовном судопроизводстве / Л. А. Зашляпин. – Екатеринбург: Изд-во УрГУ, 2007.
7. Ищенко, В. А. Противодействие предварительному расследованию в местах лишения свободы и основные направления его нейтрализации: дис. … канд. юрид. наук. / В. А. Ищенко. – М., 2007.
8. Карагодин, В. Н. Преодоление противодействия предварительному расследованию / В. Н. Карагодин. – Свердловск: Изд-во УрГУ, 1992.
9. Лавров, В.П. Криминалистические проблемы установления способа сокрытия тяжких преступлений против личности / В. П. Лавров // Вопросы криминалистики и судебной экспертизы по делам о тяжких преступлениях. – Караганда, 1985.
10. Петрунина, А. Б. Противодействие расследованию преступлений в сфере незаконного оборота наркотиков и криминалистические методы его выявления и преодоления: дис. ... канд. юрид. наук / А. Б. Петрунина. – М., 2006.
11. Противодействие расследованию преступлений и меры по его преодолению: учебник для вузов / под общ. ред. Б. Я. Гаврилова, В. П. Лаврова. – М.: Юрайт, 2017. – 205 с.
12. Тишутина, И. В. Преодоление противодействия расследованию организованной преступной деятельности (организационно-правовые и тактические основы): автореф. дис. … д-ра юрид. наук. / И. В. Тишутина. – М., 2013.
13. Эксархопуло, А. А. Предмет и система криминалистики: проблемы развития на рубеже XX–XXI веков / А. А. Эксархопуло. – СПб.: Изд-во СПбГУ, 2004.

УДК 343.98

СОВРЕМЕННЫЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Гладких Антон Валентинович
ассистент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается проблемных моментов, возникающих при исследовании противодействия терроризму и экстремизму в сети интернет. В частности, рассматриваются особенности развития цифровой техники, развития законодательства на отечественном и международном уровне. Предложены пути решения установленных проблем.

Ключевые слова: *мировое развитие, экстремизм, терроризм, сети интернет, современные особенности, информационные технологии, противодействие.*

MODERN FEATURES OF THE COUNTER-TERRORISM AND EXTREMISM ON THE INTERNET

***Gladkikh* Anton Valentinovich**
assistant
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article deals with problematic issues arising in the study of countering terrorism and extremism, the issues of the effectiveness and security of wireless video surveillance systems. In particular, the features of the development of digital technology and the capabilities of modern equipment to investigate and counter terrorism are considered. The ways of solving the established problems are proposed.

Keywords: *world development, extremism, terrorism, the Internet, modern features, information technology, counteraction.*

Современный этап мирового развития характерен тем, что большое внимание уделяется информационной среде. Характеризуется это тем, что современные общественные отношения отличаются сбором, обработкой, хранением и распространением информации- эти процессы в дальнейшем влияют как на экономическое, так и на социальное и духовное мировое развитие.

Доказательством этого является подписание руководителями восьми ведущих стран мира «Окинавской хартии глобального информационного общества» 22 июля 2000 года. В данном документе указанно, что «информационно-телекоммуникационные технологии стали одним из наиболее важных факторов, влияющих на формирование общества XXI века» [1].

Так же большим толчком в развитии информационных технологий стало изобретение смартфонов, что в свою очередь дало возможность доносить ин-

формацию в кратчайшие сроки до конкретного пользователя, причем информацию различного вида, в том числе письменную, фото и видео, а также появилась возможность вести прямые эфиры в Интернет.

Подтверждением высокого роста развития данных технологий являются данные Федеральной службы государственной статистики, а именно мониторинг развития информационного общества в Российской Федерации. По этим данным:

- Проникновение подвижной радиотелефонной (сотовой) связи на 100 человек населения в 2010 г. 166,4 единицы [2].
- Число абонентов фиксированного широкополосного доступа в Интернет на 100 человек населения в 2010г. данных нет, в 2011 г. 12,2 абонентов, в 2017 г. 21,0 абонентов.
- Число абонентов мобильного широкополосного доступа в Интернет на 100 человек населения в 2010 г. данных нет, в 2011г. 47,8 абонентов, в 2017 г. 79,9.

Исходя из этих данных, можно сделать вывод, что общество на современном этапе развития стремится к использованию информационных технологий и более того, активно использует сотовую связь и мобильный Интернет в качестве основных инструментов коммуникации.

Не смотря на общее благо данных технологий, общество создало новые потенциальные угрозы, в том числе в области терроризма и экстремизма, именно в этой сфере возникли большие изменения.

Развитие новых технологий расширило возможности террористических и экстремистских организаций и дало новые инструменты для подготовки и проведения терактов и ведения своей деятельности.

Следует подчеркнуть современные особенности терроризма и экстремизма:

- получение сильного эмоционального и психологического эффекта от своих действий также чувства неуверенности, страха и шока;
- распространение информации о совершенных терактах среди широкого круга людей, в том числе и в другие страны;
- при помощи социальных сетей нагнетать обстановку и искажать информацию о террористических актах;
- распространять свою идеологию и взаимодействовать со своими последователями путем передачи шифрованной информации в том числи с использованием социальных сетей.

Ярким примером использования Интернета в целях террористов и экстремистов может стать стрельба в мечетях города Крайсчерча два последовательных теракта произошли в мечетях во время пятничной молитвы 15 марта 2019 г. Стрелок транслировал нападение при помощи камеры GoPro в социальную сеть Facebook в дальнейшем трансляцию и саму видео запись подхватили другие социальные сети в результате нападения был убит 51 человек и ранены 49 человек, а трансляцию и последующие видео записи увидели миллионы людей в различных странах что принесло колоссальные социальные последствия в том числе разжигание новых меж религиозных конфликтов, расизма, экстремизма и чувства общего страх ведь до этого момента Новая Зеландия считалась одной из самых спокойных стран.

Несмотря на открытые действия террористов и экстремистов, всегда есть скрытое воздействие и последствие, примером может послужить распространение ложной информации через социальные сети, ведь информация в Интернете распространяется очень быстро, и в том числе эту же информацию используют неопытные репортеры и тоже становятся ее распространителями, что в последствии может привести к информационным войнам.

Все это свидетельствует о том, что есть актуальная проблема противодействия данным явлениям и существует большая потребность в создании информационных барьеров и механизмов. На практике информационная борьба с терроризмом и экстремизмом носит защитный характер и все меры по борьбе с данными явлениями сводится к тому, что после происшествия информация проверяется блокируется и опровергается и происходит это через большой промежуток времени и не несет предупредительных мер. Это на наш взгляд серьезная уязвимость ведь информационное воздействие терроризма носит именно наступательный характер.

На наш взгляд исправить сложившеюся ситуацию поможет:

- информационное противодействие терроризму, экстремизму и т. д.;
- обеспечение контртеррористической деятельности через средства массовой информации в том числе и социальные сети;
- поиск и сбор информации о деятельности не только самих террористов, но и взаимосвязь их с распространителями ложной информации и информации, направленной на запугивание людей;
- информационное воздействие на сознание самих террористов, их посредников и всех, кто им помогает;
- просвещение населения о правилах пользования информацией с целью предотвращения стихийного распространения недостоверных данных и поднятия общего самосознания населения.

По нашему мнению, стоит создать сайт с интеграцией его в мобильное приложение, в котором будет методическая информация о том, как взаимодействовать с информацией о готовящихся террористических актах или уже совершенных, а также различной экстремисткой деятельности. Необходимо это прежде всего для обучения населения, что вследствие приведет к более разумной реакции на совершаемые преступления, снизит панику и не желательное распространение ложной информации. Ведь если террористы и экстремисты не смогут посеять панику, то и смысла в совершаемых ими действиях нет.

Библиографический список

1. Окинавская хартия Глобального информационного общества 21 июля 2000 года. – URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 17.02.2020).

2. Мониторинг развития информационного общества в Российской Федерации. – URL: https://www.gks.ru/storage/mediabank/monitor_rf(3).xls (дата обращения: 18.02.2020).

УДК 004.056.53

ВОПРОСЫ ОРГАНИЗАЦИИ И ЗАЩИТЫ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ СТРАТЕГИЧЕСКИХ ОБЪЕКТОВ И ПОМЕЩЕНИЙ С МАССОВЫМ ПРЕБЫВАНИЕМ ГРАЖДАН

Гладких Антон Валентинович
ассистент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается проблемных моментов, возникающих при исследовании противодействия терроризму и экстремизму, вопросам эффективности и безопасности систем беспроводного видеонаблюдения. В частности, рассматриваются особенности развития цифровой техники, и возможности современной аппаратуры способствовать расследованию и противодействию терроризму. Предложены пути решения установленных проблем.

Ключевые слова: *мировое развитие, терроризм, сети интернет, современные особенности, информационные технологии, противодействие, системы видео наблюдения D-Dos атаки.*

ISSUES OF THE ORGANIZATION AND PROTECTION OF VIDEO SURVEILLANCE SYSTEMS OF STRATEGIC OBJECTS AND PREMISES WITH MASS RESIDENCE OF CITIZENS

Gladkikh Anton Valentinovich
assistant
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article deals with problematic issues arising in the study of combating terrorism and extremism on the Internet. In particular, the features of the development of digital technology, the development of legislation at the domestic and international level are considered. The ways of solving the established problems are proposed.

Keywords: *world development, terrorism, the Internet, modern features, information technology, counteraction, video surveillance systems D-Dos attacks*.

В современных условиях, когда терроризм как явление, перестал признавать какие-либо границы, в том числе и государственные, возрастает необходимость детального рассмотрения аспектов деятельности министерств, ведомств, а также частных организаций, в эксплуатации которых находятся объекты стратегического назначения и помещения с массовым пребыванием граждан.

Одним из основных направлений в оперативном предотвращении, раскрытии и расследовании такого вида преступлений, является идентификация личностей, входящих в состав преступной группировки, целью которой является организация, планирование и осуществление террористического акта. Проблема идентификации личности всегда была обусловлена многосторонностью объекта исследования – ведь человека индивидуализируют не только черты лица, особенности строения отдельных частей тела, предметы одежды, обуви, украшения, но и определенные функциональные особенности организма, такие

как жестикуляция, походка, мимика, иные привычки, приобретенные им в процессе определенной деятельности [1].

Память свидетеля происшествия, находящегося под воздействием внешних факторов, не способна объективно отобразить совокупность признаков, присущих определенному человеку или группе лиц так, как это под силу беспристрастному электронному «глазу» системы видеонаблюдения.

Надежность и безотказность работы систем видеонаблюдения на объектах стратегического назначения и помещениях с массовым пребыванием граждан сложно переоценить, в том числе и в случаях, когда террористический акт на объекте был допущен, а лица, участвующие в его организации, не идентифицированы, и как правило, благополучно скрылись с места преступления.

Ярким примером того, какое значение имеет информация видеонаблюдения в раскрытии и расследовании такого рода преступлений являлась серия террористических актов в декабре 2013 года произошедшая в Волгограде.

Мощный взрыв, прогремевший в вестибюле здания железнодорожного вокзала, перед пунктом досмотра багажа, унес жизни 18 человек. Перед правоохранительными структурами стояла задача: в максимально-короткие сроки определить организаторов и заказчика террористического акта. Камера видеонаблюдения, контролировавшая вестибюль, зафиксировала момент взрыва, однако, месторасположение камеры и технические характеристики самой камеры не позволили получить изображение, достаточное для идентификации террориста-смертника. Свидетели, которые находились рядом с террористом и могли его разглядеть, либо погибли, либо получили очень тяжелые ранения. Учитывая, что террорист-смертник, как правило, не работает в одиночку, были исследованы материалы со всех имеющихся камер видеонаблюдения на объекте.

В ходе обработки данных записи с камер наружного видеонаблюдения следователи обратили внимание на неестественный жест молодого человека, который правой рукой полез в левый карман своей куртки. При дальнейшем анализе видеозаписи было установлено что подозреваемый, перед тем как войти в здание вокзала, оглянулся и посмотрел в сторону одиноко стоящего мужчины с дорожной сумкой, который тут же начал движение к главному входу вокзала, вскоре после чего и произошел взрыв.

Полученная информация с камер видеонаблюдения, в совокупности со свидетельскими показаниями, позволила идентифицировать личность участвовавшего лица и оказала неоценимую помощь следствию в оперативном задержании членов преступной группировки и предотвращению иных, запланированных террористических актов [2].

Несмотря на то, что руководители объектов стратегического назначения, а также помещений с массовым пребыванием граждан, как правило, устанавливают определенные системы видеонаблюдения, в организации таких систем отсутствует профессиональный подход как в подборе камер видеонаблюдения с необходимыми техническими характеристиками, так и в тактическом размещении камер, определении оптимальной высоты установки, ракурса съемки и т. д.

Монтаж оборудования, как правило, осуществляется организациями или частными лицами, не имеющим представления о тактике закрытия дислокации объекта. Качество и количество камер видеонаблюдения определяет заказчик, исходя из финансовых возможностей, эстетических потребностей, наличием персонала для обработки видеоинформации и т. д. Ракурсы съемки камер видеонаблюдения зачастую ориентированы на контроль осуществления трудовой

деятельности сотрудников учреждений, а не ключевых сегментов помещения, путей подхода или отхода к объекту.

Серьезным удешевлением стоимости монтажа систем видеонаблюдения послужила доступность и удобство в эксплуатации систем, использующих принцип беспроводной передачи данных по радиоканалу (Wi-fi, GPRS и т. д.) на базе IP-видеокамер. Несмотря на то, что подобные системы удобны в эксплуатации, а также позволяют удаленный доступ к управлению и получению информации, подобная организация системы передачи данных уязвима от внешних воздействий кибер-преступников, которые могут входить в состав террористической группы. Радио-прозрачность помещений позволяет лицам, обладающим специальными знаниями, сканировать диапазоны излучения видеокамер с целью определения рабочего адресного пространства камер видеонаблюдения и видеосервера за территорией объекта, не попадая в зону контроля камер видеонаблюдения. На момент совершения террористического акта, сведения о рабочей адресации видеосистемы позволят совершить узкополосную D-Dos атаку, целью которой будет являться отказ работы системы видеонаблюдения, и как следствие, существенно усложнить работу правоохранительных органов по идентификации личностей участников террористической группы.

Исходя из изложенного, а также с целью защиты объектов стратегического назначения и помещений с массовым пребыванием граждан от террористических посягательств предлагаем:

1. Правительству РФ поручить разработку перечня объектов, имеющих стратегическое значение, а также помещений с массовым пребыванием граждан, обязательных для оборудования специализированными системами видеонаблюдения.

2. Обязать Ростехнадзор:

2.1. Разработать проекты систем видеонаблюдения, с учетом категории объекта, технических характеристик аппаратуры и тактики закрытия дислокации объекта, в соответствии с параметрами, обеспечивающими надежную защиту данных систем от внешнего воздействия третьих лиц;

2.2. Осуществлять контроль за выдачей специальных лицензий организациям, имеющих право производства монтажа систем видеонаблюдения на объектах стратегического назначения и помещений с массовым пребыванием граждан.

3. Законодательно обязать министерства, ведомства и частных лиц, в эксплуатации которых находятся объекты стратегического назначения и помещения с массовым пребыванием граждан, в строго установленные сроки оборудовать объекты специализированными системами видеонаблюдения, исключительно с участием монтажных организаций, которым выдана специальная лицензия.

Библиографический список

1. Габричидзе, Т. Г. Основы комплексной многоступенчатой системы безопасности критически важных (потенциально) опасных объектов муниципального и регионального уровней: монография / Т. Г. Габричидзе. – Самара: СамНЦ РАН, 2012. – 392 с.

2. Габричидзе, Т. Г. Кризис предупреждения чрезвычайных ситуаций и пути его преодоления / Т. Г. Габричидзе. – Самара: СамНЦ РАН, 2015. – 264 с.

УДК 343.1

ИСПОЛЬЗОВАНИЕ ВИДЕО-КОНФЕРЕНЦ СВЯЗИ (ВКС) В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Гладких Дарья Николаевна
ассистент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается проблемных моментов, возникающих при исследовании использования средств видеоконференцсвязи в ходе судебного заседания. В частности, рассматриваются особенности развития цифровой техники, преимущество использования данного метода. Предложены пути решения установленных проблем.

Ключевые слова: *современные особенности, информационно-коммуникационные технологии, судебное заседание, участники процесса, уголовный процесс, ход процесса, цифровизация.*

USE OF VIDEO CONFERENCES OF COMMUNICATION (VKS) IN CRIMINAL LEGAL PROCEEDINGS

Gladkikh Daria Nikolaevna
assistant
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article deals with the problematic issues arising from the study of the use of audio recording during a court session. In particular, the development features of digital technology, the advantage of using this method are considered. The ways of solving the established problems are proposed.

Key words: *modern features, information and communication technologies, court session, participants in the process, criminal process, progress of the process, digitalization.*

Видеоконференцсвязь – это вид технологии, который позволяет производить передачу данных, таких как аудио и видео, а также текстовых сообщений в режиме реального времени.

Исходя из данного определения можно сделать вывод, что видеоконференцсвязь позволяет заменить реальное общение с живым человеком или группой лиц на виртуальное с сохранением всех необходимых параметров таких как необходимость видеть и слышать собеседника.

В связи с быстрым развитием современных технологий как в сфере вычислительной техники (компьютеры, планшеты, смартфоны и т. д.) так и в сфере передачи данных в них входит увеличение оптоволоконных сетей и повышение качества мобильного Интернета. Данные технологии становятся повсе-

дневными что ведет к их удешевлению и доступности как для населения, так и для различных структур в том числе и государственных [1].

Стоит отметить положительные стороны использования видеоконференцсвязи такие как:

1. Уменьшение затрат различных ресурсов в том числе и финансовых связанных с конвоированием обвиняемого и осужденного в зал судебного заседания

2. Обеспечение безопасности участников уголовного процесса, ведь свидетель больше не подвергается давлению.

3. Сокращение сроков рассмотрения уголовных дел.

Согласно статистике, по официальным данным ежегодно проводится более 800 сеансов связи более чем в 160 000 судебных процессов в год. Исходя из данной статистике можно сделать вывод, что данная система будет развиваться и модернизироваться. Это также подтверждает постановление правительства № 1406 «О федеральной целевой программе» Развитие судебной системы России на 2013–2020 годы». Согласно данной программе, предполагается:

- Создать мобильные передвижные офисы судей с применением видеоконференцсвязи, которые позволяют проводить выездные заседания в отдаленных населенных пунктах. Таким образом будет реализовываться доступность и открытость правосудия.
- Оснастить 95 % федеральных судов общей юрисдикции комплектами видеоконференцсвязи.
- Создать систему телефонии и видеоконференцсвязи, на базе телекоммуникационных систем и объединить все 2,6 тыс. объектов территориальных округов.

Несмотря на это, практический потенциал видеоконференцсвязи используется не в полной мере в связи с недостаточной практикой применения данных систем [2]. При реализации данных программ получится реализовать важные цели, такие как:

- создание необходимых условий для осуществления правосудия;
- обеспечение независимости судебной власти;
- повышение эффективности исполнительного производства;
- обеспечение открытости и доступности правосудия.

Устранение пробелов в реализации данной технологии способствует осуществлению уголовного судопроизводства в соответствии с поставленными целями.

Библиографический список

1. Лейба, А. Видеоконференцсвязь: недостатки и неполадки / А. Лейба // ЭЖ-Юрист. – 2013. – № 27.

2. Селина, Е. В. Проблемы использования средств видеоконференц связи в уголовном судопроизводстве / Е. В. Селина // Администратор суда. – 2015. – № 4. – С. 31–34.

УДК 343.1

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ АУДИОЗАПИСИ В ХОДЕ СУДЕБНОГО ЗАСЕДАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ

Гладких Дарья Николаевна
ассистент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается проблемных моментов, возникающих при исследовании использования средств аудиозаписи в ходе судебного заседания. В частности, рассматриваются особенности развития цифровой техники, преимущество использования данного метода. Предложены пути решения установленных проблем.

Ключевые слова: *современные особенности, информационно-коммуникационные технологии, судебное заседание, участники процесса, уголовный процесс, ход процесса, цифровизация.*

MODERN FEATURES OF THE COUNTER-TERRORISM AND EXTREMISM ON THE INTERNET

Gladkikh Daria Nikolaevna
assistant
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article deals with the problematic issues arising from the study of the use of audio recording during a court session. In particular, the development features of digital technology, the advantage of using this method are considered. The ways of solving the established problems are proposed.

Keywords: *modern features, information and communication technologies, court session, participants in the process, criminal process, progress of the process, digitalization.*

На данном этапе развития общества хорошо заметен большой рост развития технологий, а в частности информационно-коммуникационных технологий.

Эти изменения не обошли и судебную систему. Примером может стать использование современных технологий судом, таких как заполнение различных форм на сайте суда, получение различного вида информации такой как: графикам рассмотрения судебных дел, информация по делам находящимся в производстве и т. д. Также стоит отметить возможность использования видеоконференцсвязи для отдаленного участия в судебном заседании, что в свою очередь значительно упростило решение различных затруднительных ситуаций, касающихся личного присутствия участников процесса, в том числе по-

зволяет экономить огромные средства, связанные с перевозкой участников.

Отдельное внимание стоит уделить использованию современных технологий при производстве протоколирования судебного заседания согласно статье 259 УПК РФ. В коде каждого судебного заседание ведётся обязательное протоколирование протокол должен быть изготовлен и подписан в течение трех суток что в свою очередь создает конкретные временные рамки. При большом количестве заседаний у секретаря судебного заседания возникает усталость, которая ведет к неблагоприятным последствиям.

Частично данную проблему помогают решить технические средства такие как ведение аудио или видео записи заседания в последующем при необходимости секретарь судебного заседания сможет обратиться к записи для дополнения протокола необходимой информацией. Применение таких средств является важным шагом для развития системы протоколирования.

Не смотря на быстрые темпы внедрения технологий остается актуальной проблема оснащения необходимыми техническими средствами суды для осуществления воспроизведения и аудио записи судебного заседания.

В целом применение средств аудио записи при протоколировании судебного заседания является весьма успешным направлением развития системы судопроизводства. Есть полная уверенность в том, что данные средства найдут применение и в других областях правореализационного процесса такие как предварительное расследование, исполнительное производство, мировые, третейские и суды общей юрисдикции [1].

Следует также отметить, что в ходе процесса участники бывают весьма эмоциональны, и секретарь вынужден вносить правки в протокол, тем самым внося долю субъективности.

Таким образом, следует отметить важные преимущества ведения аудиозаписи заседания:

1) максимально информационные протоколы, исключающие ошибки и различного вида толкования;

2) обеспечение принципа гласности и открытости, а также доступности правосудия (станет намного проще выявить ошибки как судьи, так и других участников процесса);

3) дисциплинирует всех участников процесса, находящихся в зале.

Подводя итоги, можно отметить, что использование средств аудио записи позволит обеспечивать качество и эффективность протоколирования судебного заседания. А это положительно скажется на защите прав и законных интересов физических и юридических лиц.

Библиографический список

1. Макарцев, А.В. Применение аудиопротоколирования в ходе судебного заседания / А.В. Макарцев, М.М. Колесникова // Электронный журнал Четвертого арбитражного апелляционного суда. – 2012. – № 3. – С. 53.

УДК 343.1

ПЕРСПЕКТИВЫ СИСТЕМЫ ЭЛЕКТРОННЫХ УГОЛОВНЫХ ДЕЛ В РОССИИ

Далгалы Татьяна Александровна
кандидат юридических наук
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается вопроса создания и внедрения системы электронных уголовных дел в России. Автором рассматриваются ключевые аспекты данного процесса. Особое внимание в статье уделяется анализу опыта зарубежных стран в использовании системы электронных уголовных дел. Автор делает вывод о том, что в России на сегодняшний день созданы все условия для внедрения указанной системы электронных уголовных дел.

Ключевые слова: *электронное уголовное дело, цифровизация, цифровые технологии, уголовное судопроизводство, система электронных уголовных дел.*

PROSPECTS FOR THE SYSTEM OF ELECTRONIC CRIMINAL CASES IN RUSSIA

Dalgaly Tat`yana Aleksandrovna
candidate of law
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article addresses the issue of creating and implementing an electronic criminal case system in Russia. The author considers key aspects of this process. Particular attention in the article is paid to the analysis of the experience of foreign countries in using the system of electronic corner cases. The author concludes that in Russia today all the conditions have been created for the introduction of this system of electronic criminal cases.

Keywords: *electronic criminal case, digitalization, digital technology, criminal proceedings, system of electronic criminal cases.*

В современных условиях цифровизации всех сфер жизни общества в целом и правовой сферы в частности неизбежно возникает вопрос о необходимости внедрения новых передовых электронных технологий в уголовном судопроизводстве. На первом этапе была создана достаточно эффективная система электронного документооборота в уголовном процессе, созданы шаблоны процессуальных документов, ведется статистический учет регистрации уголовных

дел и так далее. Кульминацией работы системы электронного документооборота является создание системы электронных уголовных дел. В последнее время в научной литературе авторы все чаще стали рассматривать вопрос создания данной системы и прогнозировать эффективность ее внедрения.

Сравнительно-правовой анализ законодательного регулирования системы электронных уголовных дел, действующей во многих странах, позволяет сделать вывод о необходимости теоретического осмысления и отечественной наукой. Опыт государств, в которых создана система электронных уголовных дел, является ярким примером успешного взаимодействия теоретических разработок и требований правоприменительной практики в сфере уголовного судопроизводства. В некоторых государствах данная система действует уже больше десяти лет, как например, в Бельгии, США, Саудовской Аравии. Вместе с тем, в последние несколько лет все большее количество государств присоединяются к данному процессу и создают систему электронных уголовных дел. К последним можно отнести Украину, Казахстан, Чехию и другие [1, с. 15]. В Российской Федерации к вопросу создания и внедрения системы электронных уголовных дел подходят крайне осторожно, и прежде всего это связано с необходимостью эффективной защиты информационной безопасности. Действительно, информация, которая содержится в процессуальных документах, обладает особым статусом и подлежит особой защите законом. Неустойчивость электронных систем документооборота может привести к серьезным нарушениям прав, свобод и законных интересов всех участников уголовного судопроизводства. Именно поэтому необходимо создать эффективную защиту информационной безопасности указанной системы.

В Саудовской Аравии после создания системы электронных уголовных дел сроки рассмотрения большинства уголовных дел сократились до 2 дней. В целом на 80 % сократились сроки уголовного судопроизводства. В таких странах как Грузия, Эстония, Южная Корея, Бельгия, Чехия и других опыт использования системы электронных уголовных дел также является очень успешным [3, с. 42].

Что представляет собой система электронных уголовных дел? Это платформа, с помощью которой можно загружать и осуществлять выгрузку процессуальных документов, вносить соответствующие изменения, осуществлять контроль за деятельность органов дознания и следствия, и даже оценивать эффективность. К материалам электронного уголовного дела участники получают доступ с помощью индивидуального электронного паспорта, ключа, причем каждому может быть предоставлен доступ разного уровня с соответствующими ограничениями в диапазоне разрешенных действий.

Несмотря на все преимущества системы электронных уголовных дел, так как сокращение сроков рассмотрения уголовных дел, эффективность межведомственного взаимодействия и других, можно выделить несколько задач, ко-

торые необходимо решить на пути создания и внедрения указанной системы в России. К ним можно отнести следующие:

1) законодательное закрепление возможности использования электронных уголовных дел;

2) определение субъектов, которые будут формировать электронные уголовные дела;

3) определить способы и каналы передачи электронных уголовных дел заинтересованным лицам;

4) создать систему информационной безопасности электронных уголовных дел и другие.

Таким образом, в настоящее время в России существуют все предпосылки для создания и внедрения системы электронных уголовных дел в деятельность органов расследования преступлений системы МВД России [2]. Вместе с тем этот процесс должен быть поэтапным, целостным системным.

Библиографический список

1. Абдулвалиев, А. Ф. Опять про электронное уголовное дело / А. Ф. Абдулвалиев // Право и политика. – 2013. – № 1. – С. 15–18.

2. Об утверждении Программы МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел»: приказ МВД России от 14 декабря 2004 года № 896 // СПС Консультант Плюс. – URL: http://www.consultant.ru.

3. Познанский, Ю. Н. Электронное уголовное дело в решении проблемы расследования уголовных дел в разумные сроки / Ю. Н. Познанский // Труды Академии управления МВД России. – 2015. – № 1. – С. 41–44.

УДК 343.14

К ВОПРОСУ ОБ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВАХ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Далгалы Татьяна Александровна
кандидат юридических наук
Красноярский государственный аграрный университет, Красноярск, Россия

Статья рассматривает вопрос об электронных доказательствах и допустимости их использования в уголовном судопроизводстве. Автор анализирует определение понятия «электронные доказательства», основные проблемы в определении его содержания. Действительно, проблема допустимости использования электронных доказательств в уголовном судопроизводстве в современном мире является одной из самых актуальных. Прежде всего это связано с тем, что сегодня почти все суды сталкиваются с вопросом о допустимости электронных доказательств, представленных в уголовном процессе. В статье автор делает вывод о том, что именно поэтому необходимо всецело направить теоретические и практические усилия на продвижение передовых знаний, обмена опытом и лучшими практиками. Это значительно улучшит межведомственное и трансграничное сотрудничество между органами власти государств.

Ключевые слова: *электронное доказательство, уголовное судопроизводство, компьютерная информация, цифровые технологии, нематериальные доказательства.*

ON THE ISSUE OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Dalgaly Tat`yana Aleksandrovna
candidate of law
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

The article considers the issue of electronic evidence and the admissibility of their use in criminal proceedings. The author analyzes the definition of "electronic evidence", the main problems in determining its content. Indeed, the problem of the permissibility of using electronic evidence in criminal proceedings in the modern world is one of the most relevant. First of all, this is due to the fact that today almost all courts are faced with the question of the admissibility of electronic evidence presented in criminal proceedings. In the article, the author concludes that this is why it is necessary to completely devote theoretical and practical efforts to the promotion of advanced knowledge, the exchange of experience and best practices. This will significantly improve interdepartmental and cross-border cooperation between state authorities.

Keywords: *electronic evidence, criminal proceedings, computer information, digital technology, intangible evidence.*

Проблема допустимости использования электронных доказательств в уголовном судопроизводстве в современном мире является одной из самых актуальных. Сегодня почти все суды сталкиваются с вопросом о допустимости электронных доказательств, представленных в уголовном процессе. Правила, регулирующие допустимость электронных доказательств, различаются в правовых рамках различных государств-членов и постоянно подвергаются сомнению в связи с развитием технологических устройств, таких как компьютеры, мобильные телефоны, принтеры и цифровые камеры. Все эти устройства создают много возможностей для совершения преступлений, таких как кражи личных данных, детской порнографии в интернете, интернет-мошенничество и другие.

При рассмотрении доказательственного значения электронной информации необходимо учитывать, что им являются не физические свойства материального носителя компьютерной информации, его состав, внешний вид, как это наличествует у вещественных доказательств, а содержание данной информации.

В научной литературе даже используется такой термин как «виртуальный след». В.А. Мещеряков определил его как «… любое изменение состояния автоматизированной информационной системы (образованного ею «кибернитического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (то есть информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле» [1, с. 104]. Кроме того, им введен термин «электро-цифровой объект». Под ним понимается «помеченная система дискетных электронных сигналов, предназначенная для обозначения (по установленной системе кодирования) какой-либо информации и представленная в форме, пригодной для ее автоматизированной обработки, хранения и передачи с использованием средств вычислительной техники (компьютеров)» [2, с. 163].

Согласно общему пониманию, термин «электронные доказательства» относится к любому представлению фактов, информации или концепций в форме, подходящей для обработки в компьютерной системе. Эти данные играют важную роль, например, там, где злоумышленники общаются в электронном виде или когда простое владение электронным устройством может предоставить данные о местонахождении лица. Кроме того, в течение последних нескольких лет наблюдается, что электронные данные актуальны не только в контексте классических кибер-преступлений, таких как хакерские атаки, но также в контексте традиционных преступлений, таких как мошенничество или сексуальные надругательства над детьми, которые все чаще и чаще совершаются через Интернет. Кроме того, быстро расширяется использование электронных устройств, например, в служебных и личных целях, для мобильной связи или в Интернете вещей, где устройства обмениваются информацией напрямую через Интернет, что привело к феномену больших данных – большие объемы информации хранятся в электронном виде и потенциально могут быть использованы в качестве доказательств.

Электронные данные для использования в качестве доказательств в уголовном расследовании могут быть получены от жертвы, подозреваемого или любой третьей стороны, которая, в большинстве случаев, является поставщиком услуг, чьи услуги связаны с созданием, передачей и / или хранением данных. Правоохранительные органы могут получать данные с помощью открытых или скрытых мер: домашний обыск, включая изъятие электронных устройств, таких как мобильный телефон или ноутбук, является примером мер от-

крытого расследования, в то время как перехват мобильной связи обычно проводится скрытно.

Поскольку электронные данные нематериальны – они представляют собой не что иное, как обрабатываемую последовательность нулей и единиц – они показывают характеристики, которые несопоставимы с характеристиками других вещественных материальных доказательств. В отличие от физических вещей, передача электронных данных обычно не подразумевать потерю контроля; напротив, владелец данных обычно сохраняет исходный набор данных и передает только его копию – либо в электронном виде, на устройстве хранения данных, либо в виде распечатки на бумаге. С технической точки зрения к электронным данным обычно можно получить доступ (и, следовательно, получить их) из любой точки мира, если они доступны через Интернет. Что касается сбора электронных данных, время является решающим фактором не только потому, что эти доказательства могут передаваться буквально со скоростью, близкой к скорости света, но также и потому, что такая передача может осуществляться независимо от каких-либо государственных границ. Наконец, что не менее важно, по сравнению с физическими вещами, гораздо проще создавать и обрабатывать электронные данные анонимно; следы в виртуальном киберпространстве можно скрыть гораздо лучше. Как только правоохранительные органы получили электронные данные, которые являются потенциальными доказательствами, их обычно необходимо преобразовать в совместимый, читаемый формат для дальнейшей обработки. Это подразумевает риск преднамеренного, непреднамеренного и даже незамеченного манипулирования исходной информацией.

В сложившихся современных условиях глобальной цифровизации в различных сферах жизни общества в целом, и в уголовном судопроизводстве в частности, необходимо всецело направить теоретические и практические усилия на продвижение передовых знаний, обмена опытом и лучшими практиками между судьями, прокурорами и частными юристами из государств, которые занимаются уголовным судопроизводством, где используются электронные доказательства. Это значительно улучшит знания, умения и навыки других государств о стратегиях и методах, используемых в различных странах, и в конечном итоге улучшит трансграничное сотрудничество между органами власти государств.

Библиографический список

1. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – 408 с.

2. Мещеряков, В. А. Электронные цифровые объекты в уголовном процессе и криминалистике / В. А. Мещеряков // Воронежские криминалистические чтения: сб. науч. тр. – Воронеж, 2004. – Вып. 5. – С. 153–169.

УДК 344.983.22

К ВОПРОСУ ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННЫХ БАЛЛИСТИЧЕСКИХ ИДЕНТИФИКАЦИОННЫХ СИСТЕМ ПРИ ИССЛЕДОВАНИИ ОГНЕСТРЕЛЬНОГО ОРУЖИЯ

Ерахтина Елена Александровна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет

Данная статья посвящена вопросу применения автоматизированных баллистических идентификационных систем, вопросам нового методологического подхода к данного вида исследованиям.

***Ключевые слова**: криминалистическая техника, судебная баллистика, идентификационные исследования, цифровые изображения, методический подход.*

TO THE QUESTION OF APPLICATION OF AUTOMATED BALLISTIC IDENTIFICATION SYSTEMS IN THE STUDY OF FIRE-SHOT WEAPONS

Erakhtina Elena Alexandrovna
candidate of law, associate Professor
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article is devoted to the issue of using automated ballistic identification systems, issues of a new methodological approach to this type of research.

***Keywords:** forensic technology, forensic ballistics, identification studies, digital images, methodological approach.*

Постоянный рост преступлений, совершаемых с применением огнестрельного оружия, представляет огромную опасность в условиях достаточно сложной криминальной обстановки в стране.

За 2019 г. анализ современного состояния преступности подтверждает, что в целом по стане зарегистрировано 26 557 преступлений с применением огнестрельного оружия, в том числе в Красноярском крае – 720. Из данного анализа можно сделать вывод, что в настоящее время большую значимость для расследования имеют судебно-баллистические исследования.

Сегодня судебная баллистика переживает новый рассвет с введением автоматизации в данного рода исследования.

Автоматизация баллистических исследований требует от специалистов перехода от традиционных методических взглядов на более высокий уровень. Глубокая проработка требуется именно идентификационным судебно-баллистическим исследованиям. Стремительное развитие цифровых технологий, применение экспертом различного оборудования не привели к унификации

выявления идентификационных признаков, оставив традиционные методы сравнения и анализа выявленных совпадений или различий, поставив результаты экспертиз в прямую зависимость от наличия соответствующих знаний и личного опыта конкретного эксперта.

В описанных условиях, назрела необходимость в переходе на следующий методологический уровень, который основан на применении цифровых технологий и методов анализа информации с помощью искусственного интеллекта. Допотопный метод обработки и анализа информации при решении идентификационных задач в судебно-баллистической экспертизе в своей перспективе полностью должен быть вытеснен автоматизацией данного процесса.

Отметим, что процесс автоматизации идентификационных судебно-баллистических систем уже запущен: в нашей стране («ТАИС», «Кондор», «Поиск», «Арсенал») и за рубежом (IBIS Forensic Technology) уже имеется ряд автоматизированных баллистических идентификационных систем.

Посредством указанных выше систем можно получать цифровые изображения поверхности пули, поверхностей дна и корпуса гильзы; определять положения следов холостой и боевой граней нарезов; выделить на пуле первичные следы, следы полей нарезов; выделить следы бойка и патронного упора на дне гильзы; выделить на гильзе следов отражателя, досылателя, зацепа выбрасывателя, окна ствольной коробки или кожух-затвора, загиба магазина и т.д.

Отечественные автоматизированные баллистические идентификационные системы способствуют ведению раздела «криминальных объектов» (пули и гильзы, изъятые с мест преступлений) и раздела «регистрируемых объектов» (пули и гильзы, полученных в результате контрольного отстрела оружия, стоящего на учете в органах внутренних дел, когда известны: владелец оружия, его модель, калибр и номер).

Программное обеспечение автоматизированной системы осуществляет поиск по базе данных в автоматическом режиме и, последующую идентификацию изображений объектов.

Эксперту по окончании поиска предлагается ранжированный список объектов для последующего принятия решения о том, присутствует ли в базе данный объект, выстреленный в том же экземпляре оружия, что и исследуемый объект.

Основной принцип действия автоматизированной баллистической идентификационной системы следующий.

Сначала поверхность исследуемого объекта (часть пули или гильзы), подсвеченная источником света, генерирующим световые волны заданной длины, сканируется оптическим сканером.

При этом сканер размещается под углом к поверхности объекта и микрорельеф следов на получаемом изображении проявляется посредством изменения именно интенсивности освещения, которое переводится в пиксели различной яркости и отображается в двоичном коде на матрице.

Оптический сканер, являясь универсальным, позволяет работать также с фрагментами оболочек пули гильз и с деформированными пулями. Разрешаю-

щая способность оптических сканеров составляет 2,5-4 мкм. Система автоматически рассчитывает освещение, что позволяет снизить уровень пересвета на изображениях в целях избежания потерь идентификационной информации.

В итоге морфологическое строение следов преобразуется в структуру, которая передается в базу данных и используется уже для последующего сравнения.

Рис. 1. Фрагмент изображения боковой поверхности пули (АБИС «ТАИС»)

Несомненно, использование автоматизированных баллистических идентификационных систем обеспечивает большую информативность (оперирование огромным массивом данных) и в свою очередь уменьшает время обработки и принятия решения при производстве самого исследования.

В ЭКЦ ГУ МВД России по Красноярскому краю уже более десяти лет используется АБИС «ТАИС». Данная система успешно применяется для ведения баллистических учетов, а также используется при проведении баллистических экспертиз и исследований.

Данное направление перспективно для повышения характеристик автоматических сравнений и предоставления дополнительных возможностей визуального анализа.

Обобщая изложенное, можно сделать вывод, что судебная баллистика находится на пороге нового прорыва, который позволит решать аналитические вопросы судебно-баллистической идентификации, на новом уровне.

УДК 343.9.018

ЦИФРОВЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Ерахтина Елена Александровна
канд. юрид. наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья посвящена влиянию цифровых технологий на развитие криминалистики, поиск новых методов, обнаружения, сбора, фиксации и исследования цифровых доказательств.

Ключевые слова: *информационные и коммуникационные технологии, электронные устройства, сети, сеть Интернет, специализированные программно-аппаратные комплексы.*

DIGITAL TECHNOLOGIES IN CRIMINALISM

Erakhtina Elena Alexandrovna
candidate of law, associate Professor
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article is devoted to the influence of digital technologies on the development of forensic science, the search for new methods, the detection, collection, recording and research of digital evidence.

Keywords: *information and communication technologies, electronic devices, networks, Internet, specialized software and hardware systems.*

Цифровые технологии сегодня затронули даже традиционные разделы криминалистики. Отточенные годами знания и накопленный опыт о способах и методах расследования отдельных видов преступлений сегодня требуют существенной переработки с учётом развития электронной среды, в которой действует преступник.

Поиск следов преступления, при которых преступник и жертва преступления взаимодействуют посредством информационных и коммуникационных технологий через электронные устройства и сети, прежде всего через сеть Интернет, требует поиска новых методов, обнаружения, сбора, фиксации и исследования цифровых доказательств совершённого преступления.

Дело в том, что преступность в свою очередь также прошла модернизацию благодаря появлению электронно-цифровой среды, поэтому её влияние на экономику и, как неизбежно на социальную сферу, трудно оценить.

Размах преступности в информационно-коммуникационной среде трубно выразить в цифровом выражении (это не только проблемы информационной и общественной безопасности государства, но и экономическая преступность) в силу высокой латентности многих преступлений, а также правовой неграмотности и пассивности самих потерпевших.

Однако заметим, поскольку способы, инструменты совершения преступлений, а также оставляемые преступниками следы постоянно трансформируются, то и методы противодействия цифровой преступности развиваются.

Как известно, цифровые следы, с которыми работает специалист, следователь или эксперт легко уничтожить.

Сложность состоит и в том, что при исследовании цифровых доказательств человек не может воспринимать их непосредственно, через органы чувств, для этих целей необходимы сложные программные комплексы.

Рис. 1. Специализированный программно-аппаратный комплекс для извлечения и анализа информации из мобильных телефонов UFED Touch 2 Ultimate

Цифровая сфера дает преступнику возможность использовать новые способы и новые орудия (веб-сайт, электронная почта, электронные платёжные системы) совершения преступлений.

В противовес этому появляются новые способы раскрытия преступлений (разрабатываются новые тактики следственных действий и оперативно-розыскных мероприятий, создаются специальные аппаратные и программные инструменты для сбора и исследования доказательств в цифровой среде).

Примером может служить UFED Touch 2 Ultimate, который применяется для логического извлечения информации (извлекается только та информация, доступ к которой возможен без получения прав супер пользователя «root»); физического извлечения информации (наиболее полное, включает удаленную информацию) и захвата снимков экрана.

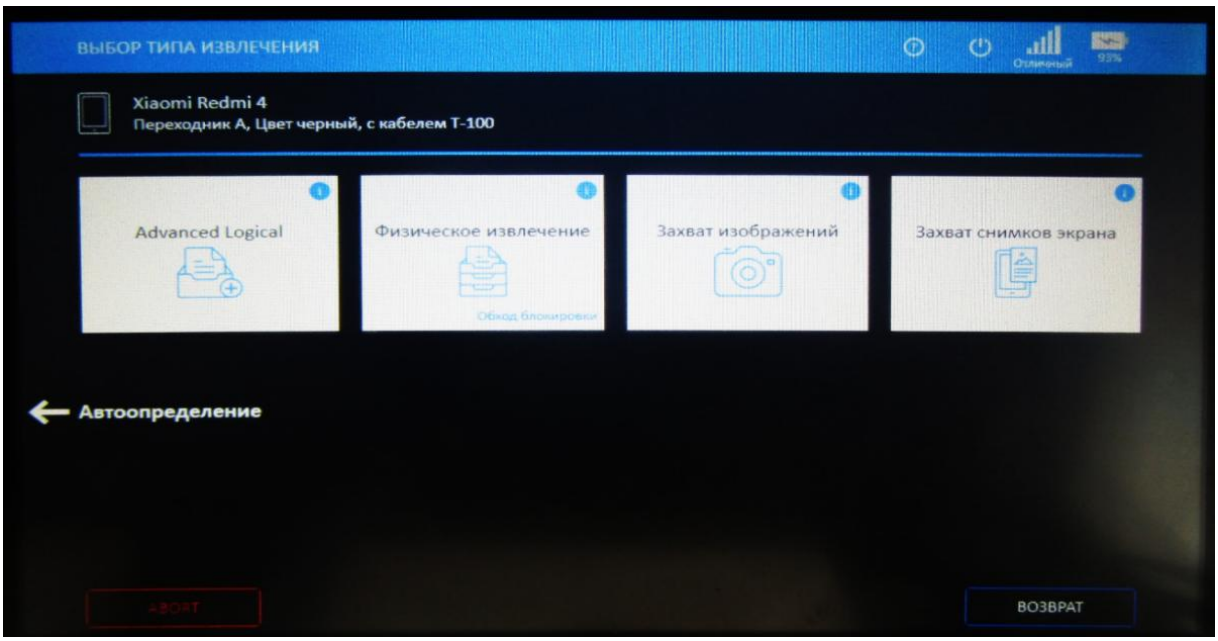

Рис. .2. Возможности UFED Touch 2 Ultimate

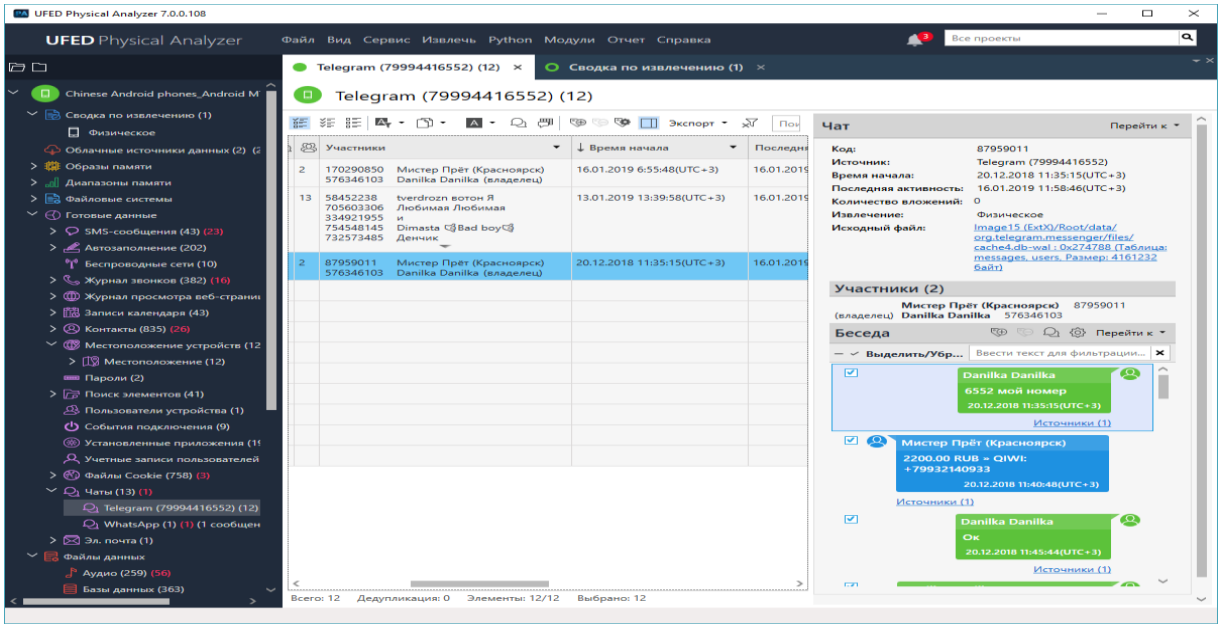

Рис. 3. Анализ извлеченной информации и формирование отчетов в UFED Physical Analyzer

Сегодня раскрытие и расследование преступлений, в которых фигурируют любые мобильные устройства, ПК, дроны, облачные сервисы, невозможно без внедрения комплексов для извлечения и анализа данных с указанных носителей цифровой информации.

В настоящее время активно внедрён и используется правоохранительными структурами программно-аппаратный комплекс «Мобильный Криминалист», который позволяет получить доступ к информации из десятков тысяч

мобильных устройств, SIM и SD-карт, а также поддерживает самое большое количество облачных сервисов и дает возможность получить к ним доступ с помощью учетных данных, найденных при изучении информации из мобильных устройств или ПК.

в

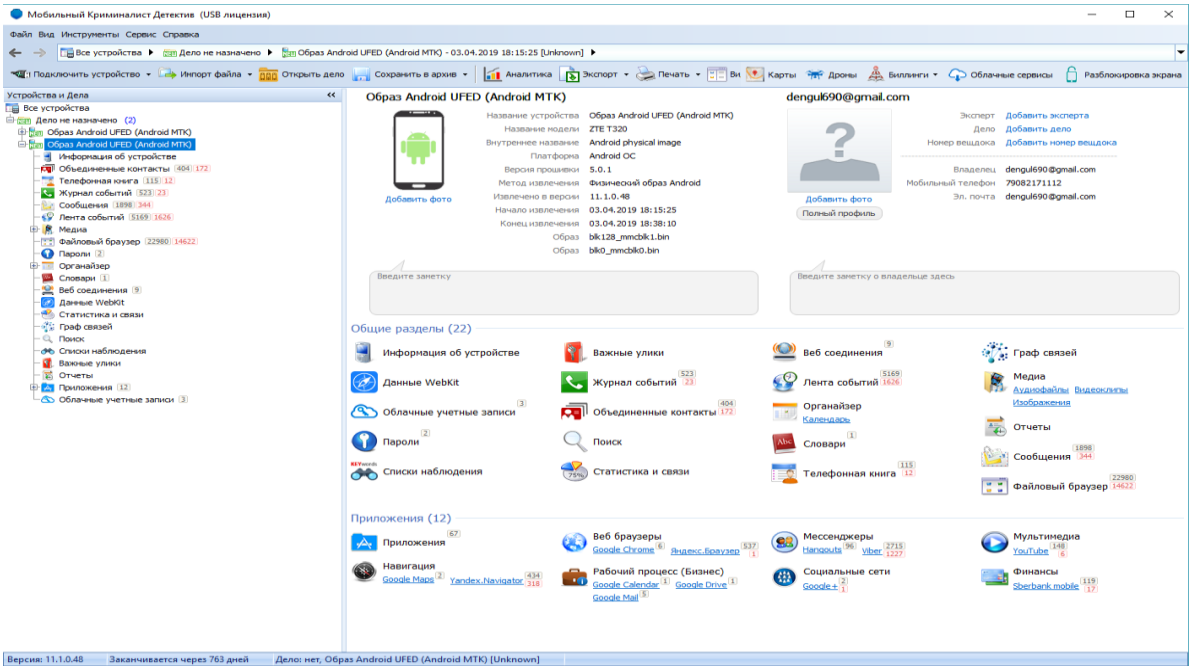

Рис. 4. Извлечение и анализ информации в Мобильный Криминалист Детектив

В случае если доступ к данным пользователя посредством штатного интерфейса невозможен, в ситуации, например, когда накопитель был намеренно поврежден преступником, на помощь правоохранительным структурам для получения цифровых доказательств приходит комплекс PC-3000 Flash.

Технология PC-3000 Flash позволяет: увеличить вероятность успешного восстановления данных даже в случае физически поврежденных накопителей; считывать информацию из микросхем Flash напрямую, минуя контроллер; считывать информацию с Flash накопителей в монолитном исполнении; применять комплекс различных мер для получения максимально возможного результата, включая изменение напряжения и read retry.

Комплекс PC-3000 Flash восстанавливает данные с USB накопителей, карт памяти, мобильных устройств хранения информации, используя при этом собственную технологию прямого доступа к микросхемам flash-памяти. При этом микросхема выпаивается из накопителя и считывается на специальном считывающем устройстве - Flash reader, входящим в состав комплекса, что позволяет получить доступ к данным даже в случаях, когда контроллер накопителя неисправен.

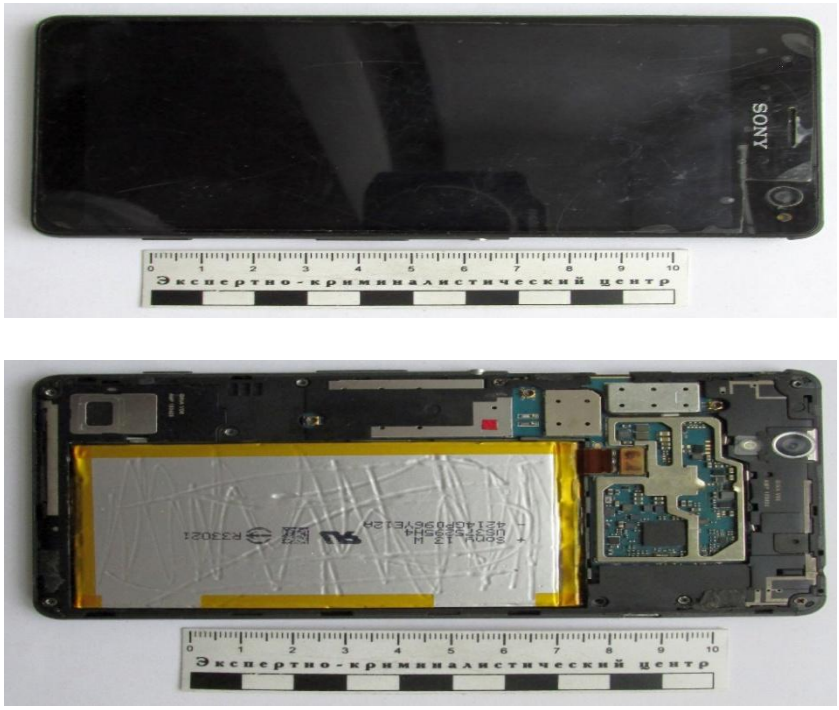

Рис. 5. Извлечение информации из памяти неисправного мобильного телефона «Sony EXPERIA»

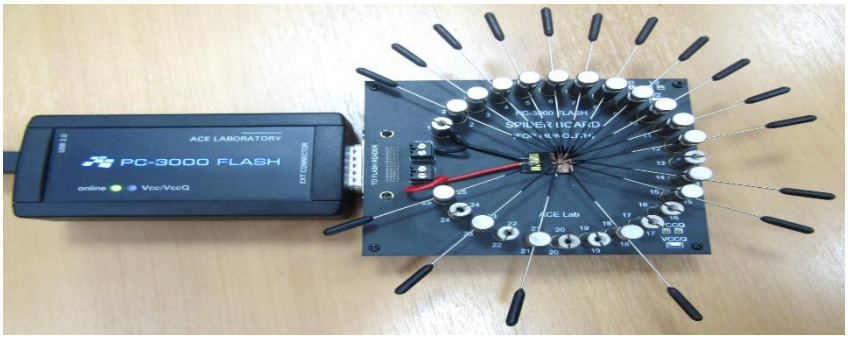

Рис. 6. Использование комплекса PC-3000 Flash для извлечения информации с неисправных Flash накопителей

Производители с каждым выпуском новых устройств стараются улучшить их защиту, оснастить аппаратным шифрованием, основанным на специальных аппаратных ключах, привязанных к устройству и т. д.

Мобильные комплексы в свою очередь также модифицируются, предлагают свои способы обхода разных усовершенствований программного обеспечения.

В заключение хотелось бы заметить, что кроме разработки и совершенствования криминалистической техники, правоохранительным структурам необходимо также вкладывать средства в подготовку новых ИТ-специалистов для соответствующих подразделений по противодействию преступности в цифровой сфере.

УДК 004;34

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ

Кальтенбергер Никита Александрович
Национальный исследовательский университет «МИЭТ», Москва, Россия

В статье изложено несколько инновационных технологий, которые уже сегодня помогают людям в решении некоторых юридических задач.

Ключевые слова: *инновационные технологии, программное, боты-юристы; Legal tech.*

INNOVATIVE TECHNOLOGIES IN LAW

Kaltenberger Nikita Alexandrovich
National Research University MIET, Moscow, Russia

The article describes several innovative technologies that already help people solve some legal problems.

Keywords: *Innovative technologies; software; legal bots; Legal tech.*

В нашем быстро меняющемся мире юристы всегда должны были широко мыслить, обладать обширными знаниями и уметь подстраиваться под все изменения, которые их каким-либо образом затрагивают. Сейчас юристу недостаточно отвечать на вопросы, который поставил клиент. Юрист должен иметь широкий спектр таких навыков как умение систематизировать, проводить алгоритмизацию, доносить и ставить задачи и работать в команде, иначе в скором времени его заменят так называемые «чат боты» или другие похожие программы.

Следует выделить «чат боты», которые уже сегодня способны заменить юриста, выполняющего несложные рутинные действия. Благодаря огромному количеству юридических документов, которые загрузили в бота разработчики, и сложных алгоритмов анализа этих документов, роботы-юристы способны распознать документ, провести его анализ и дать консультацию, либо составить по запросу заказчика определенный документ. Примерами таких роботов являются: «Docubot», «LawBot».

Docubot – это чат-бот, который помогает создавать юридические документы без встречи с адвокатом. Люди входят в систему, выбирают тип документа, отвечают на пару поставленных вопросов и Docubot генерирует документ.

LawBot – помогает проанализировать юридические контракты и документы. Все, что требуется, – отправить конкретный документ этому боту, и он предоставит обратную связь относительно всех юридических аспектов документа. Данный бот может объяснить, что означает каждая часть контракта и какие де-

тали отсутствуют. Благодаря этому боту не нужно будет вчитываться в множество страниц «технической» информации.

Вышеперечисленные чат боты работают только на английском языке, но в России, уже сейчас, есть отечественные аналоги, которые работают по схожим алгоритмам. Например, чат-бот от сайта «Правовед.ру» и чат-бот «Федор Нейронов».

Бот «Правовед.ру» способен ответить на поставленный вопрос, за считанные секунды, когда у юриста на это уйдёт несколько минут. Однако следует отметить, что сложные юридические кейсы такой бот не решает.

Федор Нейронов – бот, который подробно проконсультирует вас в семейном праве и по вопросам защиты прав потребителей, данная программа работает в формате «вопрос-ответ».

Но не стоит опасаться, что боты-роботы и аналоговые программы полностью заменят юристов, и возникнет проблема трудоустройства. Это не так, потому что в большинстве случаев чат-боты лишь выполняют рутинную задачу, которую юристы-профессионалы делать и не должны — это проверка документов, и ответы на типовые вопросы.

Высококвалифицированные юристы всегда будут востребованные, многие задачи алгоритму просто не выполнить. Это прекрасно понимают программисты и специально для таких юристов они разработали несколько сайтов и программ, которые в значительной степени облегчают работу юриста и позволяют выполнять поставленную задачу в несколько раз быстрее. Речь идет о таких программах как: аналитическая система «Сутяжник» и «Контур.Фокус».

«Сутяжник» – Российский автоматизированный сервис по подбору судебной практики на основе имеющихся у вас документов. Достаточно загрузить текст документа в программу, и он моментально найдет решения судов общей юрисдикции или арбитражных судов, которые наиболее близки проблематике, изложенной в документе.

Система «Контр.Фокус» – собирает из открытых источников информацию о компании (финансовое состояние, статус лицензии, связанные товарные знаки, информация о дочернюю компанию и многое другое), и позволяет юристу за несколько кликов узнать всю нужную информацию о контрагенте. Тем самым программа помогает с подготовкой к арбитражным делам.

Нельзя отрицать того факта, что инновации с каждым годом все больше и больше внедряются в нашу жизнь. Сейчас они вплотную подошли к юриспруденции, это осознают многие как ведущие адвокаты, так и учреждения, специализирующиеся на выпуске новых кадров, поэтому сейчас можно заметить множества новых направлений в подготовке и создание различного рода объединений, направленных на формирование высоких технологий в юриспруденции.

УДК 004; 343.1

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ

Кардашевская Марина Владимировна
доктор юридических наук, профессор
Московский университет МВД России имени В. Я. Кикотя, Москва, Россия

В статье обосновывается возможность и необходимость использования в процессе расследования неочевидных преступлений интеллектуальной системы комплексной обработки криминалистически значимой информации. Выделены научные основы данной системы, рассмотрено содержание ее элементов.

Ключевые слова. *Информационные технологии, раскрытие преступлений, криминалистически значимая информация, искусственный интеллект.*

POSSIBILITIES OF USING INFORMATION TECHNOLOGIES IN SOLVING CRIMES

Kardashewskaya Marina Vladimirovna
doctor of law, Professor
Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia

The article substantiates the possibility and necessity of using an intelligent system of complex processing of criminally significant information in the process of investigating non-obvious crimes. The scientific basis of this system is highlighted, and the content of its elements is considered.

Keywords. *Information technologies, crime detection, criminally significant information, artificial intelligence*.

Статистика МВД России за несколько последних лет свидетельствует, что в стране в среднем уровень раскрываемости по общеуголовным преступлениям составляет 38 %. При этом около 36 % преступлений раскрыты в первые сутки «по горячим следам», остальные 2 % приходятся на признательные показания задержанных о совершении ими ранее других преступлений.

Основной причиной столь низкой раскрываемости является тот факт, что уголовные дела, возбужденные по факту совершения преступления (а не в отношении конкретного лица), никем не расследуется. Если в советский период существовала специализация следователей по расследованию нераскрытых преступлений и работа такого следователя оценивалась по количеству преступлений, по которым им было предъявлено обвинение (после этого дело передавалось для дальнейшего расследования другому следователю), то в настоящее время такая специализация фактически отсутствует. Связано это, в первую очередь, с тем, что каждый следователь (дознаватель) должен закончить производ-

ство по уголовному делу, направив его в суд. В результате у каждого следователя (дознавателя) в производстве находятся уголовные дела, по которым виновные лица как установлены, так и не установлены. В ситуации ограниченных временных рамок расследования следователь (дознаватель) объективно не может эффективно работать по уголовным делам, возбужденным по факту преступления.

Считаем, что помощь в разрешении данной ситуации могла бы оказать интеллектуальная система комплексной обработки криминалистически значимой информации. Система должна включать в себя накопление, хранение, сопоставление, визуализация, поиск информации и формирование следственных гипотез (версий). Научными основами работы с криминалистически значимой информацией являются:

– криминалистическое учение о навыках преступника, в самом схематичном виде подразумевающее использование преступником тех приемов и средств, которые ранее уже применялись им при совершении преступления;

– теория криминалистической идентификации, т. е. способность лица отображаться в оставляемых им следах;

– диалектический закон перехода количества в качество, когда по мере накопления информации о лице, совершившим преступление, появляется информация о конкретной личности.

Рассмотрим более подробно элементы системы.

1. *Накопление*. При принятии к своему производству уголовного дела, возбужденного по факту совершения преступления, следователь (дознаватель) должны будут внести криминалистически значимые сведения в базу системы. К таким сведениям следует отнести: номер дела и территориальный орган, где проводиться расследование (чтобы можно было потом при необходимости это дело найти); известную информацию об элементах криминалистической характеристики преступлений (способ преступления, предмет преступного посягательства, обстановка преступления, личность потерпевшего и преступника). Причем эта информация должна быть максимально полной. Так, например, описывая место совершения квартирной кражи, должно быть указано: количество этажей в доме, степень защиты подъезда (домофон, консьерж, видеокамера), наличие лифта, этаж, на котором расположена квартира, из которой совершена кража, сколько квартир на этаже, степень охраны квартиры (глазок, количество дверей, замков). По мере поступления в ходе производства следственных действий новой информации, она также вносится в базу системы. Чем больше сведений будет в системе, тем она будет эффективнее. Естественно, что описание тех или иных признаков должно быть единообразным, что подразумевает наличие вариантов признаков в самой системе. Кроме того, в базу может быть загружено видеофайл, на котором изображен преступник, полученный с камер видеонаблюдения.

2. *Хранение*. Информация в системе должна храниться до установления лица, подлежащего привлечению в качестве обвиняемого по данному уголовному делу.

3. *Сопоставление*. Искусственный интеллект системы должен обнаружить совпадение признаков по различным уголовным делам и определить вероятность совершения нескольких преступлений одним лицом. Анализ должен проводиться не только по криминалистическим признакам криминалистической характеристики преступления, но и по результатам проведенных экспертиз, как идентификационных, так и диагностических. Система должна быть совмещена с технологией распознавания изображений для определения вероятности изображения на различных файлах одного и тоже лица. Не менее важным для эффективной работы системы является ее совмещение с технологией прогнозирования преступного поведения. Это подразумевает, что система, определив, что несколько преступлений с высокой долей вероятности совершены одним лицом, прогнозирует на основе имеющихся данных возможность совершения этим лицом нового преступления в определенном месте в определенное время.

4. *Визуализация* подразумевает возможность увидеть результат работы системы в виде графиков, схем и т. п., в том числе распечатать их.

5. *Поиск информации в системе*. При получении прогноза следователь должен будет найти информацию по другим уголовным делам для принятия необходимых процессуальных решений, например, о соединении производства по уголовным делам.

Система может использоваться по отдельным видам преступлений, прежде всего, по хищениям чужого имущества (кражи, грабежи, разбои), насильственным преступлениям, преступлениям, связанным с незаконным оборотом наркотических средств и психотропных веществ. Уровень информационной базы системы должен быть региональный, с подключением всех территориальных органов и следователей (дознавателей). На первоначальном этапе внедрения данной системы в практику правоохранительных органов, помимо текущих уголовных дел, информация должна быть загружена по нераскрытым преступлениям как минимум за последние 10 лет.

Представляется, что создание интеллектуальной системы комплексной обработки информации существенно повлияет на уровень раскрываемости преступлений.

УДК 343.72

ОСОБЕННОСТИ ОБЪЕКТА И ПРЕДМЕТА ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 159.6 УК РФ

Коновалова Елена Владимировна
старший преподаватель
ОУП ВО «Академия труда и социальных отношений», Москва, Россия

В статье рассматриваются положения ст. 159.6 УК РФ, основной и дополнительный объекты данного преступления. Анализируется их влияние на квалификацию преступления. Затронут вопрос о предмете мошенничества в сфере компьютерной информации.

Ключевые слова: *Мошенничество в сфере компьютерной информации, хищение, компьютерная информация, имущество, право на имущество.*

SPECIFICITIES OF OBJECT AND ITS SIGN PROVIDED FOR BY ARTICLE 159.6 OF THE RUSSIAN CRIMINAL CODE

Konovalova Elena Vladimirovna
senior lecturer
OUP VO «Academy of labor and social relations», Moscow, Russia

In the article it is viewing art.159.6 of Russian Criminal Code, the main and supplementary objects of this crime. Its significance is analyzing for qualification of the crime. The question about signs of fraud in computer information sphere is raised.

Keywords*: Fraud in computer information sphere, stealing, computer information, property, right to property.*

Мошенничество в сфере компьютерной информации – преступление, относительно недавно появившееся в Уголовном кодексе РФ, практика применения которого находится в процессе становления. Данный состав преступления в современном уголовном законе – это ответ на новые угрозы для разных видов общественных отношений.

Рассматриваемое в настоящей статье преступление является специальным видом мошенничества и предусмотрено в ст. 159.6 УК РФ. Согласно УК РФ мошенничество в сфере компьютерной информации – это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей. Основным непосредственным объектом рассматриваемого преступления считаются общественные отношения, направленные на защиту собственности. Однако они не являются единственными охраняемыми общественными отношениями в рамках ст. 159.6 УК РФ. Как видно из содержания статьи, в составе присутствует дополнительный непосредственный объект – общественные отношения, направленные на защиту компьютерной информации или по-другому, обеспечивающие безопасность компьютерной информации. На многообъектность рассматриваемого состава преступления обращается внимание в

научной литературе [1]. Признаком, характеризующим объект преступления, является предмет. В составе мошенничества в сфере компьютерной информации таким предметом являются альтернативно чужое имущество или приобретение права на чужое имущество.

Сложность структуры состава преступления порождает дискуссионные вопросы как в теории, так и на практике. Так, например, дополнительный непосредственный объект преступления, предусмотренного ст. 159.6 УК РФ – общественные отношения в сфере обеспечения безопасности компьютерной информации, для ряда статей является основным непосредственным объектом. Для защиты этого объекта преступления в УК РФ предусмотрены ст. 272, 273, 274, 274.1. Характерным признаком для данных составов является предмет преступления, которым является компьютерная информация. При решении вопроса о наличии или отсутствии совокупности преступлений, предусмотренных ст. 159.6 и статьями гл. 28 УК РФ, следует помнить о правилах квалификации преступлений по объекту. Так, «если при совершении преступления степень тяжести вреда, причиняемого дополнительному объекту, больше степени тяжести вреда, причиняемого основному объекту, требуется квалификация по совокупности преступлений» [2]. В судебной практике о мошенничестве в сфере компьютерной информации данный вопрос также решен в пользу совокупности преступлений. «Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ» [3].

Однако позиция законодателя относительно характера и степени общественной опасности преступления с двумя непосредственными объектами, предусмотренного ст. 159.6 УК РФ вызывает вопросы. Объект преступления показывает общественную опасность преступления: его ценность, а также количество данных объектов. Основной состав преступления, предусмотренный ст. 159.6 УК РФ, согласно действующему уголовному законодательству является менее опасным, чем основные составы преступлений, предусмотренные гл. 28 УК РФ, а также менее опасным, чем основной состав мошенничества, предусмотренный ст. 159 УК РФ. Представляется небезосновательной возможность повышения общественной опасности мошенничества в сфере компьютерной информации через усиление наказания, предусмотренного санкциями соответствующих частей ст. 159.6 УК РФ.

Правовая природа мошенничества в сфере компьютерной информации интересна также тем, что по-разному отражается в нормативных источниках. Так, по действующему уголовному российскому закону рассматриваемое преступление – это в первую очередь преступление против собственности. А если обратиться к рассмотрению аналогичного деяния, предусмотренного в международном уголовном праве, то оно закреплено как преступление в сфере компьютерной информации. В ст. 8 Конвенции о преступности в сфере компьютерной информации ETS N 185 от 23.11.2001 г. закреплено: «Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву – в случае совершения умышленно и неправомерно – лишения другого лица его собственности путем:

а: любого ввода, изменения, удаления или блокирования компьютерных данных;

b: любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица» [4].

На данный момент в российском уголовном законодательстве состав мошенничества в сфере компьютерной информации предусматривает в качестве основного непосредственного объекта только общественные отношения собственности. Однако наличие двух объектов в рассматриваемом преступлении все же должно находить отражение не только при законодательном формулировании признаков состава преступления, но и при определении видов и размеров наказаний за него.

Кроме рассмотренного выше вопроса об объекте мошенничества в сфере компьютерной информации, существуют также иные, связанные с предметом этого преступления. Компьютерная информация, как выше было рассмотрено, является предметом дополнительного объекта преступления – общественных отношений в сфере защиты компьютерной информации. Компьютерной является информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи [5]. Исходя из такого определения, компьютерной информацией в составе ст. 159.6 УК РФ следует, например, признать электронный документ, информацию о наличии денежных средств, находящихся на лицевом счет в банке и т.п. Данный предмет преступления, очевидно, следует рассматривать только в связи с другими, указанными в статье: имущество или право на имущество. В Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» также указывается, что все действия с компьютерной информацией, описанные в ст. 159.6 УК РФ для квалификации деяния по данному составу преступления должны в итоге позволить виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него [3].

Библиографический список

1. Барчуков, В. К. Непосредственный объект мошенничества в сфере компьютерной информации / В. К. Барчуков. – URL: https://cyberleninka.ru /article/n/neposredstvennyy-obekt-moshennichestva-v-sfere-kompyuternoy-informatsii (дата обращения: 05.02.2020).

2. Корнеева, А. В. Теоретические основы квалификации преступлений / А. В. Корнеева; под ред. А.И. Рарога. – М., 2008. – С. 51.

3. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // URL: https://www.garant.ru (дата обращения: 11.02.2020).

4. Конвенции о преступности в сфере компьютерной информации ETS N 185 от 23 ноября 2001 г. – URL: https://base.garant.ru/4089723/ (дата обращения: 07.02.2020).

5. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 // URL: http://www.consultant.ru (дата обращения: 10.02.2020).

УДК 343.98:004

О НЕКОТОРЫХ ПРОБЛЕМАХ РАЗРАБОТКИ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В КИБЕРПРОСТРАНСТВЕ

Корма Василий Дмитриевич
доктор юридических наук, профессор
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)

В статье изложены некоторые проблемы разработки полноценной методики расследования преступлений, совершенных в киберпространстве. Основное внимание уделено аспектам употребления единой криминалистической терминологии и использования подсистемы научного знания о следственном познании (познавательной деятельности следователя).

Ключевые слова: *методика расследования преступлений, совершенных киберпространстве; преступления, совершенные в киберпространстве; компьютерная информация; электронно-цифровые следы; следственное познание; следственное распознавание.*

ABOUT SOME DEVELOPMENT TECHNIQUES ACANCOSE EXCLUSIVE, PERFECT IN CYBERSPACE

Korma Vasily Dmitrievich
Doctor of law, Professor
Kutafin Moscow State Law University (MSAL), Moscow, Russia

The article outlines some of the challenges of developing a full-fledged methodology for investigating crimes committed in cyberspace. The focus is on aspects of the use of a single forensic terminology and the use of a subsystem of scientific knowledge about investigative cognition (cognitive activity of the investigator).

Keywords*: the methodology for investigating crimes committed in cyberspace; crimes committed in cyberspace; Computer information Electro-digital footprints; Investigative cognition; Investigative recognition.*

Расследование преступлений, совершенных в киберпространстве, вызывает у следователей определенные сложности. Происходит это зачастую на фоне низкой раскрываемости этой группы преступных деяний, что обусловлено рядом особенностей, включая специфику совершения данных преступлений, несовершенство правовой базы, малую эффективность имеющихся методов, средств и технологий их расследования, трудности с обобщением материалов следственной и судебной практики по каждому виду рассматриваемых преступных деяний, недостаточную квалификацию следователей для работы с не-

традиционными источниками доказательственной информации и др. (Киберпространство – это часть цифровой среды, где происходит управление различного рода объектами физического мира посредством использования Интернета, других сетей и телекоммуникационных каналов [1]).

Кроме того, к проблеме расследования таких преступных деяний можно отнести отсутствие общепринятой, полноценной методики расследования преступлений, совершенных в киберпространстве, которая относится к разряду общих (базовых) методик. Основанием для формирования общих (базовых) методик расследования выступает наличие общих закономерностей совершения преступлений, выделенных в группу, и общих закономерностей их расследования [2]. При этом выделенные преступления могут входить как в одну главу, так и в разные главы УК РФ в зависимости от основания объединения этих преступлений в группу.

На качество разработки данной методики расследования преступлений негативно сказывается, в первую очередь, неоднозначное употребление криминалистических понятий, выражаемых определениями и обозначениями (знаками и терминами), т.е. отсутствие единой терминологии.

Так, в отечественной криминалистической литературе изменения данных, хранящиеся в памяти компьютерных устройств, называют по-разному: «виртуальные следы», «информационные следы», «бинарные следы», «электронно-цифровые следы», «компьютерно-технические следы», «цифровые следы». По обоснованному мнению, Е.А. Лушина, наиболее точным по смыслу названием этих следов является термин «электронно-цифровые следы» [3].

Такая же неоднозначная ситуация в научных кругах обстоит и с другими криминалистическими категориями, например, «компьютерная информация» – «цифровая информация» – «компьютерные данные»; «цифровая среда» – «электронная среда» – «киберпространство» – «информационное пространство»; «компьютерная система» – «информационная система». Преступления, совершенные в компьютерных и телекоммуникационных системах, номинируются также различно: «компьютерные преступления», «преступления информационного характера», «преступления в сфере компьютерной информации и высоких технологий», «информационные преступления», «киберпреступность», «преступления в сфере обращения компьютерной информации», «преступления в сфере компьютерной информации», «преступления в сфере высоких технологий».

Р.С. Белкин, затрагивая тему о языке криминалистики, отмечал, что определения и понятия должны быть, во-первых, однозначными и общепринятыми (в идеале), а, во-вторых, выражать определенное познавательное значение [4].

Кроме того, на качество методики расследования преступлений данной категории влияет отсутствие в отечественной криминалистике полноценной, целостной, логически не противоречивой подсистемы научного знания о следственном познании (познавательной деятельности следователя). Данная подсистема знаний активно способствовала бы образованию базы для формирования теоретических и практических основ методики расследования, поскольку разработка методик расследования различных категорий преступлений связана

с определением теоретических и методических предпосылок, на основе которых можно выявить общие закономерности, свойственные следственной деятельности, и построить систему эффективных методов, средств и технологий расследования соответствующей категории преступлений. Задачи и функции методики расследования предопределяют анализ следственной деятельности как специфического процесса познания расследуемого события. По своей природе расследование преступлений является разновидностью познавательной деятельности.

Результаты ранее проведенных нами исследований в области теории о следственном познании [5] позволяют сделать следующие выводы:

1. Следственное познание, как вид практической юридической деятельности, можно определить как осуществляемый следователем в формах рассмотрения сообщения о преступлении и предварительного следствия, процесс мысленного образно-знакового воссоздания и уголовно-процессуального доказывания обстоятельств, имеющих значение для обнаружения признаков преступления, установления достоверной, соответствующей действительности картины, правовой сущности, родо-видовой принадлежности и механизма содеянного, а также для выявления и идентификации его участников и принятия адекватных содержанию объективной истины процессуальных решений, предусмотренных нормами права, регулирующими досудебное уголовное производство.

2. Понятия познание и распознавание не относятся к числу равнообъёмных категорий, а соотносятся друг с другом как род (познание) и вид (распознавание), соответственно, как целое и часть данного целого. Поэтому каждый случай распознавания является познанием, но не каждое познание является распознаванием.

3. Понятие познания как более широкое по объёму по сравнению с понятием распознавания охватывает все без исключения виды и разновидности уголовно-релевантных объектов и признаков, всю совокупность целей, задач, средств и методов уголовно-процессуальной познавательной деятельности следователя в сфере досудебного уголовного производства. Что же касается распознавательной составляющей данного процесса, то на её долю приходится только часть указанного целого. Это более узкая по объему, но и более глубокая и более богатая по своему содержанию часть.

4. Предметом следственного распознавания являются: а) ненаблюдаемые следователем уголовно-релевантные объекты (преступления, другие ненаблюдаемые деяния, сходные по своим признакам с преступлениями, но таковыми не являющиеся, а также иные ненаблюдаемые уголовно-релевантные события, явления, процессы, действия, виды поведения (деятельности), предметы и т.д.); б) чувственно не воспринимаемые сущностные, внутренние, скрытые признаки, свойства, связи и отношения наблюдаемых следователем уголовно-релевантных объектов.

5. Конечной целью распознавательной активности следователя служит полное, достоверное, доказанное знание о целостной совокупности внешних и внутренних признаков ненаблюдаемых им объектов и чувственно не восприни-

маемых сущностных, скрытых, внутренних признаков, свойств, связей и отношений наблюдаемых им же объектов. (Механизм следственного распознавания сродни механизму решения уравнения со многими неизвестными, сопряженному с преодолением информационной неопределенности).

Большое значение для разработки методики расследования преступлений имеют понятие и криминалистическая классификация преступных деяний, входящих в рассматриваемую группу. В международно-правовых документах однозначного определения понятия преступлений этой группы нет, но есть их определенный перечень.

Е.С. Шевченко, проведя глубокий анализ разнообразных подходов в понимании рассматриваемой нами группы преступлений, пришла к обоснованному выводу о том, что это общественно опасные деяния, совершаемые в киберпространстве, посягающие на общественную безопасность, собственность, права человека и иные охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которых является компьютерная информация, выступающая в роли предмета или средства преступления [6]. Иными словами, для преступлений данной категории характерно то, что компьютерная информация (компьютерные данные), будучи важным элементом механизма подготовки, совершения, сокрытия преступления во всех случаях играет одну из главных ролей в механизме отражения активности причинителя вреда. Это обстоятельство позволяет рассматривать различные виды преступлений, так или иначе связанных с компьютерной информацией, в качестве объектов специального исследования на теоретическом и прикладных уровнях. (Под компьютерной информацией обычно понимают отображение фактов, информации или понятий в форме, пригодной для распознавания, обработки или хранения с помощью компьютера, а также данные, хранящиеся на физических носителях (жестких дисках, флэш-картах, картах памяти USB), в памяти компьютерной системы, передаваемые через беспроводную или радиосвязь и их физическое изображение (например, в печатной форме или на экране устройства) [7]).

Вопросы криминалистической классификации преступлений в цифровой среде по различным основаниям рассматривались в работах В.В. Крылова (1998), В.А. Мещерякова (2001), В.Б. Вехова (2004), Д.В. Пашнева (2004), Е.С. Шевченко (2016) и других-ученых криминалистов. В.А. Образцов отмечает, что продуманное построение криминалистической классификации преступлений выступает важным и необходимым условием разработки эффективных методических рекомендаций по расследованию определенных категорий преступлений [8].

Доказательственное значение при расследовании конкретного преступления будет сама информация, запечатленная на соответствующих носителях. Именно она отражает следы преступления, и содержание ее не зависит от представленного носителя.

Средством обнаружения признаков преступления и установления обстоятельств содеянного служит так называемая дорожка электронно-цифровых сле-

дов, представляющей собой систему образования следов в компьютерной сети и состоящую из нескольких последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линии связи через коммутационное оборудование операторов связи от компьютера преступника до компьютера потерпевшего [9].

Электронно-цифровые следы занимают промежуточное место между традиционно выделяемыми в криминалистике материальными и идеальными следами. Их принципиальное отличие в том, что они сохраняют в себе отражение не свойств следообразующих объектов, а всего лишь фиксируют значения параметров формализованной (математической) модели, которая была положена в основу создания технического устройства для регистрации реальной действительности. В своей совокупности эти следы формируют такие необычные для криминалистики объекты как электронные документы, торрейт-файлы, полиморфные компьютерные программы, виртуальные машины и т. п., которые обладают уникальными криминалистическими свойствами, не вписывающимися в традиционные представления [10].

Электронно-цифровые следы обладают рядом специфических свойств, определяющих их обнаружение, извлечение и использование в качестве доказательств в ходе расследования. Так, они существуют на материальном носителе, но не доступны для восприятия следователем, т.е. являются ненаблюдаемыми уголовно-релевантными объектами. Для их обнаружения и извлечения необходимы специализированные программно-технические средства. Данные следы неустойчивы, поскольку их можно легко удалить или изменить. Поэтому собирание данных следов должно производиться с соблюдением специальных технических требований. При этом должны соблюдаться такие общие принципы как использование общепринятых технологий и процедур, привлечение квалифицированных специалистов, использование специальных методов (защита файлов, применение алгоритмов хэширования и цифровых подписей, и др.).

В плане сохранности электронно-цифровые следы как доказательства менее уязвимы по сравнению с идеальными следами, и более уязвимы по сравнению с традиционными материальными следами.

Процесс электронно-цифрового отображения механизма формирования электронно-цифрового следа имеет свою специфику и включает в себя две основные группы компонентов: 1) деятельность активных сущностей (некоего трасологического аналога следообразующих объектов); 2) человека или вычислительного процесса и программно-аппаратной среды (некоего аналога следовоспринимающих объектов). В качестве активных сущностей могут выступать: а) деятельность человека с его привычками, навыками и умениями; б) вычислительный процесс, который реализуется в соответствии с компьютерной программой или их совокупностью; в) деятельность человека в сочетании с вычислительным процессом или их совокупностью. В программно-аппаратную среду входят: а) физические носители компьютерной (цифровой) информации (винчестеры, флеш-карты, CD и DVD диски, и др.) с размещенными на них программными продуктами и информационными массивами; б) среда распростра-

нения электромагнитных волн оптического и радиодиапазонов (например, при построении вычислительных сетей, объединенных по радиоканалу (WiFi, GPRS, WiMax, 3G и т. п.). Иными словами, при формировании электронно-цифрового следа на материальном носителе фиксируются не сами свойства наблюдаемого физического процесса (например, звука, динамического изображения), а только цифровые значения параметров формализованной математической модели, которая положена в основу технического устройства регистрации его реального проявления. Структура электронно-цифрового следа включает в себя не только уголовно-релевантную информацию, но и значительный объем вспомогательной данных, отвечающих за целостность и доступность компьютерной информации следа. При этом эта структура зависитконова как от технических особенностей регистрирующего устройства, так и от его текущего состояния [11, 12].

В криминалистической литературе электронно-цифровые следы классифицируют по следующим основаниям:

1. По форме их носителя: а) на оптических носителях (CD, DVD, Blue-Ray диски и пр.); б) полупроводниковых носителях (флеш-память, SSD –носители и магнитные носители (жесткие диски).

2. По способу осуществления доступа к ним: а) локальный; б) удаленный.

В первом случае доступ может осуществляться непосредственно через устройство, содержащее носитель, на котором находятся следы (используется весь комплекс всех операций по собиранию и исследованию следов). Во втором случае доступ осуществляется путем дополнительного подключения к телекоммуникационным сетям (исключается изъятие следов в традиционном криминалистическом понимании, но могут быть скопированы на иной носитель).

3. По характеру сложности доступа: а) доступные (например, электронные документы); б) скрытые (скрытые файлы, информация, скрытая с помощью методов стеганографии); в) зашифрованные (сам факт наличия информации очевиден следователю, но доступ к ее содержанию затруднен из-за наличия паролей или иных средств ли аутентификации ее владельца или создателя).

4. По характеру происхождения электронно-цифровых следов, оставленных человеком: а) непосредственно (электронные документ, записи в социальных сетях и т.п., которые могут быть изучены следователем в ходе следственных действий); б) опосредовано (данные телеметрии, системные логи, атрибуты создаваемых файлов, и т.п., которые требуют использования специальных знаний (зачастую компьютерно-технических исследований).

5. По типу устройства, на котором находятся следы: а) стационарные (сервера, персональные стационарные компьютеры, стационарные веб-камеры); б) мобильные (смартфоны, планшеты, ноутбуки и т.д.).

6. По назначению: на выполнение полезных и вредных (трояны, вирусы, программы-«вымогатели» и др.) функций [13].

И.И. Пророков отмечал, что «знание механизма образования следов, их классификации позволяет судить о способе совершения определенных дейст-

вий, результатом которых данные следы являются, об особенностях объектов, образовавших эти следы» [14]. Применительно к нашей теме, познание закономерностей и специфики образования электронно-цифровых следов, их классификации имеет важное значение для теории и практики выявления и расследования преступлений данной категории, ибо оно может способствовать оптимизации теоретических и прикладных разработок, нацеленных на решение различных задач (например, установление данных о пользователе (имя, адрес, дата рождения, номер телефона, адрес электронной почты, адрес поставщика услуг Интернет, номер и счет, используемый для осуществления платежных операций расчетам за услуги провайдера и т.д.) и сведений о сообщении, передаваемого по техническим каналам связи (например, данные первоначального номера телефона, используемого для связи с LOG - файлом регистрации; информация о дате и времени сеанса связи; статические и динамические IP-адресные журналы регистрации провайдера в Интернет и соответствующие телефонные номера, исходящие журналы связи, включающие тип использованных протоколов, самих протоколов и т. д.).

В то же время механизм образования следов является важным элементом криминалистической характеристики преступлений, совершенных в киберпространстве. Под криминалистической характеристикой преступлений рассматриваемой категории понимается типовой, научно обоснованный информационный продукт, позволяющий составить представление о сущности, содержании и сходных признаках данной группы преступных деяний, имеющих значение для определения на практике круга обстоятельств, подлежащих установлению, основных направлений, версий, задач, средств и методов познавательной деятельности следователя при расследовании этих преступлений, ориентируясь на которые и данные, отражаемые в криминалистических характеристиках отдельных видов и разновидностей преступлений этой группы, упомянутый субъект мог эффективно реализовать функции распознавания, доказывания, уголовного преследования, и предупреждения преступлений, которые им расследуются.

Познавательная деятельность следователя в ходе расследования преступлений, совершенных в киберпространстве, направлена не только на обнаружение, фиксацию, изъятие и распознавание электронно-цифровых, но и традиционных материальных и идеальных следов преступления. Так, криминалистически значимая информация может быть получена при исследовании материальных следов (следов рук, микрообъектов, документов на бумажных носителях и т. п.) и идеальных следов (образов, возникающих в сознании, памяти людей).

Особенности технологии распознавательной деятельности следователя в стадиях возбуждения уголовного дела, первоначального и последующих этапов расследования преступлений, совершенных в киберпространстве, достаточно подробно изложены в работе Е.С. Шевченко [15].

Библиографический список

1. Россия и вызовы цифровой среды: рабочая тетрадь / гл. ред. И.С. Иванов. – М., 2014. – С. 7.
2. Кардашевская, М. В. Базовые методики расследования преступлений: основание для формирования / М. В. Кардашевская // Расследование преступлений и пути их решения. – 2017. – № 4. – С. 146–148.
3. Лушин, Е. А. О термине «электронно-цифровые следы» / Е. А. Лушин // Расследование преступлений: проблемы и пути их решения. – 2017. – № 4. – С. 161–163.
4. Белкин, Р. С. Курс криминалистики / Р. С. Белкин. – М.: Юрист, 2001. – 464 с.
5. Корма, В. Д. Следственное познание как объект междисциплинарного исследования / В. Д. Корма, В. А. Образцов // Lex Russica. – 2018. – № 12. – С. 90–100.
6. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступности: дис. … канд. юрид. наук / Е. С. Шевченко. – М., 2016. – С. 22–37.
7. Основы борьбы с киберпреступностью и кибертерроризмом / сост. В.С. Овчинский. – М., 2017. – С. 10.
8. Образцов, В. А. Проблемы совершенствования научных основ методики расследования преступлений: дис. … д-ра юрид. наук / В. А. Образцов. – М., 1985. – С. 18.
9. Вехов, В. Б. Криминалистическое значение сведений о компьютерных сетях и образующихся в них дорожках электронно-цифровых следов / В. Б. Вехов // Информационное обеспечение раскрытия и расследования преступлений. В 3 ч. Ч. 1. – Луганск: ЛГУВД, 2008. – С. 78–85.
10. Мещеряков, В. А. Криминалистика в цифровой век / В. А. Мещеряков // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сб. ст. междунар. науч.-практ. конф. – М., 2018. – С. 182–183.
11. Агибалов, В. Ю. Виртуальные следы электронных документов в компьютерных сетях / В. Ю. Агибалов, В. А. Мещеряков // Воронежские криминалистические чтения. – 2012. – Вып. 14. – С. 19–22.
12. Мещеряков, В. А. Следы преступлений в сфере высоких технологий / В. Ю. Мещеряков // Библиотека криминалиста. – 2013. – № 5. – С. 269.
13. Бахтеев, Д. В. Криминалистическая классификация цифровой доказательственной информации / Д. В. Бахтеев // Криминалистика в условиях информационного сообщества (59-е ежегодные криминалистические чтения): сб. ст. междунар. науч.-практ. конф. – М., 2018. – С. 44–49.
14. Пророков, И. И. Криминалистическая экспертиза следов / И. И. Пророков. – Волгоград, 1980. – С. 81.
15. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступности: дис. … канд. юрид. наук / Е. С. Шевченко. – М., 2016. – С. 58–76.

УДК 341

КИБЕРБЕЗОПАСНОСТЬ В КОНТЕКСТЕ МЕЖДУНАРОДНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

Костин Сергей Андреевич
кандидат юридических наук
АНО ВО «Российский новый университет», Москва, Россия

В настоящей работе исследуется трансграничный аспект киберпространства, как среды, предопределившей появление новых вызовов и угроз в области обеспечения международной безопасности перед мировым сообществом. Одновременно с этим анализируется институциональный потенциал существующих международно-правовых систем обеспечения коллективной безопасности с целью уменьшения возросших угроз в сфере обеспечения международной безопасности в связи трансграничным аспектом киберпространства.

Ключевые слова: *международная безопасность, региональная безопасность, коллективная безопасность, кибербезопасность, киберпространство, информационно-коммуникационные технологии (ИКТ).*

CYBERSECURITY IN THE CONTEXT OF THE PROCURING INTERNATIONAL-LEGAL SECURITY

Kostin Sergey Andreevich
candidate of law, executive Director of the Law Institute
ANO VO «Russian new University», Moscow, Russia

In the present article analysis, the cross-border aspect of cyberspace as an environment that predetermined new challenges and threats emergence in front of international community in the international security area. At the same time, analysis the institutional potential of existing international legal systems for ensuring collective security to reduce the increased threats to international security in connection with the cross-border aspect of cyberspace.

Keywords: *International security; Regional security; Collective security; Cybersecurity; Cyberspace; Information and communications technology (ICT).*

Одним из способов международно-правового обеспечения международной безопасности является создание систем обеспечения коллективной безопасности. Примерами таких систем являются Организация Американских Государств, Организация Североатлантического договора, Организация Договора о коллективной безопасности, Договор о коллективной обороне Юго-восточной Азии (Манильский пакт), Варшавский договор, Договор о безопасности АНЗЮС. Основополагающие документы каждой из этих международно-правовых систем говорят о том, что целью их создания является предотвращение и устранение угроз миру и безо-

пасности. В наши дни, к ставшим уже классическими, добавляются новые вызовы и угрозы в области безопасности, среди которых все более отчетливо выделяется международный терроризм в различных его проявлениях, международная наркоторговля, незаконная миграция и торговля людьми [1].

В XXI веке мы стали свидетелями стремительного развития и повсеместного применения в повседневной жизни информационно-коммуникационных технологий (ИКТ). ИКТ ускорили международное экономическое развитие, усилили потенциал государств, являющихся лидерами в этой области, а также открыли новые возможности в военно-промышленной сфере.

Появление ИКТ предопределило появление принципиально нового пространства для взаимодействия – киберпространства, пространства, не ограниченного границами, одного или даже нескольких государств. Само по себе киберпространство не представляет угрозы, однако, как и все малоизученное – настораживает, это также усугубляется тем, что киберпространство можно использовать как в благих целях, так и злонамеренно.

Трансграничный аспект киберпространства, становится вызовом перед международным сообществом в части международно-правового регулирования взаимоотношений и поддержания необходимого уровня безопасности. Здесь следует отметить, что обеспечение кибербезопасности – это меры, направленные на предотвращение использования информационно коммуникационных технологий для достижения преступных целей, направленных на подрыв основ безопасности. Способами такого преступного использования можно считать телефонный (IP) терроризм, *Ddos*-атаки, также торговлю товарами ограниченными или изъятыми из оборота в большинстве стран мира. В ряде стран таких как Германия, Израиль, Соединенные Штаты Америки, Российская Федерация и др. созданы и функционируют специальные рода войск, ориентированные на «решение задач» в киберпространстве. Говоря о борьбе с киберпреступностью, в Российской Федерации ключевая роль отводится двум ведомствам – Федеральной Службе Безопасности и Росфинмониторингу, в части противодействия финансовым преступлениям.

Неоднократно доказано, что обеспечить международную безопасность и создать прочную международно-правовую основу, регулирующую данную область международных отношений не под силу как одному государству, так и группе государств, объединенных региональными или межрегиональными соглашениями. К решению этого вопроса необходимо подходить на самом высоком международном уровне.

В ряде отношений Устав Организации Объединенных Наций является основополагающим документом всего мирового сообщества. В нем сформулированы принципы, предписывающие модель правомерного поведения в международных отношениях, внутренней и внешней политике государства. Они имеют статус императивных норм «*jus cogens*», а принимаемые нормативные акты и международные соглашения, противоречащие им, зачастую признаются ничтожными или недействительными.

В момент принятия Устава ООН мировому сообществу было незнакомо

такое понятие как киберпространство и мир не сталкивался с таким форматом международных отношений. С течением времени и все большим присутствием ИКТ в повседневной жизни в рамках ООН стали активнее обращать внимание на этот аспект. Пунктом 4 Резолюции ГА ООН 60/45 от 8 декабря 2005 г. было предусмотрено создание в 2009 г. Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ) с целью «исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению» [7]. ГПЭ были выявлены и сформулированы угрозы, риски и факторы уязвимости, связанные с обеспечением безопасности при использовании информационно коммуникационных технологий (ИКТ). Признавая факт использования ИКТ в том числе в военной сфере, в контексте обеспечения международной безопасности ГПЭ выявила две ключевые группы риск-факторов: угроза инфраструктуре ИКТ, как объекту для покушения; предупреждение преступного использования ИКТ, как средства достижения преступных целей [8]. В настоящее время создано три ГПЭ, которые занимаются изучением угроз в сфере ИКТ и кибербезопасности, а вопросы информатизации и телекоммуникаций в контексте международной безопасности периодически рассматриваются на ежегодной повестке ГА ООН [9].

В декабре 2018 года, ГА ООН одобрила Резолюцию A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [10], инициированную Российской Федерацией, и содержащую «свод международных правил, норм и принципов ответственного поведения государств», а также созыв «начиная с 2019 года, в целях придания переговорному процессу в Организации Объединенных Наций по безопасности в сфере использования информационно-коммуникационных технологий более демократического, инклюзивного и транспарентного характера рабочей группы открытого состава, действующей на основе консенсуса, в целях продолжения в качестве приоритета дальнейшей выработки норм, правил и принципов ответственного поведения государств» в интернете.

Вышесказанное не означает, что межрегиональные и региональные организации должны оставаться в стороне от участия в решении данного вопроса. В силу стремительного внедрения ИКТ, такая работа должна продолжаться на межрегиональном и региональном уровнях. Так, в частности в Североатлантическом альянсе наблюдается устойчивое развитие институциональных органов в этой области, ключевым из которых является Комитет по киберзащите – ведущий комитет по политическому управлению и политике в области киберзащиты в целом. На рабочем уровне за координацию киберзащиты во всех гражданских и военных органах НАТО отвечает Совет по управлению киберзащитой, в который входят руководители политических, военных, оперативных и технических органов НАТО, отвечающие за киберзащиту. Совет НАТО по консультациям, контролю и командованию является основным комитетом для консультаций по техническим аспектам и аспектам внедрения киберзащиты. Технический центр отвечает за предоставление услуг технической кибербезопасно-

сти по всему Альянсу. Технический центр (*NCIRC*) играет ключевую роль в реагировании на любые компьютерные инциденты, затрагивающие Альянс. Он обрабатывает и сообщает об инцидентах, а также распространяет важную информацию, связанную с инцидентами в сфере обеспечения информационной безопасности. Координационный центр является кадровым элементом, отвечающим за координацию деятельности в области киберзащиты [2].

Европейский союз также уделяет внимание вопросам, связанным с противодействием преступлениям террористической направленности, совершаемым в т.ч. с использованием киберпространства. В частности, конец 2017 и 2018 годы прошли под эгидой активных действий, связанных с началом работы Постоянного структурированного сотрудничества (*PESCO*) [3], за координацию расследования преступлений, касающихся двух и более государств, отвечают Евроюст и Европол. Перечень компетенций Евроюста предусмотрен статьей 4 Решения Совета (2002/187/JHA) [4], Европола, также статьей 4 Решения Совета [5], которые включают в себя преступления террористической направленности.

Уставом Организации Договора о Коллективной Безопасности предусматривается, что «члены координируют и объединяют свои усилия в борьбе с международным терроризмом и экстремизмом, незаконным оборотом наркотических средств и психотропных веществ, оружия, организованной транснациональной преступностью, нелегальной миграцией и другими угрозами безопасности государств – членов» [6]. В 2014 году в рамках ОДКБ был создан Консультационный координационный центр по вопросам реагирования на компьютерные инциденты (ККЦ ОДКБ). ККЦ ОДКБ образован с целью координации взаимодействия уполномоченных органов по вопросам, связанным с компьютерными инцидентами, несущими угрозы функционированию информационно-телекоммуникационных сетей и информационных систем любого из государств – членов ОДКБ.

Однажды международное право сделало границы между государствами прозрачными, свидетельством чему является всё, что нас окружает в повседневной жизни: товары различных стран лежат на прилавках; мобильная связь и Интернет доступны из любой точки Мира; можно отправлять и получать денежные переводы по всему миру; присутствует повсеместное морское, авиа и автомобильное сообщение; осуществляется международная доставка грузов, а также много другое. Это стало возможно благодаря единому правовому регулированию, благодаря общему международному праву.

Решение вопроса правового регулирования взаимоотношений в киберпространстве лежит в плоскости международного права. Здесь Организация Объединенных Наций, в силу своего универсального характера, а также наибольшей вовлеченности со стороны членов мирового сообщества, должна играть главную роль в деле институционализации отношений, а новая концепция международно-правового обеспечения коллективной безопасности должна включать в себя элемент, связанный с обеспечением безопасности в киберпространстве.

Библиографический список

1. Потемкина, О. Ю. Усиление угрозы терроризма в Европе и ответ Европейского союза / О. Ю. Потемкина. – URL: http://www.instituteofeurope.ru /images/uploads/analitika/an39.pdf.

2. Cyber defence. Evolution // NATO official website. – URL: https://www.nato.int/cps/cz/natohq/topics_78170.htm.

3. Протокол заключения Совета ЕС от 14 дек. 2017 г. (EUCO 19/1/17 REV1) // Официальный сайт Совета Европейского Союза. – URL: http://www.consilium.europa.eu/media/32204/14-final-conclusions-rev1-en.pdf.

4. Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA). Official Journal of the European Communities. Eurojust official website // URL: http://www.eurojust.europa.eu.

5. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. Official Journal of the European Communities // URL: https://www.europol.europa.eu.

6. Устав ОДКБ. Официальный сайт ОДКБ. – URL: https://odkb-csto.org/documents/ustav_organizatsii_dogovora_o_kollektivnoy_bezopasnosti.

7. Резолюция ГА ООН 60/45 от 8 дек. 2005 (A/RES/60/45) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Официальный сайт ООН. – URL: https://undocs.org/ru/A/RES/60/45 (дата обращения: 20.11.2019).

8. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/68/98*) // Официальный сайт ООН. – URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

9. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // Управление ООН по вопросам разоружения. – URL: https://www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т.

10. Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/73/27) от 5 дек. 2018 г. // Официальный сайт ООН. – URL: https://undocs.org/ru/A/RES/73/27.

УДК 343.141

ОСОБЕННОСТИ ЦИФРОВОГО УГОЛОВНОГО СУДОПРОИЗВОДСТВА С УЧАСТИЕМ ЛИЦ С ОГРАНИЧЕННЫМИ КОГНИТИВНЫМИ СПОСОБНОСТЯМИ

Курбатова Светлана Михайловна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья касается вопросов правового статуса участников производства по уголовному делу из числа лиц с ограниченными когнитивными способностями с учетом тенденций по цифровизации уголовного судопроизводства в России. Недостаточное внимание урегулированию данных аспектов может повлечь за собой ряд проблем правоприменительного характера, связанных с нарушением прав человека у лиц, у которых имеются ограниченные когнитивные способности, и которые вовлекаются в уголовный процесс в качестве его участников.

Ключевые слова: *уголовное судопроизводство цифровое судопроизводство, участники уголовного судопроизводства, ограниченные когнитивные способности, когнитивный подход.*

FEATURES OF DIGITAL CRIMINAL PROCEEDINGS INVOLVING PERSONS WITH COGNITIVE DISABILITIES

Kurbatova Svetlana Mikhailovna
Candidate of Law, Associate Professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article deals with the legal status of participants in criminal proceedings from among persons with limited cognitive abilities, taking into account trends in the digitalization of criminal proceedings in Russia. Insufficient attention to the resolution of these aspects can lead to a number of law enforcement problems related to the violation of human rights in persons who have limited cognitive abilities and who are involved in criminal proceedings as participants.

Keywords: *criminal proceedings digital proceedings, participants in criminal proceedings, limited cognitive abilities, cognitive approach.*

Интенсивное развитие общества в последние десятилетия создало потребность в новых средствах коммуникации, что способствовало развитию процесса по замене низких технологий высокими. В России эта тенденция нашла свое правовое оформление сначала в указе Президента РФ № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», где одной из важнейших задач, стоящих перед государством, была обозначена задача по обеспечению использования российских информационных и коммуникационных технологий в органах государственной власти Российской Федерации, компаниях с государственным участием, органах местного само-

управления; затем – в распоряжении Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации», впоследствии утратившем силу, и в пришедшей ей на замену национальной программе «Цифровая экономика Российской Федерации», утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16.

Это не могло не затронуть сферу судопроизводства. И действительно, понимая серьезность и важность данного вопроса, свое внимание ему уделяют многие ученые: К. Г. Вивчарук [5], О.В. Колга, Е.Б. Калашникова [10], В.Н. Григорьев, С.С. Суходолов [8] и др.

Особое внимание уделяется цифровизации уголовного судопроизводства, что и понятно, учитывая его специфику и повышенные риски нарушения прав человека в сфере его действия [3, 7, 9].

Так, Л.В. Бертовский считает, что такое цифровое уголовное судопроизводство это «урегулированная нормами процессуального права деятельность суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел, в которой ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность» [3, с. 175].

Основными сквозными цифровыми технологиями, используемыми в рамках цифрового судопроизводства, могут стать: большие данные, получаемые из внутренней информации предприятий и организаций, из систем видеонаблюдений, из различного рода криминалистических и иных учетов и т.д.; нейротехнологии и искусственный интеллект; компоненты робототехники и сенсорика; технологии блок-чейн; технологии беспроводной связи; технологии виртуальной и дополненной реальностей (визуализации информации при производстве следственных действий, представление доказательств в суде, моделирование исследуемых в судебном процессе событий) [3, с. 176].

Однако эти разработки не затрагивают вопроса решения проблемы участия в уголовном судопроизводстве лиц с ограниченными когнитивными способностями, хотя отдельные аспекты данной проблематики можно встретить в научной литературе [2, 4]. А когнитивные особенности личности являются важным фактором, влияющим на объем реализации правового статуса участников уголовного судопроизводства, на что нами ранее обращалось внимание [11].

Так, снижение когнитивных способностей проявляется не только в оценке ситуаций, но зачастую у таких лиц снижается и двигательная возможность, т. е. в ряде случаев они просто физически не могут явиться в суд. И таких лиц, на самом деле, достаточно много. Это лица: перенесшие инсульт или транзиторную атаку; с черепно-мозговой травмой; с болезнью Паркинсона; имеющие рассеянный склероз; находящиеся в хронической или острой депрессии; страдающие сердечной недостаточностью, гипотиреозом, сахарным диабетом тяжелой степени и др. [13, с. 13]. Много и других физических, психологических, психофизиологических состояний также сказывается на двигательных функциях людей, ограничивая их в реализации своих прав и исполнении своих обязанностей, в том числе в сфере уголовного судопроизводства.

В связи с этим предлагаем для таких лиц установить возможность дистанционного участия и выступления в судах, предусмотреть в соответствующих кодексах (не только в Уголовно-процессуальном) возможность во время судебного процесса устанавливать судебными приставами в месте нахождения такого лица видео-конференц связи. В случае, если такое лицо находится в больнице, привлекать в качестве специалиста лечащего врача, который бы представлял характеристику данного человека, его состояния, рекомендовал лучшее время для его допроса и др.

Отдельно хотелось бы остановиться на таких категориях граждан, как инвалиды по зрению, по слуху. Считаем, что они незаслуженно обойдены вниманием уголовно-процессуального законодателя. Например, лица с проблемами со зрением общаются с внешним миром в основном с помощью шрифта Брайля и на сегодняшний день имеющиеся технологии позволяют им через программное обеспечение конвертировать компьютерный текст в Брайль и быть активными пользователями ПК, а для лиц, у которых ограниченные слуховые возможности, разработаны специальные компьютерные технологии, при которых голос говорящего человека преобразуется в визуальные символы на экране монитора.

Однако данные технологии не находят своего применения в рамках уголовного судопроизводства. Предоставление же переводчика таким лицам не в полной мере решает проблему их ограниченного участия в уголовном процессе. Более того, тем самым утрачивается один из принципов уголовного судопроизводства – непосредственность восприятия (хотя в настоящее время он отнесен законодателем к общим условиям судебного разбирательства, с чем, на наш взгляд, нельзя согласиться), который является очень важной идеей, пронизывающей весь уголовный процесс [6, 14]. Хотя цифровые технологии в других областях успешно применяются для содействия данным категориям лиц.

Так, в институте Georgia Tech Research Institute (GTRI) уже давно разработана система формирования субтитров, призванная помочь глухим и слабослышащим людям, основанная на беспроводной мобильной технологии связи и специальном программном обеспечении COMMplements фирмы Peacock Communications Inc. Программа распознает речь и формирует несколько каналов субтитров для одновременно звучащих источников, включая те, что требуют языкового перевода. Субтитры по беспроводному каналу 802.11b передаются на КПК и любое другое подходящее для отображения текста устройство [17]. Корпорация IBM во второй половине 80-х гг. прошлого века уже представила вниманию профессиональных логопедов США настольную систему «Видимая речь» на базе персонального компьютера для формирования и коррекции фонетической стороны речи. В нашей стране освоение этой компьютерной программы началось в 90-х гг. прошлого века. В 1991 г. в Институте коррекционной педагогики РАО была русифицирована ее первая версия [16].

Компания Duxbury Systems с 70-х гг. прошлого века стала заниматься автоматизированием программ для незрячих людей, став сегодня мировым лидером программного обеспечения для данной категории лиц. А созданная данной компанией программа Duxbury Braille Translator (DBT) используется сейчас во всем мире для подготовки к печати любой документации на Брайле. Эта программа осуществляет двунаправленный перевод. Обыкновенный шрифт

переводится в азбуку Брайля и обратно. Но этим ее свойства не ограничиваются. DBT — это полнофункциональный текстовый редактор, при помощи которого можно подготовить любой документ к печати по брайлю на нескольких десятках языков, в самых разнообразных кодировках.

Duxbury BrailleTranslator позволяет импортировать файлы в формате MS Word, WordPerfect, HTML. Текст также можно создавать непосредственно в редакторе DBT. Вводить его можно как обычным способом, так и азбукой Брайля. Во втором случае клавиши основного ряда клавиатуры работают как клавиши брайлевской печатной машинки. Существует большое количество так называемых «ключей форматирования» – встроенных команд, позволяющих задать необходимый формат документов. Комбинации ключей форматирования позволяют создавать «стили», ещё более облегчающие работу с текстом. В комплект поставки основные стили уже входят, при том, что пользователю даны также все инструменты для создания новых. Совокупность стилей, ключей форматирования и текста можно сохранить в качестве шаблона и использовать в дальнейшем для создания других документов. DBT также включает в себя орфографический словарь на 300000 слов. А функция «Quick Find Misspelling» позволяет быстро обнаружить орфографические ошибки и устранить их. Программа DBT поддерживает практически все существующие модели брайлевских принтеров [18].

В связи с этим считаем возможным предусмотреть возможность изготовления протоколов процессуальных действий с участием таких лиц с использованием подобного рода программ, а также распечатки протоколов с использованием шрифта Брайля. Учитывая же как ценовые характеристики таких принтеров (от ста тысяч и выше), так и тот факт, что количество незрячих участников уголовного судопроизводства все же не так велико, то много таких аппаратов и не потребовалось бы, например, 1–3 на субъект РФ. Зато это бы способствовало обеспечению равенства прав участников производства по уголовному делу и соответствовало бы догмам международной доктрины [12] и положениям международных конвенций, призывающих государства создавать такие условия, в которых бы лица с ограниченными возможностями могли бы сами в полном объеме реализовывать свои права и обязанности, оставаясь активными членами общества.

Библиографический список

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.12.2019) // СПС Консультант плюс.

2. Антонов, В.П. Криминалистика: учебник / В.П. Антонов, И.И. Белозерова, Л.В. Бертовский и др. – М.: РГ-Пресс, 2018. – 960 с.

3. Бертовский, Л.В. Цифровое судопроизводство: проблемы становления / Л.В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства. Сб. мат-в междунар. научно-практич. конф. 2018. – С. 173–178.

4. Бертовский, Л.В. К вопросу о получении вербальной информации от лиц с особенностями когнитивного развития // Современная молодежь и вызовы экстремизма и терроризма в России и за рубежом: сб. мат-лов Всерос. (с междунар. участием) науч.-практ. конф. / под ред. Х.П. Пашаева. – Горно-Алтайск, 2019. – С. 125–128.

5. Вивчарук, К. Г. Электронное судопроизводство: отечественный опыт – достоинства и недостатки / К.Г. Вивчарук // Бизнес. Общество. Власть. – 2013. – № 14. – С. 15.

6. Виницкая, Ю.Л. К вопросу о понятии непосредственности в уголовном процессе / Ю.Л. Виницкая // Вестник ЮУрГу. – Сер. «Право». – 2016. – Т. 16. – № 1. – С. 35-43.

7. Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости / Л. А. Воскобитова // Lex russica (Русский закон). – 2019. – № 5. – С. 91–104.

8. Григорьев, В.Н. Цифровые информационные платформы как предмет нормативно-правового регулирования в сфере уголовного судопроизводства / В.Н. Григорьев, А.П. Суходолов, С.С. Ованесян и др. // Всероссийский криминологический журнал. – 2019. – Т. 13. – № 6. – С. 873–883.

9. Карташов, И. И. «Цифровые доказательства» в уголовном процессе / И. И. Карташов. – URL: http://cscb.su/n/0115s01/0115s01008.htm.

10. Колга, О. В. «Цифровое» направление развития правосудия в России / О. В. Колга, Е. Б. Калашникова // Актуальные проблемы юриспруденции: сб. ст. по мат-лам XVI междунар. науч.-практ. конф. – № 11 (15). – Новосибирск: СибАК, 2018. – С. 51–57.

11. Курбатова, С. М. Когнитивные особенности личности как фактор, влияющий на объем реализации правового статуса участников уголовного судопроизводства / С. М. Курбатова // Современная молодежь и вызовы экстремизма и терроризма в России и за рубежом: сб. мат-лов всерос. (с междунар. участием) научно-практич. конф. / под ред. Х.Л. Пашаева. – Горно-Алтайск, 2019. – С. 134–136.

12. Курбатова, С. М. Международное право и когнитивный подход как источники правового регулирования участия в уголовном судопроизводстве лиц с психическими расстройствами / С. М. Курбатова // Бизнес. Образование. Право. – 2019. – № 4 (49). – С. 371–377.

13. Левин, О.С. Диагностика и лечение когнитивных нарушений / О.С. Левин, Е.Е. Васенина. – М.: Изд-во РМАПО, 2013. – 51 с.

14. Михайлов, А. А. Виды непосредственности в уголовном процессе / А. А. Михайлов // Уголовная юстиция. – 2017. – № 10. – С. 56–65.

15. ГОСТ Р 52872-2012. Интернет-ресурсы. Требования доступности для инвалидов по зрению (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2012 г № 1789-ст.) // СПС Консультант Плюс.

16. Ходченкова, О. А. Использование современных информационных технологий при формировании речи при ее недоразвитии / О. А. Ходченкова // Сб. работ молодых ученых МГПУ. – М., 2009. – С. 234–239.

17. URL: https://forum.detective-agency.info/index.php?threads/Компьютерные-устройства-для-глухих-и-инвалидов.2574.

18. URL: https://elitagroup.ru/pages/prod-DBT.php.

УДК 35:004.9

*ЦИФРОВИЗАЦИЯ РОССИЙСКОГО ГОСУДАРСТВА: **НЕКОТОРЫЕ** АСПЕКТЫ*

Курбатова Светлана Михайловна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

Тенденции по снижению темпов роста производительности и необходимости перехода к новому укладу экономики, проявившиеся в начале XXI в. в большинстве индустриальных государств, затронули и Россию, что вызвало необходимость проработки новых путей развития и экономики и государственного и муниципального управления. И, как и у большинства стран, эти новые пути пошли в направлении развития цифровизации общества и государства, о чем и идет речь в данной статье.

Ключевые слова: *государство, политика, информационные технологии, экономика, государственное и муниципальное управление, цифровизация.*

DIGITALIZATION OF THE RUSSIAN STATE: SOME ASPECT

Kurbatova Svetlana Mikhailovna
Candidate of Law, associate Professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

Trends in declining productivity growth and the need to transition to a new way of economy, manifested in the beginning of the XXI century in most industrial countries, affected Russia, which caused the need to work out new ways of developing the economy and state and municipal management. And, as in most countries, these new ways have gone in the direction of digitalization of society and the state, which is what this article is about.

Keywords: *state, politics, information technology, economy, state and municipal management, digitalization.*

Тенденция снижения темпов роста производительности, сформировавшаяся в начале XXI в. во многих индустриально развитых странах, и возникшая в контексте проявившихся к тому времени целого ряда проблем [2], продемонстрировала:

– несоответствие современным потребностям существовавшего на то время уклада экономики;

– необходимость выработки новой экономической парадигмы, с учетом ожиданий общества и государства.

На ее формирование оказало существенное влияние повсеместное использование информационных технологий.

В результате многими странами стала проводиться осознанная и выстроенная государственная научно-технологическая и инновационная политика, целью которой стало стимулирование разработки и внедрения субъектами различных отраслей экономики таких технологий, которые бы автоматизировали, роботизировали и интеллектуализировали производственные процессы в этих отраслях для повышения их производительности, обеспечивая принципиально иное качество роста экономики.

Итогом этого должны стать:

– рост общей производительности экономики и социальной сферы;

– переход на более высокий уровень качества производственно-технологических процессов;

– выпуск продукции, «открывающей» новые рынки.

Соответственно, до 2035 года (а именно данная временная точка указывается аналитиками для подведения итогов реализации данной политики) одной из основных целей для России называется активное включение в новую технологическую революцию, для чего необходимо на государственном уровне разрабатывать правовую и информационную основы [12], которые в дальнейшем должны развиваться и внедряться в конкретных сферах экономики и социальной системы с учетом их специфики, гибкости и готовности. Например, весьма подвижна в данном направлении система высшего образования [13], где информационные технологии уже давно используются [11], являясь одним из факторов, влияющих на качество образования [9] и на формирование личности [1]. Востребованы информационные технологии при раскрытии и расследовании преступлений, особенно, если те совершаются с применением информационных компьютерных технологий [8], что открывает соответствующие перспективы для расширения их использования в уголовном судопроизводстве [5]. Тогда как некоторые сферы более консервативны для этого направления, например, аграрный сектор [6]. Реализация этой цели осуществит переход на новую модель развития, фундаментом которой станут высокотехнологичные индустрии, основанные на научных знаниях и инновационных технологиях» [8, с. 15–16].

В связи с изменение концептуальных позиций в экономике и социальной сферах, резонным является постановка вопроса об обновлении и системы государственного управления. Уже имеется ряд видений этого развития, например, представлен такой вариант как «Государство-как-Платформа» (ГкП, Платформа), которая представляет собой симбиоз интегрированных и цифровизированных процессов и перспективных технологий (единой системы сбора и хранения данных, цифровой инфраструктуры, автоматизированного принятия решений и т. д.).

Предлагаемая авторами концепция «Государства-как-Платформы» основана на переходе осуществления функций государственного управления на новом, более информационном и технологичном уровне, что должно подготовить и осуществить переход от нерелевантных подходов к планированию и контролю исполнения планов (с показателями типа «освоено средств», «уровень средней заработной

платы» и т. п.), используемых в настоящее время, к точным «индивидуализированным» индикаторам и показателям (уровня жизни населения, развития отдельных отраслей экономики и т.д.) для обеспечения оперативного получения обратной связи от объектов управленческой деятельности [7, с. 10].

Безусловно, идея данной концепции неоднозначна, исходя из устоявшихся взглядов на сущность государства как таковое. Тем не менее, потребности общества и государства диктуют свой заказ на дальнейшее развитие информационных технологий в той или иной сферах. Например, показательными являются банковская среда [14], система судопроизводства [4], и область криминалистики [2], сфера образования и ряд других, где уже на сегодняшний день мы можем наблюдать не только процесс внедрения данных технологий, но и их результаты, а главное – результативность.

Библиографический список

1. Айснер, Л.Ю. Роль образования в формировании личности / Л. Ю. Айснер, С. М. Трашкова // Казанская наука. – 2017. – № 10. – С. 126–128.

2. Актуальные психолого-педагогические, философские, экономические и юридические проблемы современного российского общества: колл. монография / Л. Ю. Айснер, Ю. В. Андреева, О. В. Богдан [и др.]. – Ульяновск, 2016. – 286 с.

3. Антонов, В. П. Криминалистика: учебник / В. П. Антонов, И. И. Белозерова, Л. В. Бертовский [и др.]. – М.: РГ-Пресс, 2018. – 960 с.

4. Бертовский, Л. В. Цифровое судопроизводство: проблемы становления / Л. В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства: сб. мат-лов междунар. науч.-практ. конф. – М., 2018. – С. 173–178.

5. Бертовкий, Л. В. Перспективы применения технологий «блокчейн» в уголовном судопроизводстве / Л. В. Бертовский, Г. С. Девяткин // Деятельность правоохранительных органов в современных условиях: сб. мат-лов XXIV междунар. науч.-практ. конф. – Иркутск, 2019. – С. 115–118.

6. Власов, В. А. Аграрная политика Российской Федерации как важнейший фактор модернизации российского государства / В. А. Власов // Аграрное и земельное право. – 2011. – № 3 (75). – С. 19–33.

7. Государство как платформа: доклад / М. Петров, В. Буров, М. Шклярук, А. Шаров. – М.: Центр стратегических разработок, 2018. – 53 с.

8. Девяткин, Г. С. Способы фиксации хода и результатов осмотра места происшествия при раскрытии и расследовании преступлений, совершенных с

применением информационных компьютерных технологий / Г. С. Девяткин, П. В. Малышкин, Н. Г. Балашкин // Трансформация социальных систем: проблемы и поиски путей решения: сб. науч. тр. по мат-лам всерос. науч.-практ. конф. (с междунар. участием). – Саранск, 2017. – С. 477–482.

9. Наумкина, В. В. Факторы, влияющие на качество высшего образования / В. В. Наумкина // Университетский комплекс как региональный центр образования, науки и культуры: мат-лы всерос. науч.-метод. конф. – Оренбург, 2019. – С. 4027–4030.

10. Новая технологическая революция: вызовы и возможности для России: экспертно-аналитический доклад / под ред. В. Н. Княгинина. – М.: Центр стратегических разработок, 2018. – 136 с.

11. Трашкова, С. М. Информационные технологии в образовании / С. М. Трашкова // Проблемы и перспективы развития науки в России и в мире: Сб. статей Междунар. научно-практич. конф. / отв. ред. А. А. Сукиасян. – Казань, 2015. – С. 118–121.

12. Трашкова, С. М. Основы правового регулирования информационных технологий в системе образования / С. М. Трашкова // Проблемы современной аграрной науки: мат-лы заочн. научн. конф. / отв. А. А. Кондрашев, Ж. Н. Шмелева. – Красноярск, 2015. – С. 226–228.

13. Фастович, Г. Г. Модернизация системы высшего образования как фактор повышения эффективности деятельности государственного механизма / Г. Г. Фастович, С. А. Бондаренко // Право и государство: теория и практика. – 2019. – № 1 (169). – С. 29–31.

14. Legaltech и юристы будущего (выступления участников) // Закон. – 2017. – № 11. – С. 20–38.

УДК 343.14

К ВОПРОСУ О «ЦИФРОВОЙ» КРИМИНАЛИСТИКЕ

Кустов Анатолий Михайлович
доктор юридических наук, профессор,
заслуженный юрист Российской Федерации
Академия управления МВД России, Москва, Россия

Статья посвящена дискуссионным вопросам, связанным с новым направлением в науке – цифровой криминалистикой. Дается авторское видение содержания цифровой криминалистики, предложено направление в использовании компьютерного моделирования модели механизма совершенного преступления в предварительном расследовании.

***Ключевые слова**: модель, компьютерное моделирование, механизм совершенного преступления, следователь, преступник, потерпевший, информационная модель.*

TO THE QUESTION OF «DIGITAL» CRIMINOLOGY

Kustov Anatoly Mikhailovich
Doctor of Law, Professor,
Merited Law Expert of the Russian Federation,
Management Academy of the Ministry of the Interior of Russia, Moscow, Russia

The article is devoted to discussion issues related to a new direction in science – digital criminology. The author's vision of the content of digital criminology is given, and the direction in using computer modeling of the model of the mechanism of the committed crime in the preliminary investigation is suggested.

***Keyword**: model, computer simulation, mechanism of the committed crime, investigator, criminal, victim, information model.*

«Цифровая» криминалистика - новый еще в науке не устоявшийся термин и спорный. В юридической литературе можно обнаружить его синонимы - «ЭВМ в криминалистике», «электронная криминалистика», «компьютерная криминалистика», «цифровая технология науки» и т. д.

С учетом анализа становления и развития криминалистической науки можно говорить о перспективном подходе данного направления в науке, имеющим непосредственное отношение к реалиям ее развития и развития современного информационного общества.

Анализ следственно-судебной практики показал, что гражданское общество и правоохранительная практика требуют быстрого научного и практического (прикладного) становления этого направления. Существующие научные разработки давно вышли за рамки обеспечения расследования преступлений в сфере компьютерной информации, назначения и производства сложных ком-

пьютерно-технических и иных судебных экспертиз. Сегодня отдельные отрасли криминалистической техники изучают и исследуют данные, обнаруженные на цифровых устройствах и связанные с совершением различных экономических и технических преступлений.

Криминалистические знания в этой сфере, в основном, базируются на понимании особенностей функционирования современных информационно-коммуникационных технологий и используются для выявления объективных закономерностей:

а) преступной деятельности, направленной на воспрепятствование нормальному функционированию информационных систем и их компонентов;

б) преступной деятельности, направленной на использование последних в качестве орудий или средств совершения иных преступлений; в) криминальной деятельности по созданию или изменению информации на электронных носителях, в информационно-телекоммуникационных сетях и т. д.

В основном учеными-криминалистами формировались правила и осуществлялись разраблевиотки:

а) по собиранию цифровой информации с выполнением технических процедур обеспечения ее юридической значимости;

б) по исследованию цифровой информации, сохраненной в отдельных информационных объектах, а также в информационной среде электронного носителя информации для нужд следствия;

в) по оценке полученных результатов, соотнесения их с действиями виновного и использования для квалификации преступного деяния и определения направления будущего следствия;

г) по интеграции цифровых доказательств в систему существующих судебных доказательств с соблюдением процессуальной формы их получения и т. д.

Это все в определенной степени позволяло обеспечивать расследование сложных и особо сложных преступлений (в техническом смысле), совершенных в сфере компьютерной информации. Возможности цифровых технологий, на наш взгляд, реализуются крайне недостаточно. Так, без внимания ученых-криминалистов осталось еще одно направление в развитии криминалистического обеспечения расследования преступлений – *это реализация такого метода познания как моделирование.*

Моделирование – общенаучный метод познания, используемый как в криминалистической науке, так и в следственной, экспертной и судебной практике, когда, например, прямое исследование фактов, происшедших в прошлом, затруднено. При моделировании для исследования объекта (явления) используется не сам объект (так как часто это не представляется возможным), а заменяющая его модель. Реализация данного метода познания заключается в построении и изучении модели каких-либо явлений, процессов, объектов или их системы для тщательного исследования.

Криминалистическая модель представляет собой искусственно созданную систему, воспроизводящую с определенной степенью сходства заменяемый ею объект, явление или процесс, связанный с исследуемым криминальным событием. Изучение и проверка модели позволяет получить новые знания об ориги-

нале и использовать их для решения поставленных перед правоохранительными органами задач по расследованию совершенных преступлений.

Моделирование при производстве предварительного расследования или судебного разбирательства используется для проверки имеющихся и получения новых доказательств, выдвижения и исследования криминалистических версий в тех случаях, когда непосредственное изучение объекта, явления или процесса, связанного с преступным событием, невозможно или нецелесообразно.

Поскольку использовать отсутствующие объекты или исследовать происшедшее в прошлом явление невозможно или нецелесообразно, следователь (иные участники уголовного процесса, судья) прибегает к моделированию. Приемы моделирования при расследовании различны: это мысленное моделирование, материальная реконструкция (обстановка места происшествия до совершения преступления), математическое моделирование, изготовление муляжей и слепков, воссоздание происшедшего явления и фиксация его с помощью фото-, кино-, видеосъемки и т. д.

Анализ следственно-судебной практики показал, что с первых минут расследования следователь сталкивается со сложностями, связанными со значительным дефицитом информации о событии преступления, его маскировкой, отсутствием данных о преступнике или потерпевшем и о многих иных обстоятельствах совершения преступления. Более того, модели, строящиеся на первоначальном этапе расследования, обычно содержат разрозненные сведения, изобилуют большим количеством пробелов. Только по мере проверки полученной информации о происшедшем событии они корректируются, уточняются и совершенствуются.

Сегодня набирает оборот прогрессивное компьютерное моделирование произошедшего крупного события (т.е. с тяжкими последствиями) – авиакатастрофа с человеческими жертвами, дорожно-транспортное происшествие со смертельным исходом, аварии на железнодорожном или водном транспорте и т. д.

Создание и изучение таких моделей способствуют проверке и получению новой информации; позволяют исследовать и объяснить связи между фактами и явлениями, способа совершенного преступления и образовавшимися последствиями, вскрыть взаимосвязь и взаимообусловленность между действиями как прямых, так и косвенных участников события и т. д.

Объектами компьютерного моделирования, на наш взгляд, могут быть различные криминальные обстоятельства, условия и состояния, которые, в целом, могут описать механизм конкретного совершенного преступления, отдельные его элементы, поведенческие акты преступника, потерпевшего и других участников произошедшего преступного события.

Источниками данной информации могут быть:

– следователь (в сознании которого сформировалась информационная модель механизма совершенного преступления);

– подозреваемый (в сознании которого имеется модель механизма будущего преступления, и информация по совершенным действиям);

– потерпевший и свидетель-очевидец (в сознании которых сохранилась информация о произошедшем криминальном событии);

– вещественные и иные доказательства (которые на себе несут информацию о совершенном преступлении и его участниках);

– эксперты и специалисты (которые выявили и закрепили доказательственную или дополнительную информацию о совершенном преступлении).

Компьютерная модель является моделью информационной. Она замещает недостающие звенья, пробелы в объяснении фактов, способствует отысканию доказательств и раскрытию неизвестного. Она упорядочивает полученную информацию в определенную систему и позволяет истолковывать и оценивать свойства и качества процесса, явления или объекта познания. При этом она является версионной, компьютерной моделью, поскольку допускает различное толкование данного объекта или явления.

Она способствует: а) выявлению неизвестных объектов и лиц, связанных с преступным событием, и их поведенческие акты; б) установлению событий, которые предшествовали, сопутствовали и последовали после преступления; в) установлению происхождения и связи между фактами, их временной и пространственной характеристик, устранению противоречий между фактами; г) определению направления поиска неизвестного и всего хода расследования и т. д.

Анализ следственной практики показал, чтобы обеспечить полное и всестороннее расследование, следователю необходимо обращаться, прежде всего, к компьютерной модели механизма совершенного и им расследуемого преступления. Она непосредственно знакомит его с конкретной обстановкой места происшествия, с поведенческими актами подозреваемого, потерпевшего и другими непосредственными участниками преступного события, с документами, вещами, отдельными объектов и предметами окружающей среды и т. д.

Модель раскрывает существо происшедшего события, его внутренние процессы взаимодействия и связь между фактами, она становится информационным фондом и тем средством, которое способствует установлению причинно-следственных и пространственно-временных связей между элементами механизма совершенного преступления. Это связано с тем, что компьютерное моделирование отталкивается от известных закономерностей механизма преступления более высокого уровня, определяющих характер взаимосвязей и взаимодействий различных элементов механизма преступления, а также от конкретных известных ему элементов, которые могут быть использованы в качестве деталей создаваемой модели.

Формирование целостной компьютерной модели механизма совершенного преступления поможет следователю (дознавателю) решить следующие задачи: объяснить факты, происшедшие явления, обладающие признаками преступления; дать уголовно-правовую оценку исследуемому событию и соответственно правильно квалифицировать деяния правонарушителя; установить и объяснить пространственно-временные и причинно-следственные связи в расследуемом событии; установить такие связи между действиями участников события и теми изменениями, которые произошли в материальной обстановке; установить и объяснить механизм следообразования; определить направление поиска известных или неизвестных материальных последствий, а по систематизированной криминалистически значимой информации – преступника, неустановленных свидетелей и

косвенных участников преступного события или потерпевшего; определить направление поиска похищенного имущества, вещественных доказательств и иных носителей криминалистически значимой информации о самом преступлении и его участниках; определить программу расследования на первоначальном, последующем, а затем и на заключительном этапе и ее тактику и т. д.

Необходимо отметить, что исходной точкой компьютерного моделирования механизма совершенного преступления является предварительный этап проверки материалов для решения вопроса о возбуждении уголовного дела или его отказе.

Начальная стадия компьютерного моделирования характеризуется следующими операциями: а) собирание, изучение, логическое упорядочение и мысленная переработка первичных фактических данных; б) выделение из имеющегося информационного фонда сведений, относящихся к отдельным элементам механизма преступления, обстановке, в которой совершено криминальное событие, и личности преступника и потерпевшего; в) построение системы версий об обстоятельствах содеянного и неизвестных внешних признаках преступника или потерпевшего; г) использование личных криминалистических знаний и опыта расследования аналогичных дел для построения мысленной модели механизма преступления; д) использование криминалистической характеристики данного вида (подвида) преступления; е) использование родовой типовой модели механизма или схожего преступления и т. д.

На основе разработанной компьютерной модели механизма совершенного преступления работники соответствующих правоохранительных органов (и с данным выводом ученых-юристов мы согласны) могут решать следующие задачи:

– по внешним признакам, изложенным в показаниях очевидцев и потерпевшего, по признакам способов совершения преступления, предмета посягательства, орудий и средств достижения преступного результата устанавливают преступника;

– организовывают техническое, оперативное, кадровое и информационное обеспечение планируемой деятельности по раскрытию и расследованию преступления;

– оценивают ход и результаты проделанной работы, принимают решение о направленности, содержании и характере работы на следующем этапе расследования и т. д.;

– получают новую информацию о самом преступлении или его участниках;

– моделируют личности неустановленных участников преступного события, предметов хищения, орудий и средств достижения преступного результата для их дальнейшего поиска;

– разрабатывают операции по поиску преступника, потерпевшего или очевидца преступления;

– уточняют программы собирания дополнительных данных о предмете доказывания, фактах, имеющих вспомогательное значение, и т. д.

УДК 004.056

ЧАСТНАЯ ЖИЗНЬ – НОВАЯ «НЕФТЬ»?

Левина Мария Ильинична
кандидат юридических наук, доцент
Национальный исследовательский университет «МИЭТ», Москва, Россия

Статья посвящена современным проблемам обладания и защиты персональных данных, права на частную жизнь.

***Ключевые слова**: персональные данные, неприкосновенность частной жизни, информационное законодательство, конфиденциальная информация.*

PRIVACY – «NEW OIL»?

Levina Maria Ilyinichna
candidate of law, associate Professor
National Research University of Electronic Technology (MIET) Moscow, Russia

The paper covers the issues of modern content privacy right and personal information, a person's right to own its personal data.

***Keywords**: personal data, privacy, privacy right, personal information, the legislation on information.*

Заголовок сегодня столь же банален, как и то, что со всеми нами происходит, – за последние 10–15 лет мы стремительно теряем свою частную жизнь.

Информационное законодательство [1, 2] гарантирует нам сохранность наших персональных данных, не говоря уже о конституционных и иных законодательных гарантиях права на частную жизнь. Верим ли мы сами в то, что наши данные неприкосновенны и хранятся в соответствии с законодательством?

Условный «Большой брат» знает о нас все: как и на что тратим свои деньги, куда ездим, что любим и не любим, чем интересуемся, каких врачей и как часто посещаем, сколько детей, как они учатся, какие кружки посещают, сколько тратим денег и минут на общение и с кем. Про банки и говорить не приходится. Сбербанк же, на наших глазах превращающийся в гигантскую технологическую платформу, клиентами которого являются миллионы, уж точно знает все о своих клиентах, а будет знать еще больше. При этом Большой брат – это не только и не столько государство, которое не настолько расторопно, как крупнейшие технологические платформы и корпорации.

Мы имеем дело с двумя взаимосвязанными, но различными понятиями: правом на частную жизнь и персональными данными.

Традиционное представление о праве на частную жизнь включает в себя ряд прав, обеспечивающих личную, индивидуальную свободу человека, неприкосновенность его частной жизни. Частная жизнь человека определяется как «физическая и духовная сфера, которая контролируется самим индивидом» [3, с. 146].

Неприкосновенность частной жизни рассматривается как один из аспектов индивидуальной свободы человека. Сама ее неприкосновенность заключается в том, что законодательство не только не может вторгаться в эту сферу, но и должно ограждать от таких вторжений в частную жизнь как со стороны государства, так и любого лица – физического или юридического.

Однако ни одно право не является абсолютным и подлежит ограничениям. Ограничения права на неприкосновенность частной жизни устанавливаются Конституцией РФ, федеральными законами, судебными решениями и нормами международного права.

В российской Конституции данному праву посвящены по крайней мере две статьи – 23 и 24, которые делают право на частную жизнь зонтичным сразу для нескольких прав. Право на неприкосновенность частной жизни конкретизировано – к нему относятся личная и семейная тайна, защита части и доброго имени (ч. 1 ст. 23 Конституции РФ). К ним добавляются права на тайну переписки, телефонных переговоров и разного рода сообщений – почтовых, телеграфных и иных (ч. 2 ст. 23 Конституции РФ). Подрастающему цифровому поколению наверно трудно представить, что речь идет об обычной почте, а не электронной (которая для этого поколения также порядком устарела). Помимо электронной почты можно смело причислить разнообразные мессенджеры и социальные сети.

Значение прав, закрепленных в ст. 23 Конституции РФ подтверждается конституционным положением ст. 56, предусматривающим ограничение прав в условиях чрезвычайного положения. В соответствии со ст. 56 Конституции РФ право на неприкосновенность частной жизни не может быть ограничено даже в условиях чрезвычайного положения.

Ст. 24 Конституции РФ содержит запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

Когда Конституция РФ принималась, смысл указанных положений был понятен. Формулировка этих положений – это не только норма закона, имеющего высшую юридическую силу конституционного положения, но и важнейшая этическая норма, складывающаяся в течение многих веков.

В условиях происходящей (произошедшей?) цифровой революции зачастую мы вступаем в отношения, которые законом не регулируются, но нуждаются в регулировании законом и защите со стороны государства (хотя бы в силу требований статей 23 и 24 Конституции РФ. Вместе с тем, ст. 24 предусматривает согласие лица на распространение его информации и информации о нем.

Сбор и обработка персональных данных стали уже привычными, как привычны видеонаблюдение крупных транспортных узлов, общественных мест, школ, а также анкетирование на сайтах интернет-магазинов и служб доставки. Все это удобно и безопасно, но есть существенные минусы в виде утечек данных. Ответственность за сохранность данных о себе несет, в первую очередь, обладатель этих данных. Защита от проникновения в частную жизнь зависит от знаний и умений каждого отдельного лица технически защитить свою информацию в киберпространстве. При этом обладатель данных и носитель этих данных не всегда совпадают в одном лице.

Еще на памяти скандал с Facebook в США, когда компания была оштрафована на 5 млрд долларов за утечку данных 87 млн. пользователей [4]. В России памятны также скандалы со Сбербанком, РЖД, но неизвестно, привлечены ли виновные к ответственности. Все эти скандалы только подчеркивают, насколько беззащитными могут оказаться пользователи социальных сетей и не только они. В России преступления против неприкосновенности частной жизни не рассматриваются как общественно-опасные.

Новый министр связи, Максут Шадаев 27 января 2020 г. выступил на заседании рабочей группы Госсовета по направлению «Коммуникации, связь, цифровая экономика». Согласно презентации, к 2024 г. все уполномоченные сотрудники, ведущие оперативно-розыскную деятельность, смогут получить доступ к различным типам данных о гражданах в режиме онлайн. Речь идет о государственных данных, данных банков, операторов мобильной связи и интернет-сервисов. Доступ к другим типам данных правоохранительные органы получают по-разному, в том числе по решению суда. Такое решение, нужно, например, для получения доступа к записям телефонных переговоров, электронной почте, смс, сообщениям в мессенджерах и т. п. Оно же требуется для получения банковской информации, например, о движении средств по счетам и остатку по ним у физлица [5]. При этом, одни юристы считают, что что воплотить инициативу Шадаева об онлайн-доступе без изменения законодательства и Конституции невозможно. Другие уверены, что это возможно, т.к. ограничение конституционных прав возможно в силу статьи 55 Конституции в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства

Для борьбы с киберпреступностью многие страны обновляют технологические решения и законодательные меры, которые, как правило, носят превентивный характер. Речь в основном идет о борьбе с неправомерным получением и использованием данных посредством минимизации их сбора. В частности, законы запрещают бизнесу и некоторым государственным структурам собирать, хранить и использовать биометрические данные граждан без их согласия. В ЕС действует регламент GDPR, который защищает все данные человека (в том числе фотографии) и предусматривает их использование и обработку только в случае оказания медицинской помощи или угрозы национальной безопасности, т.е. только с согласия суда и спецслужб [6].

Человек, озабоченный действительной неприкосновенностью своей частной жизнью, может и не пользоваться социальными сетями или пользоваться ими крайне осторожно. Это может не понравиться банкам (например, при выдаче кредита) или потенциальным работодателям, «охотникам за головами» (собирающим цифровые следы) или кому-то еще.

Все цифровые информационные отношения, в которые мы вступаем в каждом отдельном случае регулируются значительным количеством самых разнообразных норм. К сожалению, по отдельности и все вместе они не обеспечивают в необходимой мере неприкосновенность частной жизни и личной информации. Цифровые информационные правоотношения, связанные с обеспечением неприкосновенности частной жизни регулируются двумя основными федеральными законами «О персональных данных» и «Об информации, ин-

формационных технологиях и защите информации». Они содержат термины, которые являются ключевыми для защиты неприкосновенности частной жизни и личной информации. Первый из законов раскрывает понятие «персональные данные», которое трактуется как любая информация, прямо или косвенно относящаяся к субъекту персональных данных (п. 1 ст. 3).

Второй закон дает легальное определение конфиденциальной информации. Здесь под конфиденциальной информацией понимается обязанность лица, имеющего доступ к такого рода информации, не передавать ее третьим лицам без согласия ее обладателя (п. 7 ст. 2). Остается напомнить только, что цель Федерального закона «О персональных данных» заключалась, среди прочего, в защите права на неприкосновенность частной жизни, личной и семейной тайны при обработке данных (ст. 2).

Трактовки этих понятий, достаточные в веке прошлом, уже недостаточны в веке нынешнем, хотя оба закона постоянно обновляются. Эти и другие трактовки не только не позволяют лицу защитить информацию о себе. Они позволяют без ведома субъекта, с формального согласия (а иногда и без формального согласия) использовать информацию в коммерческих целях.

Рынки пользовательских данных, в том числе и нелегальные, уже вполне сформировались, сложились тарифы на «пробивки на заказ». Ни для кого не секрет, что любые личные данные можно купить на соответствующих сайтах и платформах: паспортные данные, информацию о перемещениях по городу, детализацию телефонных разговоров и даже кодовое слово банковской карты.

Поставщики информации – рядовые сотрудники салонов связи, отделений банков, работники, налоговой, полиции. Кроме того, существенным источником утечек персональных данных является государство и связанные с ними организации. Еще одним существенным источником утечек персональных данных являются социальные сети и такие цифровые монстры как Гугл, Амазон, Яндекс и др.

Федеральный закон «Об информации, информационных технологиях и защите информации» дает государственным органам, банкам и иным организациям собирать, среди прочего, биометрические данные гражданина РФ (п. 2 ст. 14.1) и взимать плату за предоставление государственным органам и организациям этих сведений (п. 24 ст. 14.1).

В России государство в ряде случаев может обрабатывать биометрические данные без письменного согласия гражданина, в том числе если гражданин подозревается в угрозе безопасности, совершении коррупционных действий, а также если это происходит в государственных и общественных интересах. Очевидно, система распознавания лиц в Москве будет собирать данные в публичных местах и сможет предоставлять их различным службам в случае правонарушений, спорных ситуаций и проч. В таком случае решение направлено на обеспечение безопасности граждан и не противоречит закону. При этом безопасность обеспечивается в только том случае, если понятие «общественные и государственные интересы» не трактуется слишком широко и неопределенно.

Несомненно, в законах остается и будет оставаться много спорных моментов, т. к. сфера биометрических данных слишком нова, слишком быстро развивается технологически, слишком непредсказуема траектория ее развития.

Поэтому юридические нормы будут отставать, а правоприменительная практика – находиться в состоянии формирования.

Главная же проблема как правового регулирования, так и правоприменительной практика заключается в неопределенности *собственника* информации. Федеральный закон «Об информации, информационных технологиях и защите информации» содержит лишь определение *обладателя* информации как лица, самостоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (п. 5 ст. 2). За статус *собственника* информации и разворачивается сегодня борьба между государством, бизнесом и частными лицами. Частное лицо в этой борьбе далеко от выигрыша – слишком многое стоит на кону. Тот, кто обладает данными, большими данными, персональными данными – обладает конкурентным преимуществом, т.к. обладает информацией о клиентах. Эта информация принадлежит не клиентам, а банкам и другим организациям. И у государства, и у бизнеса есть системы, собирающие персональные данные. В Москве уже появилась сеть городского видеонаблюдения, опознающая лица людей.

Человек может самостоятельно попытаться минимизировать возможности утечки своих данных, в том числе ограничивая их предоставление там, где это не нарушает закона. Важно понимать, что сегодня ценность персональных данных, которые мы, часто не задумываясь, раздаем устройствам, сервисам и структурам, возрастает с каждым днем.

Вопрос о собственности на информацию о себе становится только насущней. Если собственником становится государство и (или) бизнес мы окончательно расстаемся с нашей частной жизнью и правом на нее. Если обязать государственные структуры и бизнес (в первую очередь, банки и технологические платформы, ядром которых все равно являются банки) передавать по запросу частного лица любую информацию любым организациям, то это меняет расстановку сил и наносит удар по монополиям.

Библиографический список

1. Федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 02.12.2019) «Об информации, информационных технологиях и о защите информации» // СПС Консультант Плюс.

2. Федеральный закон от 27.07.2006 № 152-ФЗ (в ред. от 31.12.2017) «О персональных данных» // СПС Консультант Плюс.

3. Права человека: учебник для вузов / отв. ред. Е.А. Лукашева. – М.: НОРМА-ИНФРА, 1999. – 573 с.

4. Юдников А. Больше данных, меньше утечек / А. Юдников // Ведомости. – URL: https://www.vedomosti.ru.

5. Максим Шадаев предлагает открыть персональные данные граждан силовикам // Ведомости. – URL: https://www.vedomosti.ru.

6. Юдников, А. Больше данных, меньше утечек / А. Юдников // Ведомости. – URL: https://www.vedomosti.ru.

УДК 343.14

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ

Луценко Павел Александрович
кандидат юридических наук, доцент
Спесивцев Д. О.
Воронежский ГАУ, Воронеж, Россия

В настоящее время доказательства являются основой для разрешения дела как гражданском, так и уголовном судопроизводстве. Помимо доказательств на бумажном носителе существуют и электронные источники доказательств, и на современном этапе развития они набирают все большую и большую популярность. Тем не менее от письменных доказательств никто не собирается отказываться, так как для большинства людей они являются более стандартными.

***Ключевые слова**: электронные доказательства, уголовный процесс, относимость, допустимость.*

ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Lutsenko Pavel Alexandrovich
candidate of law, associate Professor
Spesivtsev D. O.
Voronezh state agricultural university*, Voronezh, *Russia

Currently, evidence is the basis for resolving the case in both civil and criminal proceedings. In addition to paper evidence, there are also electronic sources of evidence, and at the present stage of development, they are gaining more and more popularity. However, no one is going to refuse written evidence, since for most people it is more standard.

***Keywords**: electronic evidence, criminal procedure, relevance, admissibility.*

Тематика научной работы обусловлена тем, что в наше время получают наибольшее распространение электронные источники доказательств в судебных заседаниях, что послужило безусловным интересом рассмотрения данного вопроса. В современной юридической науке тема цифровых доказательств обсуждается уже давно. Различные ученые уже долго пытаются разъяснить, каким же образом возможно применение цифровых доказательств. На данный момент множество федеральных законов содержат в себе такие понятия, как «электронный ресурс», «электронный документ», «электронная почта» и т. д. Однако также многие специалисты выступают против таких видов доказательств, аргументируя тем, что это подразумевает под собой ненадежный формат, лично мое мнение состоит в том, что здесь можно выделить как массу плюсов, так и минусов, и для того чтобы внедрить такой институт в действующую систему, необ-

ходимо провести огромную работу и предусмотреть все риски. В рамках статьи невозможно будет провести анализ, чтобы выявить – все же пользу понесет такой формат доказательств или скорее отрицательный эффект, но мы постараемся рассмотреть, как можно подробнее это нововведение и провести параллели и сделать вывод о том, полезнее ли будет внедрение этих доказательств в систему или же нет, а самое главное, будет ли это эффективно в борьбе с преступностью.

Хотелось бы начать с того, что такой новый формат как электронные ресурсы можно бесспорно внедрить в систему оповещения судами граждан, попробую это аргументировать, безусловно, такой процесс сэкономит кучу времени и сил работникам судов, так как уже люди будут оповещаться о новых заседаниях либо еще какой то информации заходя в свою электронную почту, а не проверяя свой почтовый ящик, этот процесс также может и ускорить процесс получения писем, плюсов от этого я считаю гораздо больше чем минусов так как этот новый формат будет полезен обеим сторонам, в свою очередь работники будут тратить меньше сил а получатели будут экономить время, ведь для того чтобы зайти на электронную почту достаточно 5 минут. Помимо этого, можно улучшить такой аспект взаимодействия между людьми как ответственность, например, при явке в суд гражданин будет обязан ознакомиться и подписать документ в котором будет сказано, что о дальнейшем заседании суда ему будет известно по электронной почте и если он проигнорирует, то к нему будут применены санкции.

Теперь по поводу именно электронных доказательств в суде, так как прогресс не стоит на месте и развивается не только различные судебные системы также развивается и жизнь обычных людей которая становится взаимосвязана с интернетом, в свою очередь некоторая часть преступления в том числе может протекать и в сети интернет от чего можно сделать вывод что новые электронные доказательства могут заметно помочь в раскрытии таких преступлений и тем самым выступать как модель предотвращения новых, так как люди будут понимать что в сети интернет невозможно что то скрыть и если будет совершен противоправный поступок его можно будет с легкостью раскрыть. В тоже время необходимо обратить внимание на то что при изъятии обнаружении и поиске информации необходимо руководствоваться международными принципами так как часто может возникнуть такая ситуация что изъятие какой либо информации может нарушать право гражданина на свободу переписки и т. д. Могу привести пример, из личных показаний гражданина Гуриева бывшего главы РЭШ, было известно о том, что следователем в плане приобщений электронных материалов к делу, а именно электронных писем, было нарушено право личной переписки, о чем в последующем было множество споров, каким же образом возможно обойти нарушение чьих-либо прав.

Гаврилина Ю.В. говорит «что для достижения целей уголовного процесса правовой режим электронных носителей нужно распространять не только на съемные носители информации но и на персональные компьютеры и серверы, что позволит избежать терминологической чехарды» По моему мнению, это тоже бу-

дет играть заметную роль в том плане, что если рассмотреть все вопросы, связанные с тем, каким образом изъять информацию, необходимо и обозначить уже в самом судебном заседании все механизмы, связанные с этим процессом, а именно нужна будет своя база по таким вопросам, которые пересекаются с информационными преступлениями, необходимо грамотное юридическое закрепление терминов в законе, что может составить некоторые сложности.

Также необходимо указать о «скриншоте» – это такой новый вид доказательства, который часто встречается в делах об административных правонарушениях, могу привести пример, решение Арбитражного суда Забайкальского края от 30.03.2017 по делу № А78-1667/2017. В данном судебном споре был рассмотрен случай, когда оператор связи был привлечен к ответственности, поскольку оператор связи не ограничивает доступ к запрещенному информационному ресурсу. И в качестве доказательств правомерного привлечения к административной ответственности суд принял скриншот электронной страницы.

Согласно части 1 статьи 26.2 КоАП Российской Федерации, доказательствами по делу об административном правонарушении являются любые фактические данные, на основании которых судья, орган, должностное лицо, в производстве которых находится дело, устанавливают наличие или отсутствие события административного правонарушения, виновность лица, привлекаемого к административной ответственности, а также иные обстоятельства, имеющие значение для правильного разрешения дела. Таким образом, скриншоты подтверждают наличие события административного правонарушения.

Еще одним приложением, которое используют компании и физические лица, является WhatsApp. В Решении Арбитражного суда Республики Карелия от 19.09.2016 по делу №А26-4401/2016 юридическое лицо признано виновным в совершении административного правонарушения, предусмотренного частью 4 статьи 15.25 КоАП РФ. Действия его квалифицированы как невыполнение участником юридического лица в установленный срок обязанности по получению на свои банковские счета в уполномоченном банке иностранной валюты. Юридическое лицо привлечено к административной ответственности в виде штрафа.

Также, принимая во внимание обстоятельства дела, степень общественной опасности совершенного правонарушения и характер данного деяния, суд считает необходимым применить положения, которые изложенные в пункте 2 Постановления Конституционного суда Российской Федерации от 25.02.2014 № 4-П и снизить административную санкцию ниже низшего предела.

Таким образом, Skype и WhatsApp в совокупности с другими доказательствами признаются в качестве допустимых.

Применение электронных доказательств, все больше находит отражение в судебной практике, но для ежедневного применения электронных доказательств необходимо внесение надлежащих поправок в нормативно-правовые акты. Таким образом, можно подвести итог вышесказанному, безусловно, электронные доказательства – это серьезный шаг к созданию нового института доказательств, что облегчит в свою очередь работу многим должностным лицам и

вероятнее всего поднимет процент раскрытия преступлений. Также это необходимо изучить глубже, чтобы выявить все проблемы, с которыми есть шанс столкнуться и предотвратить их на начальном этапе внедрения такого института. Можно сказать, что уголовно правовая форма приобретает изменения и любое законодательство должно идти в ногу со временем, тем самым необходимо сказать, что необходимо изучать эту изменяющуюся правовую форму, изменение которой вызвано не только открытием новых доказательств, но и внедрением новых технологий в систему расследования преступлений и рассмотрения уголовно правовых споров.

Библиографический список

1. Конституция Российской Федерации. Принята всеобщим голосованием 12 декабря 1993 г. (с учетом поправок, внесенных законами РФ, о поправках к Конституции РФ от 30.12.2008 №7 ФКЗ, от 21.07.2014 № 11 ФКЗ) // Собрание законодательства РФ. – 2014. – № 31. – Ст. 439.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2019) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

3. Бастрыкин, А. И. Уголовное право России / А. И. Бастрыкин, А. В. Наумова. – М., 2017. – 102 с.

4. Батычко, В. Т. Уголовное право / В. Т. Батычко. – Таганрог: ИТА ЮФУ, 2015. – 345 с.

5. Козаченко, И.Я. Уголовное право: учебник / отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 4-е изд. – М.: Норма, 2017. – 1008 с.

6. Решение Арбитражного суда Республики Карелия от 19.09.2016 по делу № А26-4401/2016 // URL: www.consultant.ru.

7. Решение Арбитражного суда Забайкальского края от 30.03.2017 по делу № А78-1667/2017 // URL: www.consultant.ru.

УДК 340:004

К ВОПРОСУ О ПРАВОВОЙ ИНФОРМАТИЗАЦИИ

Наумкина Валентина Владимировна
доктор юридических наук, доцент
ФГБОУ ВО «Хакасский государственный университет им. Н.Ф. Катанова», Абакан, Россия

Информатизация процессов и использование цифровых технологий используется в различных сферах жизнедеятельности. В статье рассматриваются вопросы использования информационных технологий в юриспруденции. Выделяются направления и специфика цифровизации. Проводится анализ исключения субъективного фактора.

Ключевые слова: *цифровые технологии, информатизация, правовая цифровизация.*

ON THE ISSUE OF LEGAL INFORMATIZATION

Naumkina Валентина Владимировна
Doctor of law, associate Professor
Khakassia state University, Abakan, Russia

Informatization of processes and the use of digital technologies is used in various spheres of life. The article deals with the use of information technologies in law. The directions and specifics of digitalization are highlighted. The analysis of the exclusion of the subjective factor is carried out.

Keywords. *Digital technologies, Informatization, legal digitalization*

Информатизация и цифровые технологии стали широко использоваться в различных сферах жизнедеятельности [7, с. 140], в качестве инструмента автоматизации типовых задач. Автоматизация позволяет ускорить документооборот и исключить технические ошибки. Цифровые технологии имеют большой потенциал для социально-экономического развития государства [8, с. 9; 9, с. 71]. В сфере юриспруденции цифровые технологии широко используются во многих развитых странах [4; 10], положительный опыт привел к распространению технологий и в Российской Федерации.

Понятие «правовая информатизация» стало использоваться в начале 90-х годов. Указом Президента Российской Федерации от 28 июня 1993 г. № 966 «О концепции правовой информатизации России» правовая информатизация была отнесена к важным факторам развития демократического правового государства [1]. К направлениям правовой информатизация были отнесены: информатизация правотворческой деятельности; информатизация правореализационной деятельности; правовое обеспечение процессов информатизации. Первоначально под информатизацией понималась доступность информации и гласность результатов деятельности органов. В настоящее время информатизация охватывает процесс, или действия органов власти.

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы информатизация рассматривается как средство оптими-

зации предоставления товаров и услуг [2]. Несомненно, автоматизация услуг является преимуществом. Цифровизация, несомненно, ускоряет процессы, может использоваться для экономии времени и эффективного использования трудовых ресурсов. При этом не все процессы можно автоматизировать и перевести в цифровое поле.

В качестве основных сфер применения цифровых технологий в праве можно выделить: автоматизацию документооборота, юридических действий [8, с. 10; 5, с. 30] и следственных действий [4], информатизацию правотворческой деятельности [12], цифровое судопроизводство [3].

Правовая информатизация является ближайшим будущим. При этом исключение участия человека может иметь как положительные, так и отрицательные стороны. Автоматизация приводит к исключению коррупционной составляющей и возможности повлиять на результат. Автоматизированные процессы являются «прозрачными» и однообразными независимо от участников процесса. Стандартизация действий исключает корыстный интерес. При этом автоматизированная система (программа) не может учитывать всех нюансов ситуации. Действия программы являются предсказуемыми, поэтому можно «просчитать» слабые места программы и получить желаемый результат зная алгоритм действий.

Степень цифровизации должна зависеть от сферы применения. Например, использование в подготовке локальных актов, договоров, инструкций и так далее позволяет эффективно использовать специалистов. Что касается следственных действий или принятие судебных решений в данных сферах информатизация может иметь ограниченное использование. Человек способен гибко реагировать на ситуацию, оценить мотивацию поступка и т. д. При внедрении технологий нельзя ставить знак равенства между цифровизацией процесса и использованием цифровых технологий для частичной автоматизации процесса.

Правовая информатизация требует наличия специально подготовленных специалистов [3, с. 175; 14, с. 568], владеющих компьютерными технологиями. Кадровое обеспечение является еще одной проблемой информатизации. Программное обеспечение динамично развивается, поэтому юрист должен обладать способностью совершенствовать свои навыки. В настоящее время на направлении «юриспруденция» информатика изучается на уровне общекультурного развития. Изучение специальных программ, которые используются на практике (например, нотариусами, органами государственной власти и т. д.) не входит в программу изучения и не доступны для студента. Доступ к специализированным программам ограничен, поэтому даже в период прохождения практики у студента нет возможности ознакомиться с программным обеспечением. Профессиональная мобильность предполагает наличие специфических качеств личности [6, с. 88], правового урегулирования использования информационных технологий в образовании [12], разработки отдельных теоретических аспектов такого использования [11].

Правовая информатизация требует четкого определения границ внедрения цифровых технологий для обеспечения оптимального баланса между автоматизацией и использованием индивидуального подхода. Кроме того, информатизация не возможна без подготовки кадров, обладающих необходимыми компетенциями.

Библиографический список

1. Указ Президента РФ от 28 июня 1993 г. № 966 «О концепции правовой информатизации России» // Собрание актов Президента и Правительства Российской Федерации от 5 июля 1993 г. № 27. Ст. 2521.

2. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС Гарант.

3. Бертовский, Л. В. Цифровое судопроизводство: проблемы становления / Л. В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства: сб. мат-лов междунар. науч.-практ. конф. – М., 2018. – С. 173–178.

4. Бирюков, П. Н Искусственный интеллект и «предсказанное правосудие» / П. Н. Бирюков // Lex Russica. – 2019. – № 11 (156). – С. 79–87.

5. Грищенко, Г. А. Возможности применения технологий искусственного интеллекта в юриспруденции / Г. А. Грищенко // Инноватика и экспертиза: науч. тр. – 2019. – № 1 (26). – С. 27–33.

6. Карелина, Н. А. Подготовка профессионально мобильных кадров для цифровой экономики / Н. А. Карелина // Проблемы педагогики. – 2019. – № 6 (45). – С. 88–89.

7. Курбатова, С. М. Правовые основы системы государственного информационного обеспечения в сфере сельского хозяйства. / С. М. Курбатова, Л. Ю. Айснер // Аграрное и земельное право. – 2018. – № 6 (162). – С. 139–142.

8. Луканов, А. С. Современный информационные технологии как инструментарий правой системы государства / А. С. Луканов // Юридический вестник Самарского университета. – 2017. – Т. 3, № 3. – С. 9–12.

9. Рахинский, Д. В. Информационные технологии как ресурс развития человека / Д. В. Рахинский // Человеческие ресурсы как важнейший фактор в развитии экономики региона: тез. докл. науч.-практ. конф. – Красноярск, 2000. – С. 71.

10. Сапожников, А. А. Будущее искусственного интеллекта в юриспруденции / А. А. Сапожников // Проблемы управления, экономики, политики и права в глобализирующемся мире: сб. докл. Фестиваля науки ЮРИУ РАНХиГС. – М., 2019. – С. 248–252.

11. Трашкова, С. М. Некоторые теоретико-правовые аспекты по использованию информационных технологий в образовании / С. М. Трашкова // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. науч.-практ. конф. / отв. за вып. В. Л. Бопп. – Красноярск, 2016. – С. 82–84.

12. Трашкова, С. М. Основы правового регулирования использования информационных технологий в образовании / С. М. Трашкова // Инновационные тенденции развития российской науки: мат-лы IX междунар. науч.-практ. конф. / отв. за вып. В.Л. Бопп. – Красноярск, 2016. – С. 27–30.

13. Шарыпова, Т. Н. Информатизация правотворческой деятельности / Т. Н. Шарыпова, Т. Ш. Чомаев // Аллея науки. – Т. 1, № 3 (30). – 2019. – С. 531–533.

14. Халин, В. Г. Подготовка кадров для цифровой экономики России: состояние, проблемы и перспективы / В. Г. Халин, Г. В. Чернова // Устойчивое развитие: общество и экономика: мат-лы VI Междунар. науч.-практ. конф. – 2019. – С. 568–572.

УДК 343.148

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

Омельянюк Георгий Георгиевич
доктор юридических наук, доцент
заместитель директора ФБУ РФЦСЭ при Минюсте России,
профессор кафедры судебно-экспертной деятельности ФГАОУ ВО РУДН,
профессор кафедры цифровой криминалистики МГТУ им. Н.Э. Баумана,
Москва, Россия
Усов Александр Иванович
доктор юридических наук, профессор
первый заместитель директора ФБУ РФЦСЭ при Минюсте России, профессор кафедры судебно-экспертной деятельности ФГАОУ ВО РУДН, профессор кафедры цифровой криминалистики МГТУ им. Н.Э. Баумана, член AAFS,
Москва, Россия

Потребности современного судопроизводства диктуют необходимость модернизации форм использования специальных знаний. Прежде всего, это касается ее основной формы – судебной экспертизы и всех видов обеспечения судебно-экспертной деятельности, в том числе научно-методического, информационного, кадрового, организационного, финансового обеспечения, а также формирования системы менеджмента качества судебно-экспертных организаций.

Ключевые слова: *специальные знания, судебная экспертиза, судопроизводство, информационные технологии, цифровизация.*

ACTUAL PROBLEMS OF DEVELOPMENT OF JUDICIAL-EXPERT ACTIVITY

Omelyanyuk George Georgievic
Doctor of legal Sciences, associate Professor, Deputy Director of the Federal center of forensic expertise under Ministry of justice of Russia, Professor of the Department of forensic activities RUDN, Professor of digital forensics The Bauman Moscow State Technical University, Moscow, Russia
Usov Alexander Ivanovich
Doctor of legal Sciences, Professor, first Deputy Director of the Federal center of forensic expertise under Ministry of justice of Russia, Professor of the Department of forensic activities RUDN, Professor of digital forensics The Bauman Moscow State Technical University, Moscow, Russia

The needs of modern legal proceedings dictate the need to modernize the use of special knowledge. First of all, this applies to its main form - forensic examination

and all types of forensic support, including scientific, methodological, informational, personnel, organizational, financial support, as well as the formation of a quality management system for forensic organizations.

***Keywords**: special knowledge, forensic science, legal proceedings, information technology, digitalization*

Актуальными проблемами развития судебно-экспертной деятельности на современном этапе являются:

– совершенствование и гармонизация законодательства в сфере судебно-экспертной деятельности,

– обеспечение единого научно-методического подхода к использованию специальных знаний в различных видах судопроизводства,

– развитие инновационных механизмов повышения качества и снижения сроков судебно-экспертного производства;

– стандартизация судебно-экспертной деятельности в национальном, региональном и международном форматах.

Потребности современного судопроизводства диктуют необходимость модернизации форм использования специальных знаний. Прежде всего, это касается ее основной формы – судебной экспертизы и всех видов обеспечения судебно-экспертной деятельности, в том числе научно-методического, информационного, кадрового, организационного, финансового обеспечения, а также формирования системы менеджмента качества судебно-экспертных организаций.

Современный этап совершенствования судебно-экспертной деятельности Российской Федерации связан с ее переводом на новый перспективный уровень использования специальных знаний, гармонизированный с лучшими мировыми практиками. Очевидным также является то, что именно экспертные технологии сегодня являются основным каналом применения современных достижений науки и техники в судебном процессе. Основная цель указанных процессов сопряжена с вопросами повышения качества и снижения сроков судебно-экспертного производства.

В целях совершенствования судебно-экспертной деятельности в Российской Федерации ожидается принятие нового федерального закона «О судебно-экспертной деятельности в Российской Федерации», который будет гармонизирован с процессуальным законодательством и введет в действие ряд инновационных механизмов государственного регулирования судебно-экспертной деятельности.

Особой проблемой является отсутствия гармонизации терминологии и методологии в зарубежной (прежде всего имеется ввиду - дальнее зарубежье) и отечественной методологии судебной идентификации. Основные труды, на которые в свои дискуссиях, прежде всего, ссылаются современные западные ученые (например, работы Поля Л.Кирка «The Ontogeny of criminalistics» (Онтогенез криминалистики), Тона Бродерса «Principles of Forensic Identification Science (Принципы судебно-экспертной идентификации), Д. Мюли «Forensic Individualisation from Biometric Data (Судебно-экспертная индивидуализация на

основе биометрических данных), труды профессоров Квана, Франко Тарони, Яна Эветта, Колина Аткина и др., к сожалению, практически не известны нашим ученым и практикам. Поэтому весьма своевременным представляется преодоление этой проблемы, сближение разных научных и практических школ судебной экспертизы в современном мире [1].

В 2016 году в США опубликован доклад «Судебная экспертиза в уголовных судах: обеспечение научной достоверности методов сопоставления признаков» (Forensic Science in the Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods), подготовленный Комитетом советников по науке и технике (далее – PCAST) при президенте США. PCAST пришел к выводу, что в настоящее время в судебной экспертизе заслуживают особого внимания две проблемы: (1) необходимость достижения четкой ясности в отношении научных стандартов, применяемых для оценки достоверности и надежности судебно-экспертных методов и (2) возможность оценки конкретных судебно-экспертных методов на предмет их научности и достоверности.

Принцип состязательности, который лежит в основе судопроизводства большинства развитых стран, предполагает открытую конкуренцию позиций (версий) сторон в процессе доказывания. Применительно к доказательствам, полученным в результате производства судебных экспертиз, реализация данного принципа, сводящаяся к представлению сторонами конкурирующих заключений эксперта, не показала своей эффективности.

Современное российское судопроизводство также осуществляется на основе принципов состязательности и равноправия сторон. Например, уголовно-процессуальное законодательство предусматривает при производстве по уголовному делу доказывание не только обстоятельств, подтверждающих преступность и наказуемость деяния, но и исключающих эти обстоятельства. В связи с этим в настоящее время продолжается изучение вопросов использования байесовских методов, включая применение концепции отношения правдоподобия, для интерпретации и оценки результатов судебно-экспертного исследования [2].

Полагаем, что в отечественной судебной экспертологии назрела крайняя необходимость формирования частной теории оценки неопределенности результатов экспертного исследования, включающей в себя категорию отношения правдоподобия и нацеленной на установление достоверности полученной информации об объекте экспертизы. Представляется, что дальнейший теоретический анализ и адаптация положений указанного выше издания внесут свой существенный вклад в инновационный путь развития российской судебно-экспертной науки, оно будет востребовано не только ученым и практиками в области судебной экспертизы и в целом сферы правоприменения, но и в смежных областях, таких как обеспечение качества результатов испытаний, аккредитация судебно-экспертных лабораторий и др.

На европейском пространстве в рамках деятельности Европейской сети судебно-экспертных учреждений (ENFSI), членом которой с 2005 года является ФБУ РФЦСЭ при Минюсте России, ведущие зарубежные ученые заявляют, что

концепция отношения правдоподобия является логически наиболее подходящей основой для оценки результатов судебно-экспертного исследования. В результате многолетних исследований международной группой европейских ученых было подготовлено Руководство ENFSI по оценочной отчетности в судебной экспертизе (ENFSI Guideline for Evaluative Reporting in Forensic Science. Strengthening the Evaluation of Forensic Results across Europe). В 2015 году Руководство было принято и опубликовано ENFSI в качестве нормативно-методического документа, представляющего собой практическое пособие по оценке экспертами доказательственной значимости выводов, получаемых ими в результате проведения исследований в конкретных видах судебной экспертизы, а также рекомендаций по оформлению результатов такой оценки в рамках так называемого оценочного отчета. В настоящее время данный документ носит обязательный характер для судебно-экспертных организаций Европейского Союза. Учитывая теоретический и практический интерес к данному документу в ФБУ РФЦСЭ при Минюсте России была проведена научно-методическая работа по подготовке его комментированного перевода в виде соответствующего издания [3].

Следующей примечательной чертой сегодняшнего дня является цифровизация все сфер деятельности, отличающаяся глобальным проникновением во все жизненные процессы. Данная область характеризуется с одной стороны высокой латентностью преступлений, а с другой сверхтехнологичной спецификой совершаемых деяний. Новые способы совершения преступлений требуют адекватной реакции всех институтов, использующих инструментарий различных компьютерных знаний. Преступления в сфере компьютерной информации, а также и многие другие составы преступлений, сопряженных с компьютерными технологиями, требуют активного развития судебной компьютерно-технической экспертизы со всеми возможными ее специализациями. Особого упоминания в аспекте судебной экспертизы заслуживают объекты компьютерной имитации, которые, как правило, не относятся к информационно-технологическим (компьютер, программы, информация, сети), а имеют другую природу (стандартные документы, изображения печатей и штампов, имитация письменных текстов, показаний аналитических приборов, фонограммы, фотоснимки, видеозаписи и пр.). Объекты компьютерной имитации могут быть предметом исследования различных видов экспертиз, например, судебно-технической экспертизы документов, судебной почерковедческой экспертизы, криминалистической экспертизы материалов, веществ и изделий и пр. Однако при подобных исследованиях эксперты могут констатировать только отклонения выявленных особенностей объектов экспертизы от подлинных объектов. В тех случаях, когда ставится вопрос о способе имитации (например, возможности использования высокоточного графопостроителя при имитации подписи) необходимо организовывать комплексные исследования с участием экспертов инженерно-технической специализации.

Одним из таких примеров, демонстрирующих возможности судебной экспертизы, являются результаты рассмотрения межгосударственной жалобы

«Грузия против России (II)» в Европейском суде по правам человека, обстоятельства которой касаются событий вооруженного конфликта на территории Абхазии и Южной Осетии в августе 2008 года. Российские эксперты с применением современных экспертных технологий выявили совокупность признаков, позволившую в дальнейшем сделать вывод о фальсификации видеодоказательств, предоставленных грузинской стороной.

Интеграция любого государства в правовое и экономическое пространство мирового сообщества, а также повышение активности всех субъектов судопроизводства по использованию специальных знаний в международных судах, в числе первостепенных задач требует подтверждение технической компетентности судебно-экспертных организаций в соответствии с международными стандартами, т.е. их аккредитации. Поэтому сегодня особо подчеркивается, что системы менеджмента качества экспертного производства — это инновационные модели, которые позволяет перевести судебно-экспертные организации на новый уровень судебно-экспертной деятельности, отвечающий критериям сокращения сроков экспертного производства и повышения качества проводимых исследований [4].

В качестве базовой современной тенденции, безусловно, выступает стандартизация судебно-экспертной деятельности. С одной стороны, мы являемся свидетелями бурного развития законодательного регулирования стандартизации как самостоятельной деятельности по разработке и применению документов по стандартизации.

С этими процессами тесно взаимоувязано создание национальных и межгосударственных комитетов по судебной экспертизе (так, в России создан ТК 134 «Судебная экспертиза», в СНГ – МТК-545«Судебная экспертиза»), разработка и принятие первых стандартов по судебной экспертизе и т. д. Такие понятия, как стандарт, стандартная операционная процедура, сертификация и валидация мелодического обеспечения, оценка неопределенности, отношение правдоподобия и др. – постепенно проникают в нашу повседневную судебно-экспертную жизнь. Хотя, в целом, следует отметить, что регламентация механизмов оценки пригодности методических материалов по производству судебной экспертизы, критерии их достоверности и научной обоснованности в российском законодательстве до сих пор отсутствуют.

В то же время при производстве судебной экспертизы традиционно большую роль играют такие понятия как творческий подход и свобода выбора методов и средств, необходимых для решения поставленных экспертных задач, возможность широкого использования всего доступного инструментария для проведения исследования и поиска ответов. Вспомним, что прямого ограничения эксперта в выборе методов в законодательстве не имеется, исключение составляют случаи, когда объектом является человек, а также обеспечение безопасности проведения исследования. Как известно, задачи судебной экспертизы могут быть как типовыми, стандартными, так и творческими (эвристическими), требующими нестандартного подхода, разработки новой или модернизации действующей экспертной методики. Не следует забывать и о возможностях экспертной инициативы, которая, кстати, также так до конца и не урегулирована нормам процессуального права.

В разных государствах и правовых системах проблема стандартизации судебно-экспертной деятельности и ее гармонизация с методологическими основами судебной экспертизы, решается по-разному.

В качестве основного ориентира, по нашему мнению, должны выступать международные стандарты, разработанные комитетом ИСО/ТК 272 «Forensic Sciences» в международной организации по стандартизации (ISO). В настоящее время указанный комитет рассматривает проекты стандартов серии ISO 21043 «Forensic sciences». При этом два стандарта из этой серии уже приняты: ISO 21043-1:2018 (Часть 1. Термины и определения) и ISO 21043-2:2018 (Часть 2. Обнаружение, описание, сбор, транспортировка и хранение объектов экспертизы). Продолжается разработка проектов стандартов, связанных с проведением исследования, интерпретацией полученных результатов и составлением заключения эксперта (отчета).

Стандартизация важна не только для процессов собирания доказательств, проведения судебно-экспертного исследования, но всех обеспечивающих составляющих этих действий, включая требования к техническим средствам, реактивам и вспомогательным материалам.

Таким образом, для решения актуальных проблем развития судебно-экспертной деятельности как в России, так и за рубежом необходима реализация системных проектов по качественному совершенствованию судебно-экспертной деятельности на основе внедрения стандартов в повседневную деятельность по организации и производству судебных экспертиз.

Библиографический список

1. Омельянюк, Г. Г. Тенденции развития судебно-экспертной деятельности: вызовы времени и решения / Г. Г. Омельянюк, А. И. Усов // Фундаментальные и прикладные исследования в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации: мат-лы Всерос. науч.-практ. конф. с междунар. участием (17–18 октября 2019 г., Уфа). – Уфа: Изд-во БашГУ, 2019. – С. 205–212.

2. Бебешко, Г.И. К вопросу об использовании байесовских методов для метрологической оценки и интерпретации результатов судебно-экспертного исследования / Г. И. Бебешко, С. А. Войтов, Г. Г. Омельянюк, А. И. Усов // Теория и практика судебной экспертизы. – М., 2014. – № 1 (33). – С. 148–158.

3. Руководство ENFSI по оценке совокупности выявленных признаков объектов судебной экспертизы статистическими методами: комментированный перевод / О. Б. Градусова, С. А. Кузьмин, А. И. Селин [и др.]; под ред. А.И. Усова; ФБУ РФЦСЭ при Минюсте России. – М., 2018. – 128 с.

4. Омельянюк, Г. Г. Использование инновационных механизмов повышения качества экспертного производства при совершенствовании законодательства о судебно-экспертной деятельности / Г. Г. Омельянюк // Теория и практика судебной экспертизы. – 2014. – № 1. – С. 10–17.

УДК 004:347.9

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ПРИНЦИПА СОСТЯЗАТЕЛЬНОСТИ ПО ДЕЛАМ УПРОЩЕННОГО ПРОИЗВОДСТВА

Орлова Александра Ивановна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В статье на основе анализа гражданского процессуального и арбитражного процессуального законодательства исследуется влияние информационных технологий на реализацию принципа состязательности по делам упрощенного производства. Автор делает вывод о том, что заимствование положений АПК РФ об упрощенном производстве при конструировании аналогичного института в гражданском процессе произведено законодателем без учета фактора наличия у субъектов арбитражного процесса более широких возможностей использования информационных технологий, обеспечивающих состязательность процесса.

***Ключевые слова**: арбитражный процесс, гражданский процесс, информационные технологии, упрощенное производство, состязательность, информационно-коммуникационная сеть «Интернет».*

INFORMATION TECHNOLOGIES AS A MEANS OF ENSURING THE PRINCIPLE OF COMPETITION IN SIMPLIFIED PROCEEDINGS

Orlova Alexandra Ivanovna
candidate of law, associate Professor
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

Based on the analysis of civil procedure and arbitration procedural legislation, the article examines the impact of information technologies on the implementation of the principle of competition in simplified proceedings. The author concludes that the borrowing of provisions of the APC on a simplified production when designing similar Institute in civil proceedings made by the legislator without considering the factor of whether the subjects of the arbitration process with more opportunities to use information technology to ensure competitiveness of the process.

***Keywords**: arbitration process, civil procedure, information technology, simplified production, competition, information and communication network «Internet».*

Повышение качества правосудия и совершенствование судебной защиты прав и законных интересов граждан и организаций рассматривается на современном этапе в качестве основной цели развития российской судебной системы [3]. Одним из способов достижения данной цели является внедрение в гражданский и арбитражных процесс упрощенных форм судопроизводства, которые

способны сократить временные затраты суда на рассмотрение дел небольшой сложности и тем самым оптимально распределить нагрузку на судей.

По справедливому замечанию В.В. Яркова, как в России, так и за рубежом поиск вариантов рационализации процессуальных форм разрешения дел, позволяющих достичь целей судопроизводства путем упрощения основных составляющих судебного процесса, носит постоянный характер [7, с. 27]. Одной из упрощенных форм судопроизводства в российском цивилистическом процессе является упрощенное производство, изначально существовавшее только в рамках арбитражного процесса (глава 29 АПК РФ). Положительный опыт рассмотрения дела в порядке упрощенного производства арбитражными судами привел к внедрению данного института сначала в административный процесс (глава 33 КАС РФ), а с июня 2016 года и в гражданский процесс (глава 21.1 ГПК РФ) [1]. Согласно пояснительной записке к проекту Федерального закона «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации и в Арбитражный процессуальный кодекс Российской Федерации» целями введения упрощенного производства в гражданском процессе являются сближение систем судов общей юрисдикции и арбитражных судов, унификация процедур и правил, применяемых этими судами в ходе рассмотрения и разрешения споров и иных юридических дел, в целях повышения качества и эффективности правосудия, что позволит установить аналогичный порядок рассмотрения судами общей юрисдикции сходных по своей правовой природе дел посредством введения институтов, успешно применяемых в течение последних лет арбитражными судами и доказавших свою эффективность [4].

Сравнение положений арбитражного и гражданского процессуального законодательства об упрощенном производстве позволяет прийти к выводу о том, что нормы ГПК РФ, устанавливающие порядок рассмотрения дел упрощенного производства, фактически дословно повторяют положения главы 29 АПК РФ, за исключением требования об обязанности суда размещать на официальном сайте суда в информационно-телекоммуникационной сети «Интернет» в режиме ограниченного доступа исковое заявление и прилагаемые к такому заявлению документы, отзыв на исковое заявление, доказательства и иные документы, а в режиме свободного доступа – определение о принятии искового заявления к производству.

Принимая во внимание преследуемую законодателем цель унификации арбитражного и гражданского процессов, а также тот факт, что в настоящее время арбитражные суды в гораздо большей степени используют информационные технологии при рассмотрении дел, нежели суды общей юрисдикции, невключение законодателем в ГПК РФ норм о размещении судом в сети «Интернет» поступивших по делу процессуальных документов и доказательств можно было бы расценить как адаптацию положений арбитражного процесса под реалии процесса гражданского. Вместе с тем более детальное рассмотрение механизма упрощенного производства в гражданском процессе обнаруживает, что заимствование положений АПК РФ о порядке рассмотрения дела с одновременным отказом от использования информационных технологий как неотъ-

емлемой части данного порядка, приводит существенному снижению процессуальных гарантий реализации принципа состязательности при рассмотрении судами общей юрисдикции дел упрощенного производства.

Отметим, что состязательный характер не исключается наукой процессуального права. По мнению, И.В. Решетниковой, «состязательность упрощенного производства проявляется прежде всего в том, что стороны обмениваются состязательными документами и раскрывают имеющиеся доказательства» [6]. Ю.А. Кондорина в качестве признака состязательности упрощенного производства отмечает то, что «стороны имеют равные возможности по представлению своих позиций по вопросам заявленных требований и возражений и обосновывающих их доказательственных материалов» [5]. Однако одной из особенностей упрощенного производства, направленной, прежде всего, на сокращение срока рассмотрения дела, является установление законодателем относительно небольших сроков направления суду состязательных документов. Так, с момента вынесения судом определения о возбуждении производства по делу, рассматриваемому в порядке упрощенного производства, ответчику предоставляется пятнадцатидневный срок (увеличение данного срока судом допускается законом, но не используется на практике) для представления отзыва на иск с обосновывающими его документами. В этот же срок истец вправе представить дополнительные доказательства (ч. 2 ст. 228 АПК РФ, ч. 2 ст. 232.3 ГПК РФ). Еще один срок - не менее 30 дней со дня вынесения судом определения о возбуждении производства по делу - установлен законодателем для представления сторонами дополнительных документов, содержащих пояснения и возражения относительно заявленных требований, которые при этом не могут содержать ссылки на доказательства, не раскрытые в первый срок. Закон устанавливает достаточно жесткие требования к пропуску сторонами данных сроков – возвращение судом документов, поступивших в суд с пропуском срока, за исключением случая, если эти лица обосновали невозможность представления указанных документов в установленный судом срок по причинам, не зависящим от них (ч. 4 ст. 228 АПК РФ). Как отмечает И.В. Решетникова, «данный подход законодательно выдержан в духе ч. 2 ст. 9 АПК РФ – процессуальный риск несовершения определенных действий лежит на лицах, участвующих в деле» [6]. Аналогичные последствия установлены частью 4 статьи 232.3 ГПК РФ для сторон гражданского процесса.

Теперь проведем параллели между практической реализацией положений об упрощенном производстве в арбитражном и гражданских процессах через призму информационных технологий.

Во-первых, ответчик, как сторона, вовлекаемая в судебный процесс помимо его воли, должен располагать достаточным временем для подготовки и направления в суд своей позиции по делу. С точки зрения законодателя, этот срок не должен быть менее 15 дней со дня принятия судом определения о возбуждении производства по делу. Установление в качестве момента начала течения срока даты принятия определения судом, а не даты получения сторонами этого определения, неизбежно влечет необходимость исключить из данного

срока период времени, необходимый на почтовую доставку ответчику данного определения. Безусловно, доставка почтовой корреспонденции не зависит от вида процесса, но, во-первых, ответчик в арбитражном процессе вправе рассчитывать на получение от истца копии иска и обосновывающих иск документов, отсутствующих у ответчика, не позднее дня обращения истца в суд, в противном случае суд оставит исковое заявление без движения (п. 1 ч. 1 ст. 126, ч. 1 ст. 128 АПК РФ). Во-вторых, в рамках программы «Электронное правосудие» по инициативе Высшего Арбитражного Суда РФ был разработан сервис арбитражного суда «Электронный страж» (guard.arbitr.ru). Это часть личного кабинета «Мой арбитр» системы арбитражных судов. При помощи сервиса «Электронный страж» зарегистрированный в системе пользователь может добавить любое дело либо участника в картотеку отслеживаемых дел. Таким образом, «подписавшись» на себя как на участника, лицо приобретает возможность незамедлительно получить в личный кабинет уведомление о возбуждении арбитражным судом любого дела с его участием, в том числе дела упрощенного производства, в котором данное лицо является ответчиком. Владея соответствующей информацией, ответчик может предпринять все необходимые меры по оперативному ознакомлению с текстом искового заявления в целях формирования своей позиции по делу, в том числе ознакомиться с материалами электронного дела, размещенными на сайте суда.

В гражданском процессе ответчик может узнать о существе заявленных истцом требований только из копии искового заявления, направленной ему судом вместе с определением о возбуждении производства по делу. К моменту получения данной копии значительная часть 15-дневного срока, предусмотренного для направления суду отзыва, истечет, тем самым время на подготовку отзыва и сбор необходимых контрдоказательств, существенно ограничивается. В случае пропуска срока на представление отзыва, ответчик вправе рассчитывать на принятие судом документов лишь при условии, что суд сочтет причины пропуска уважительными.

В заключении необходимо отметить, что в настоящее время в отношении судов общей юрисдикции законодателем сделаны значительные шаги в направлении электронного правосудия. Так, с 1 января 2017 г. вступили в силу масштабные изменения в ГПК РФ [2], предусматривающие широкое использование информационных технологий в гражданском процессе. Однако, во-первых, как следует из п. 4 ст. 12 Федерального закона от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» сама возможность использования информационных технологий в гражданском процессе лицами, участвующими в деле, связывается законодателем не с вступлением в силу законодательных изменений, а с наличием технической возможности в конкретном суде, что позволяет предположить о наличии проблем материально-технического оснащения судов. Во-вторых, даже с учетом внесенных изменений в ГПК РФ обозначенные нами проблемы упрощенного производства остаются нерешенными как ввиду отсутствия у пользовате-

лей интернет-сервиса ГАС «Правосудие» возможности оформить подписку на дела с их участием, так и ввиду отсутствия обязанности суда размещать электронные копии состязательных документов сторон в режиме ограниченного доступа в информационно-коммуникационной сети «Интернет» по делам упрощенного производства.

Библиографический список

1. Федеральный закон от 02.03.2016 N 45-ФЗ «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации и Арбитражный процессуальный кодекс Российской Федерации» // СПС Консультант Плюс (дата обращения: 19.02.2020).
2. Федеральный закон от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» // СПС Консультант Плюс (дата обращения: 19.02.2020).
3. Федеральная целевая программа «Развитие судебной системы на 2013 –2020 годы», утвержденная Постановлением Правительства РФ от 27.12.2012 № 1406 (ред. от 25.12.2019) // СПС Консультант Плюс (дата обращения: 19.02.2020).
4. Пояснительная записка к проекту Федерального закона «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации и в Арбитражный процессуальный кодекс Российской Федерации» // СПС Консультант Плюс (дата обращения: 19.02.2020).
5. Кондюрина, Ю.А. Реализация принципов арбитражного и гражданского процесса в упрощенном производстве / Ю.А. Кондрюшина // Арбитражный и гражданский процесс. – 2017. – № 1. – С. 55–59.
6. Решетникова, И.В. Размышляя о судопроизводстве: избранное / И.В. Решетникова. – М.: Статут, 2019. 510 с.
7. Ярков, В.В. Развитие цивилистического процесса в России: отдельные вопросы / В.В. Ярков // Вестник гражданского процесса. – 2011. – № 1. – С. 17–53.

УДК 343.4

ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ: НА ПРИМЕРЕ ЛЕГАЛИЗАЦИИ ДЕНЕЖНЫХ СРЕДСТВ ИЛИ ИНОГО ИМУЩЕСТВА, ПРИОБРЕТЕННЫХ ЛИЦАМИ ПРЕСТУПНЫМ ПУТЕМ

Пелисова Ирина Павловна
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья посвящена развитию и использованию информационных технологий, в целях предотвращения и раскрытия преступлений. Роль информационных технологий в борьбе с преступностью сама по себе разнообразна. С их помощью эксперты способны восстановить данные, которые были удалены, зашифрованы на компьютере или скрыты в мобильных устройствах. Выявлены проблемы и предложены пути решения.

***Ключевые слова**: информационные технологии; преступления; правоохранительные органы; легализация.*

USE OF HIGH TECHNOLOGIES FOR THE DISCLOSURE OF CRIMES: ON THE EXAMPLE OF LEGALIZATION OF MONEY OR OTHER PROPERTY PURCHASED BY PERSONS IN CRIME

Pelisova Irina Pavlovna
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article is devoted to the development and use of information technology in order to prevent and solve crimes. The role of information technology in the fight against crime is diverse in itself. With their help, experts are able to recover data that has been deleted, encrypted on a computer or hidden on mobile devices. Identified problems and suggested solutions.

***Keywords**: information technology; crimes; law enforcement agencies; legalization.*

По мнению видного ученого П.В. Сороколетова, мир сегодня стоит на пороге четвертой информационной революции [1]. Все более интенсивно протекают процессы глобализации, в том числе информатизации.

На сегодняшний день резко увеличиваются темпы развития и использования информационных технологий в различных странах мира. Речь идет о переходе к построению глобального информационного общества с развитой системой информационных телекоммуникаций. Интенсивное внедрение передовых информационных технологий охватывает все сферы юридической деятельности, в том числе, использование высоких технологий при раскрытии преступлений. При этом значительный объем информационных функций, выполняе-

мых органами внутренних дел, - это интенсивный обмен информацией с помощью современного набора средств информационного обмена[2].

С каждым годом возрастает роль компьютерных технологий при раскрытии преступлений, где создаются информационно-поисковые системы для учета уголовных дел, лиц, совершивших преступление, похищенного имущества и оружия, транспортных средств и т. д., вводятся вспомогательные подсистемы для учета подготовки сотрудников правоохранительных органов, и т. д. Но не стоит забывать, что достижения в области высоких технологий использует и преступный мир.

Роль информационных технологий в борьбе с преступностью сама по себе разнообразна. Так, при проведении оперативно-розыскной деятельности могут быть успешно использованы для раскрытия преступлений и пресечения преступной деятельности на ранних стадиях их подготовки и осуществления какого-либо преступления.

С помощью современных технологий эксперты способны восстановить данные, которые были удалены, зашифрованы на компьютере или скрыты в мобильных устройствах [3].

Применение современных высоких технологий успешно помогают бороться с экономическими преступлениями, в которых, при осуществлении преступной деятельности, используются различные компьютерные устройства. В качестве примера можно привести отмывание денег, деятельность, которая направлена на уничтожение незаконного происхождения денежных средств, приобретенных в результате совершения преступления, и придание этим деньгам законного вида. В основе отмывания денег лежит сокрытие имущества, приобретенного преступным путем.

Денежные средства стали отмывать с помощью онлайн-аукционов и продаж, вебсайтов азартных игр и виртуальных игровых сайтов, где неправомерно полученные деньги конвертируются в игровую валюту, а затем возвращаются в реальные, пригодные для использования и не отслеживаемые «чистые» деньги [4].

Предупреждение преступного деяния по отмыванию денег, является важным компонентом предупреждения преступности, поскольку доходы от такой деятельности, как правило, обеспечивают капитал для совершения других преступлений [5]. Компьютерные устройства, применяемые при раскрытии и расследовании таких дел, оказывают значительную помощь и помогают успешно справиться с расследованием преступлений.

Стоит отметить, что для противодействия преступлениям, которые совершаются с помощью компьютерной техники, правоохранительные органы должны обладать знаниями способов совершения таких преступлений, тактики и методики выявления, раскрытия и расследования преступлений данной категории; стремиться к превосходству над злоумышленниками в уровне технической оснащенности и скорости получения информации. Однако многие сотрудники органов внутренних дел, осуществляющие противодействие преступлениям, совершенным с использованием современных информационно-коммуникационных технологий, сталкиваются с рядом существенных трудностей при

получении необходимой информации, что негативно сказывается на итогах оперативно-служебной деятельности, к ним относятся:

1. Несвоевременность получения информации о соединениях между абонентами и (или) абонентскими устройствами, особенно в случаях, когда информация необходима от оператора связи, не имеющего представительств в регионе местонахождения инициатора запроса.

2. Длительность получения информации от интернет-провайдеров, а также от владельцев и администраторов различных интернет-ресурсов.

3. Сложность идентификации и обнаружения фактических собственников, а также администраторов и пользователей некоторых интернет-ресурсов.

Очевидно, эти проблемы требуют оперативного решения. Одним из способов решения представляется внесение изменений в нормативные правовые акты, регламентирующие порядок взаимодействия ОВД с операторами связи, интернет-провайдерами, владельцами и администраторами различных интернет-ресурсов с учетом развития информационно-телекоммуникационных технологий, а также ряда иных факторов.

Библиографический список

1. Сороколетов, П. В. Мир на пороге четвертой информационной революции / П. В. Сороколеов. – URL: http://dissers.ru/books/2/755-1.php (дата обращения: 18.02.2020).

2. Болатова, А. С. Использование информационных технологий в уголовном расследовании. / А. С. Болатова. – М., 2013. – С. 1156–1159.

3. Расследование компьютерных преступлений с использованием криминалистических средств и технологий. – URL: https://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology (дата обращения 18.02.2020).

4. Пелисова, И. П. Легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем с помощью использования криптовалюты / И. П. Пелисова // Государство и право: проблемы и перспективы совершенствования: сб. науч. тр. 2-й междунар. науч. конф. – Курск, 2019. – С. 168–171.

5. Предотвращение отмывания денег. – URL: https://www.poliisi.fi/crimes/prevention_of_money_laundering (дата обращения: 19.02.2020).

УДК 34:004

ЦИФРОВЫЕ СЕРВИСЫ В ЮРИСПРУДЕНЦИИ

Петров Станислав Валерьевич
Национальный исследовательский университет «МИЭТ», Москва, Россия

Сервисы становятся важными помощниками для юристов. Они удобны, экономят время пользователя и облегчают его работу. В зарубежных странах юристы активно внедряют в свою деятельность высокие технологии, что способствует повышению качества юридических услуг.

***Ключевые слова**: цифровые сервисы, приложения для юристов, цифровизация, автоматизация.*

DIGITAL SERVICES IN LAW

Petrov Stanislav Valerevich
National Research University MIET, Moscow, Russia

Services are becoming important assistants for lawyers. They are convenient, save the user's time and make their work easier. In foreign countries, lawyers are actively implementing high technologies in their activities, which contributes to improving the quality of legal services.

***Keywords**: digital services, applications for lawyers, digitalization, automation.*

Последние годы юристы все чаще используют высокие технологии в своей работе. Здесь и далее под «сервисами» следует понимать приложение для смартфона (компьютера) либо программу, предназначенную для юристов либо их доверителей.

Цифровые сервисы в юриспруденции выполняют ряд важных задач.

Основное преимущество использования сервисов - экономия времени. Юрист может тратить большое количество времени на довольно обычные вещи. Например, проверка документов на наличие каких-либо стандартных условий. Более того, чаще всего сервисы представлены в виде визуализированных данных, что сокращает трату времени на поиск конкретных данных. Сервисы позволяют быстро выполнить то, что нужно пользователю.

Следующее преимущество сервисов – минимизация технических ошибок в документе. Нередко юристы сталкиваются с большим количеством информации, которую необходимо проверить. Соответственно, в силу вступает человеческий фактор, когда юрист может, например, допустить техническую ошибку, которая не позволит по формальному основанию принять судом искового заявления. Сервисы обладают своей базой данных, тем самым позволяя указать на недочеты в документе.

При использовании сервисов юрист загружает документ на сервис, который за него проверит необходимую информацию, что, соответственно, приво-

дит к экономии собственных сил, так как уже не нужно изучать большой массив «технических» данных.

Чаще всего, сервисы визуализируют данные, что позволяет быстро и эффективно получить необходимые сведения.

Кроме того, некоторые сервисы помогут рассчитать вероятность, например, выигрыша дела, с каким успехом отклонят или же удовлетворят ходатайство и многое другое.

Одним из таких уникальных сервисов является Ravel Law.

Ravel Law – это компания, предоставляющая доступ к юридическим исследованиям. У них имеется два сервиса, предлагающие облегчить работу юристам: Judge Analytics (Аналитика Судьи) и Case Analytics (Аналитика Дел).

Judge Analytics занимается изучением и интерпретацией решений судьи по анализу ходатайств. На их основе сервис подсказывает, какие слова и словосочетания следует подбирать при разговоре в суде для наиболее вероятного выигрыша дела. Более того, Judge Analytics показывает пользователю, сколько ходатайств и какого типа рассматривал судья, какова вероятность принятия или отклонения конкретного заявления. Следует отметить, что основная ценность данного продукта заключается в его полезности для юристов, а также в его уникальности. Такой сервис уменьшает временные и умственные затраты. К тому же, информация визуализирована, что позволяет быстро и эффективно с ней работать. Недостатком Judge Analytics является его доступность по платной подписке.

Case Analytics дает пользователю подробную информацию по конкретному судебному делу:

– сколько времени оно длится;

– показывает, какой судья его рассматривает, какими делами он занимался ранее;

– иные значимые элементы.

К тому же, сервис позволяет создавать собственные заметки, которые будут видны только пользователю.

Достоинства этой услуги заключаются в подробной визуализации данных, значимые цитаты судьи на заседании, помеченные для пользователя и его бесплатность.

Еще одним полезным сервисом является Luminance. Этот продукт обнаруживает слова в документе, которые можно заменить на юридические понятия. Искусственный интеллект анализирует файл, затем по своим алгоритмам высчитывает области, в которых слова возможно поменять. Также следует выделить, что сервис проверяет документы: отсутствие каких-либо страниц, нахождение дополнительных положений и указывание на неправильные формулировки. Данные проблемы демонстрируются юристу, тем самым помогая ему подготовить правильные документы или же обнаружить ошибки в других. Достоинством сервиса является визуализация данных, его полезность и простота. Недостаток – сервис платный.

УДК 343.98:004

НАЧАЛЬНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ РАССЛЕДОВАНИЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ

Поляков Виталий Викторович
кандидат юридических наук
Красноярский государственный аграрный университет, Красноярск, Россия

Исследован начальный этап расследования высокотехнологичных преступлений, проанализирована его специфика и выявлены сложности в расследовании. Определены границы и взаимосвязь данного этапа с другим этапами. Выделены и проанализированы существующие на этом этапе следственные ситуации. Предложены алгоритмы разрешения типичных и не очевидных следственных ситуаций. Даны универсальные тактические рекомендации, повышающие эффективность по достижению целей, поставленных на начальном этапе расследования высокотехнологичных преступлений.

***Ключевые слова**: следственная ситуация, высокотехнологичные преступления, компьютерные преступления.*

INITIAL INVESTIGATIVE SITUATIONS OF INVESTIGATION OF HIGH-TECHNOLOGICAL CRIMES

Polyakov Vitaliy Viktorovich
candidate of law
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The initial stage of the investigation of high-tech crimes is investigated, its specificity is analyzed and difficulties in the investigation are identified. The boundaries and the relationship of this stage with other stages are determined. The investigative situations existing at this stage are highlighted and analyzed. Algorithms for resolving typical and non-obvious investigative situations are proposed. Universal tactical recommendations are given that increase efficiency in achieving the goals set at the initial stage of the investigation of high-tech crimes.

***Keywords**: investigative situation, high-tech crime, computer crime.*

Происходящие в последние годы процессы цифровизации сопровождаются ростом компьютерной преступности и использованием в ней высоких информационных технологий. Это особенно заметно по возникновению высокотехнологичных преступлений, связанных как с новыми цифровыми технологиями, непосредственно используемыми преступниками [1, с. 188–191], так и с появлением новых реалий в связи с формированием новых отраслей цифровой экономики [2, с. 49–57]. Использование цифровых технологий при совершении преступлений требует от правоохранительных органов адекватного ответа в виде опережающего применения этих технологий для расследования преступлений. Решение этой сложной задачи возможно лишь с помощью научно-обоснованной криминалистической теории [3, с. 173–178].

В криминалистическом плане при расследовании высокотехнологичных преступлений весьма значимым является начальный этап расследования, так как именно на нем формируется наибольшее количество доказательств. На последующем этапе эти доказательства расширяются, закрепляются и исследуются, определяются основные элементы механизма преступления. В силу этого для эффективного противодействия высокотехнологичной преступности наиболее значима разработка теоретических основ расследования именно для этого этапа.

Криминалистические ситуации начального этапа были достаточно подробно описаны в криминалистической литературе [4, 5] и наиболее тщательно исследованы. Этот этап начинается с момента возбуждения уголовного дела. Верхняя граница этапа была предложена В.К. Гавло, В.Е. Клочко и Д.В. Кимом, именовавшими его как «первоначальный этап предварительного расследования» [6, с. 145] и полагавшими, что он завершается моментом вынесения следователем постановлений о привлечении в качестве обвиняемых лиц, которые по проверенной версии следствия причастны к преступлению. О возможности введения такой верхней границы писали также Н.П. Яблоков и А.С. Князьков, считавшие, что в определенных случаях «моментом окончания данного этапа может быть вынесение постановления о привлечении лица в качестве обвиняемого» [7, с. 15]. В отношении содержания этапа можно согласиться с мнением Р.С. Белкина, считавшего, что «Основная направленность этапа - интенсивный поиск, обнаружение и закрепление доказательств» [8, с. 286].

Исходные информационные данные на рассматриваемом этапе формируются на основе данных, полученных до возбуждения уголовного дела на предыдущем (проверочно-следственном) этапе, в том числе с помощью оперативно-розыскных мероприятий. Совокупность исходных данных вместе с исходными условиями первоначального расследования образуют исходную следственную ситуацию. Дальнейшее развитие исходной следственной ситуации происходит на этапе «наиболее сложном, характеризующемся, как правило, повышенной информационной неопределенностью» [9, с. 403]. С качественной стороны для начальных следственных ситуаций характерен недостаточный объем информации и доказательств.

Серьезные затруднения, возникающие на этапе начальных следственных ситуаций при расследовании высокотехнологичных преступлений, связаны с характерными особенностями данного вида преступлений. Это связано в большой степени с использованием преступниками технологий удаленного доступа [10, с. 146–152]. Кроме того, затруднения усиливаются еще и тем, что «С криминалистических позиций высокотехнологичный способ совершения компьютерных преступлений является полноструктурным, поскольку он включает стадии подготовки к преступлению, самого его совершения и действий по сокрытию следов» [11, с. 123–126]. Сокрытие следов преступления, совершаемого с применением компьютеров, удаленно расположенных от объекта преступного посягательства, значительно затрудняет благоприятное разрешение следственных ситуаций. Для такого разрешения требуются криминалистические действия, позволяющие провести установление принадлежности следов преступле-

ния конкретному лицу и получить доказательства этого, установить необходимые причинно-следственные связи, в случае преступной группы определить наличие заказчиков, организаторов и руководителей группы и т.д. Необходимо также учитывать, что преступники освоили такие способы сокрытия следов при совершении высокотехнологичных преступлений, когда подозрения падают на невиновных лиц, что представляется особенно опасным [12, с. 184–187].

При расследовании высокотехнологичных преступлений на начальном этапе у следствия уже имеется первичная информация о преступниках или преступлении, и она складывается либо в очевидную, либо в неочевидную следственную ситуацию. Первый вид ситуаций для высокотехнологичных преступлений не свойственен и возникает, например, когда имеются достаточные доказательства для обоснованного предположения о личности преступников, нет проблем в их задержании, получении от них признательных показаний, либо существуют не значительные сложности, например, связанные с их розыском. Второй вид ситуаций, когда расследование не носит очевидного характера, обычно может быть связан с наличием некоторых сведений о преступлении при отсутствии важных данных, входящих в предмет установления и доказывания. Распространены или типичны ситуации, когда известны потерпевшие, но ни им, ни следствию не известны преступники. Другая типичная неочевидная ситуация расследования, когда имеются данные о предполагаемых преступниках, но отсутствуют данные о потерпевших, например, это бывает при выявлении оперативно-розыскным путем преступной деятельности организованной преступной группы, однако в отношении кого именно, сколько преступлений или эпизодов ими совершено, когда и каким образом они осуществлялись, не известно. Менее распространена начальная ситуация, когда следствию не известны ни преступники, ни потерпевшие, например, при обнаружении вредоносного программного обеспечения, когда нет данных о том, кто его создал, использовал или распространял, а также кто и как от него пострадал.

Отметим, что на начальном этапе расследования в ситуации неочевидности, как правило, первостепенной задачей является определение места происшествия, что повышает эффективность последующих криминалистических действий. Однако по высокотехнологичным преступлениям решение этой, казалось бы, не сложной задачи вызывает большие трудности, так как за счет использования информационных сетей место совершения преступления может включать места подготовки к преступлению, место нахождения преступника в момент непосредственного совершения преступления и место наступления противоправных последствий, например, где находилась компьютерная техника и защищаемая законом компьютерная информация потерпевшего. Более того, по высокотехнологичным преступлениям преступников всегда несколько, и обычно они совершают преступления на систематической основе. Для этого они могут использовать мобильные средства совершения преступлений, перемещаемые в пространстве. Средствами совершения преступлений могут быть «виртуальные машины» и выделенные серверы, которые арендуются и задействуются преступниками с помощью различной техники удаленно. Отметим, также, что почти всегда в высокотехнологичных преступлениях применяются

анонимайзеры, задача которых заключается в сокрытии, например, путем подмены реальных IP – адресов устройств, по которым можно пытаться определить их местонахождение. В некоторых способах совершения данных преступлений могут быть использованы одновременно тысячи компьютеров, зараженных вредоносным программным обеспечением, а их местоположение может быть на территории разных государств.

В ситуации информационной неопределенности на начальном этапе целесообразно проведение судебных компьютерно-технических экспертиз и использование помощи специалистов. Специалисты могут обнаружить криминалистически значимую информацию о способе, средствах совершения преступлений, например, выявить вредоносное программное обеспечение, связанное с управляющим сервером, на который пересылаются данные и, соответственно, которым пользуется преступник. Такая информация может позволить выдвинуть новые следственные версии, получить искомые данные, скорректировать план расследования, принять правильные тактические решения [13, с. 130–134].

Целесообразно по возможности осуществить как можно более раннее задержание предполагаемых преступников, поскольку с их стороны при высокотехнологичных преступлениях весьма вероятно оказание противодействия расследованию. Следует учитывать, что такое противодействие может оказаться весьма результативным, чему способствует организованная форма деятельности преступных групп и сообществ, а также зачастую имеющиеся технические возможности воздействия на объекты и следы преступления. После задержания открываются б**о**льшие возможности на последующем этапе расследования, например, по производству осмотра мест происшествия, проведению обысков, выемок, получении компьютерной информации и информации о соединениях между абонентами и (или) абонентскими устройствами и т.д.

Таким образом, высокотехнологичные преступления имеют свою специфику, накладывающую существенный отпечаток на следственные ситуации, возникающие на начальном этапе расследования. Учет этой специфики необходим для благоприятного разрешения этих ситуаций и тем самым - для успешного расследования в целом.

Библиографический список

1. Polyakov V.V., Starodubtseva, M.A. (2019). Factors influencing motivation for terrorist activities being implemented with the use of information technologies in transboundary regions. The role of transnational corporations in the globalization of the economy. Advances in Social Science, Education and Humanities Research, Vol. 364, Pp. 188-191.

2. Вехов, В.Б. Преступления в сфере цифровой экономики: криминалистически значимые сведения о технологии «блокчейн» / В.Б. Вехов, И.М. Комаров // Уголовно-процессуальные и криминалистические чтения на Алтае: Проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул: Изд-во Алтайского ун-та, 2018. – Вып. IX. – 228 с.

3. Бертовский, Л. В. Цифровое судопроизводство: проблемы становления / Л. В. Бертовский// Проблемы применения уголовного и уголовно-процессуального законодательства // Сб. мат-лов междунар. науч.-практ. конф. – Симферополь: Ариал. – 2018. – С. 173–178.

4. Драпкин, Л.Я. Основы теории следственных ситуаций. / Л.Я. Драпкин. – Свердловск: Изд-во УрГУ, 1987. – 164 с.

5. Гавло, В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. / В.К. Гавло. – Томск: Изд-во Томского гос. ун-та, 1985. – 334 с.

6. Гавло, В.К. Судебно-следственные ситуации: психолого-криминалистические аспекты: монография. / В.К. Гавло, В.Е. Клочко, Д.В. Ким / под ред. В.К. Гавло. – Барнаул: Изд-во Алтайского гос. ун-та, 2006. – 226 с.

7. Яблоков, Н.П. Этапность как метод структурирования предварительного следствия и повышения уровня его организации / Н.П. Яблоков, А.С. Князьков // Вестник Московского университета. – Сер. 11. Право. – 2012. – № 1. – С. 3–18.

8. Белкин, Р.С. Курс криминалистики: учеб. пособие для вузов: в 3 т. / Р.С. Белкин. – 3-е изд., дополненное. – М., 2001. – 394 с.

9. Баев, О.Я. Избранные работы по проблемам криминалистики и уголовного процесса: сб. – М.: Эксмо, 2011. – 614 с.

10. Гавло, В.К., Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации / В.К. Гавло, В.В. Поляков // Российский юридический журнал. – 2007. – № 5 (57). – С. 146–152.

11. Поляков, В.В. О высокотехнологичных способах совершения преступлений в сфере компьютерной информации // Уголовно-процессуальные и криминалистические чтения на Алтае: мат-лы ежегод. всерос. науч.-практ. конф., посвящ. 50-летию юридического факультета и 40-летию Алтайского государственного университета. – Барнаул: Изд-во Алт. гос. ун-та, 2012. – Вып. 11–12. – С. 123–126.

12. Гавло, В.К. Проблемы расследования преступлений в сфере компьютерной информации / В.К. Гавло, В.В. Поляков. // Использование современных информационных технологий в правоохранительной деятельности и региональных проблемах информационной безопасности: мат-лы науч.-практ. конф. – Калининград: Калининград. юрид. ин-т МВД России, 2006. – Вып. 7. – С. 184–187.

13. Закатов, А.А. Особенности первоначального этапа расследования хищений денежных средств, совершенных с использованием вредоносных компьютерных программ А.А. Закатов, В.В. Намнясев // Юридическая наука и практика: вестник Нижегородской академии МВД России. – 2017. – № 4 (40). – С. 130–134.

УДК 004:343:347

ЦИФРОВЫЕ ТЕХНОЛОГИИ И СОВРЕМЕННОЕ РОССИЙСКОЕ СУДОПРОИЗВОДСТВО

Пыжиков Михаил Александрович
старший следователь-криминалист следственного управления Следственного комитета Российской Федерации по Ивановской области
подполковник юстиции, аспирант
Московская академия Следственного комитета Российской Федерации, Москва, Россия

В статье рассматриваются некоторые аспекты использования цифровых технологий в уголовном процессе. Указаны факторы, влияющие на возможность перехода к применению на практике «цифрового уголовного дела».

***Ключевые слова**: цифровые технологии, уголовный процесс, «цифровое уголовное дело».*

DIGITAL TECHNOLOGIES AND MODERN RUSSIAN LEGAL PROCEEDINGS

Pyzhikov Mikhail Alexandrovich
senior forensic investigator of the investigative Department of the Investigative Committee of the Russian Federation for the Ivanovo region, Lieutenant Colonel of justice, postgraduate student
Moscow Academy of the Investigative Committee of the Russian Federation Moscow, Russia

The article deals with some aspects of the use of digital technology in criminal process. The factors affecting the possibility of transition to the application of the "digital criminal case" in practice are indicated.

***Key words:** digital technologies, criminal process, «digital criminal case».*

На протяжении последних лет наблюдается рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, по данным МВД и Генеральной прокуратуры РФ, в 2019 году правоохранительными органами России зарегистрировано 294 409 таких преступлений, что на 68,5 % больше по сравнению с предыдущим годом. Удельный вес таких преступлений от общего числа зарегистрированных преступлений составил 14,5 % [1]. Последний из указанных показателей обращает на себя внимание. Так, практически каждое 7 зарегистрированное в 2019 году в стране преступление совершено с использованием информационно-телекоммуникационных технологий. Для большей наглядности, укажем: удельный вес преступлений экономической направленности составил 5,2%, преступлений, связанных с незаконным оборотом наркотиков – 9,4 %.

При этом, более чем в половине преступлений, совершенных с использованием информационно-телекоммуникационных технологий, применялась сеть Интернет – 157 036 зарегистрированных фактов (53,3 %), что больше на 45,4 % чем в предыдущем году [2].

С учетом роста пользователей указанных технологий и распространенности сети Интернет в повседневной жизни, когда они стали фактически «обыденными» явлениями, наблюдается рост их использования в различных противоправных действиях. Специфика сети Интернет позволяет преступнику за короткий промежуток времени или одновременно совершать несколько противоправных действий либо однотипные действия в отношении нескольких потерпевших, находящихся в различных местах (населенных пунктах, регионах, государствах). Указанные и иные обстоятельства существенно затрудняют процессы выявления и доказывания преступной деятельности, негативно влияют на процессуальные сроки рассмотрения поступивших сообщений, расследования уголовных дел.

Рост таких преступлений не остаётся без внимания российских властей. Не так давно, в 2016 году, заместитель председателя комитета по конституционному законодательству Совета Федерации Российской Федерации Е.Б. Мизулина, выступая на Форуме безопасного Интернета, предложила признать использование интернета отягчающим обстоятельством преступлений, «чтобы всякий раз, когда с помощью интернета совершалось преступление, облегчалось совершение преступлений, организовывалось преступление, это учитывалось при назначении наказания» [3]. Такая инициатива вызвала неоднозначную реакцию и не нашла своего легального отражения, вместе с тем указывает о значимости затронутой проблематики.

В контексте настоящей статьи хотелось бы акцентировать внимание на следующих обстоятельствах.

1. Развитие цифровых технологий, их использование в совершении преступлений ставит новые вызовы российской правоохранительной системе. Выявление и пресечение противоправных действий, совершенных с использованием цифровых технологий, а также их профилактика находятся в прямой причинной связи с возможностями сотрудников правоохранительных органов: как наличием у них специальных познаний в этой области, так и наличием соответствующего технического обеспечения. Зачастую те или иные вопросы правоприменительной деятельности упираются в нехватку «кадров» либо оборудования, позволяющего решать конкретные задачи по конкретным уголовным делам.

2. Даже при расследовании уголовных дел о преступлениях, совершенных без использования цифровых технологий, часто требуется применение специальных знаний и возможностей современной техники. Наличие технической возможности может иметь решающее значение для раскрытия особо тяжких преступлений.

Так, следственными органами Ивановской области расследовалось два уголовных дела об убийствах, совершенных на территории г. Иваново в 2017 и 2019 годах [4]. Несмотря на проведенные следственные действия и оперативно-розыскные мероприятия, установить лиц, подлежащих привлечению в качестве обвиняемых, не представилось возможным. При этом по обоим уголовным делам, у следствия имелись важные доказательства – видеозаписи с камер наблюдения, расположенных непосредственно на местах происшествий. По одному из дел на видеозаписи имеется изображение, по всей видимости, преступника, проходящего на место происшествия и идущего следом за ним через буквально 1,5 минуты потерпевшего. По второму делу видеозаписи, имеющиеся в распо-

ряжении следствия, отобразили весь механизм преступной деятельности: приход преступника на место происшествия, выбор позиции для выстрела, непосредственно сам выстрел, уход с места происшествия. Тем не менее, установить личности преступников, выявить какие-либо криминалистически значимые сведения о них не представилось возможным, несмотря на обращения в экспертные учреждения с соответствующими вопросами: при попытках улучшения видеоизображений положительного результата не достигнуто, получены «пиксализации» изображений, не позволяющие идентифицировать запечатленных на них лиц. Это только частные случаи и по стране их достаточно, тем не менее, они наглядно демонстрируют, что при наличии специальной технической возможности обработки полученной следственным путем цифровой информации, результаты расследования имели бы кардинально другой результат.

3. В научной литературе в течение достаточно продолжительного времени обсуждается возможность перевода процесса уголовного судопроизводства в цифровой формат. Высказывались как положительные, так и отрицательные соображения по данному вопросу [5–7]. Ознакомившись с разными точками зрения, проанализировав практический опыт, полагаем, что в настоящее время российская система уголовного судопроизводства не готова к полному переходу на цифровой формат. Переход на «цифру» предполагает прекращение или существенное снижение «бумажного» документооборота. Цифровые технологии в той или иной мере присутствуют в различных стадиях, при проведении различных следственных действий. Это отчетливо заметно, если сравнивать современные реалии с практикой 10–15-летней давности. К примеру, в настоящее время большинство протоколов составляется при помощи компьютера, следственные действия проводятся с применением средств фото или видеофиксации и так далее. Тем не менее, использование компьютера при подготовке процессуальных документов не снимает вопрос об их изготовлении в «бумажном» виде и проставлении подписей, применение средств фиксации хода и результатов следственных действий не отнимает необходимость составления протокола с описанием произведенных действий и полученных результатов. Как предлагается некоторыми авторами, вопрос с проставлением подписей мог бы быть решен посредством использования электронных подписей, однако, не все субъекты правоотношений имеют даже представление о наличии такой возможности.

Возможно использовать цифровой формат судопроизводства «по желанию» субъекта, т.е. предоставить последнему право выразить своё мнение по данному вопросу на начальной стадии расследования. К примеру, при первом допросе подозреваемого ему разъясняется возможность отличного от обычно практикующегося документооборота, и при его согласии дальнейшие следственные действия с участием данного субъекта проводятся в цифровом формате. В таком случае возникают вопросы: как должно быть оформлено такое согласие – сразу в электронном виде или сначала все-таки в бумажном формате; как быть с иными участниками судопроизводства, которые не хотят применения такого формата правоотношений; как компоновать материалы уголовного дела при смешанном формате документооборота уголовного судопроизводства, когда часть лиц высказывается за цифровой процесс, часть настаивает на классическом варианте.

Кроме того, объективными факторами, ограничивающими возможность применения цифрового формата судопроизводства, выступают территориальный масштаб государства (не во всех следственных ситуациях, даже в Центральной России, возможно использование цифровых технологий при выездах на места происшествий, к субъектам правоотношений – либо их использование может быть затруднено по объективным причинам); консервативность населения (боязнь всего нового, непонятного); существенные отличия разных народов страны, в том числе, в их отношении к правоприменительной деятельности.

Таким образом, полагаем, в настоящее время наша система уголовного судопроизводства, несмотря на существенное увеличение количества использования «цифры» в различных практических вопросах, не готова к отказу от существующего порядка документооборота. На данный момент такой переход не согласуется с реалиями российской процессуальной системы и возникающими практическими трудностями. Тем не менее, безусловно, необходимо изучать и обобщать опыт других государств по внедрению цифрового формата документооборота в уголовный процесс, выявляя в первую очередь негативные моменты и встречающиеся на практике недостатки, анализируя, как это может быть использовано в российской действительности. Положительные же стороны такого изменения очевидны.

Библиографический список

1. Состояние преступности в России за январь – декабрь 2019 г.: стат. сб. // Сайт Генеральной прокуратуры РФ. – URL: http://www.genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf.

2. Состояние преступности в России за январь – декабрь 2019 г.: ст. сб. // сайт МВД РФ. – URL: https://мвд.рф/reports/item/19412450/.

3. Мизулина предложила сделать интернет отягчающим обстоятельством преступлений. – URL: https://www.vedomosti.ru/technology/articles/2016/04/27/639325-mizulina-internet

4. Материалы уголовных дел №№ 2017410007, 11902240002000013, находившихся в производстве СУ СК России по Ивановской области, по признакам преступления, предусмотренного ч.1 ст.105 УК РФ, производство по которым приостановлено на основании п.1 ч.1 ст.208 УПК РФ // URL: www.consultant.ru.

5. Долгов А.М. Электронное уголовное дело в досудебных стадиях уголовного процесса в России. – URL: https: //www.kubsu.ru/sites/default/files/users/19203/portfolio/statya_dolgov_a.m.pdf.

6. Зуев, С.В. Электронное уголовное дело: за и против. / С.В. Зуев. – URL: https://cyberleninka.ru/article/n/elektronnoe-ugolovnoe-delo-za-i-protiv/viewer.

7. Зуев, С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы. / С.В. Зуев. – URL: (https://cyberleninka.ru/article/n/tsifrovaya-sreda-ugolovnogo-sudoproizvodstva-problemy-i-perspektivy/viewer.

УДК 343.0:004

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ УБИЙСТВ, ОБУСЛОВЛЕННЫХ РЕЛИГИОЗНОЙ МОТИВАЦИЕЙ

Рябинин Дмитрий Александрович
старший следователь по особо важным делам Главного военного следственного управления Следственного комитета Российской Федерации
Главное военное следственное управление Следственного комитета Российской Федерации, Москва, Россия

В настоящей статье освещаются отдельные вопросы использования цифровых технологий в раскрытии и расследовании убийств, совершенных по религиозным мотивам, автором представлен свой взгляд на их роль и значение в структуре доказывания. Рассматриваются возможные формы позитивного использования информационных технологий в практике расследования таких преступлений с приведением конкретных примеров из судебно-следственной практики.

***Ключевые слова**: цифровые информационные технологии, религия, убийство, религиозно мотивированное убийство, расследование преступлений*.

ON THE USE OF DIGITAL TECHNOLOGY IN THE INVESTIGATION OF MURDERS CAUSED BY RELIGIOUS MOTIVATION

Ryabinin Dmitry Aleksandrovich
senior investigator for particularly important cases of the Main military investigative Department of the Investigative Committee of the Russian Federation
Main military investigative Department of the Investigative Committee of the Russian Federation, Moscow, Russia

This article highlights certain issues of the use of digital technology in the disclosure and investigation of murders committed for religious reasons, the author presents his view on their role and significance in the structure of evidence. Possible forms of the positive use of information technology in the practice of investigating such crimes are examined with specific examples from judicial investigative practice.

***Keywords**: digital information technologies, religion, murder, religiously motivated murder, investigation of crimes.*

В последние годы использование в раскрытии и расследовании преступлений различного рода современных высоких технологий, основанных на применении возможностей электронно-вычислительных машин и информационно-

телекоммуникационных сетей, приобретает все большее значение, вследствие чего не могло не стать объектом пристального внимания со стороны ученых-криминалистов. Ряд из них высказывают обоснованное мнение о необходимости и перспективности разработки теории информационно-компьютерного обеспечения криминалистической деятельности [1, с. 110].

Необходимость использования в процессе расследования преступлений цифровых технологий и компьютерной информации, отвечающих современным требованиям развития науки, неоднократно подчеркивалась руководством Следственного комитета Российской Федерации, была предметом дискуссий на различных научных форумах, конференциях и круглых столах.

Субъектами поисково-познавательной деятельности отмечается, что вследствие использования преступниками в своей противоправной деятельности новых информационных технологий наметились процессы уменьшения количества традиционных трасологических следов на фоне значительного увеличения т. н. цифровых следов преступления, выявление которых без использования в процессе доказывания высоко технологического оборудования представляется весьма проблематичным.

Использование цифровых информационных технологий в расследовании преступлений – урегулированная нормами процессуального права деятельность субъектов доказывания, участвующих в деле лиц и других участников уголовного процесса, состоящая в использовании средств и методов обнаружения, извлечения, сбора, передачи и исследования (обработки) данных в цифровом виде, имеющих доказательственное значение, в целях получения новой информации о состоянии объекта, процесса или явления, а также достижения иного поставленного результата.

Под компьютерной информацией понимается информация, представленная в цифровой форме, необходимой для ее хранения, обработки и передачи средствами вычислительной техники [2, с. 358].

На сегодняшний день невозможно представить себе работу следователя без электронно-вычислительных машин, смартфонов, цифровых фото- и видеокамер, других аналогичных устройств, фиксирующих информацию в цифровой форме.

Как правило, следователь не обладает специальными знаниями в области информационных технологий, не имеет опыта работы с источниками доказательственной информации, находящейся в электронной форме, вследствие чего в большинстве случаев для исследования компьютерной информации, оставленных цифровых следов ему необходима помощь сведущих лиц, в качестве которых могут быть привлечены как специалисты, так и эксперты в области компьютерной техники, информационных сетей и систем.

Объектом пристального внимания правоохранителей ввиду повышенной общественной опасности на современном этапе развития общества является противоправная деятельность деструктивных религиозных групп (культов), ак-

тивно использующих современные информационные технологии, в том числе всемирную систему объединенных компьютерных сетей для хранения и передачи информации (Интернет).

В среде таких групп на первый план по уровню общественной опасности выходят такие преступления, как религиозно мотивированные убийства, совершаемые как лидерами и активными членами религиозных групп, так и отдельными гражданами, использующими в своих преступных действиях религию в качестве инструмента преступного воздействия на личность.

Под убийством, совершенным по религиозному мотиву, мы понимаем умышленное причинение смерти другому человеку, совершенное лицом (лицами) в соответствии с имеющимися у него религиозными (культовыми) представлениями «высшего порядка», связанными с верой в существование обожествляемых сверхъестественных сил, либо лицом (лицами), придерживающимся атеистических взглядов, в целях удовлетворения внутренних духовных потребностей либо приобретения духовных, а также прочих ценностей для себя, иных лиц или представляемой религиозной организации.

Убийства с религиозной мотивацией, как правило, не являются преступлениями, совершенными с использованием средств вычислительной техники и высоких компьютерных технологий, но потребность в применении специальных знаний в этой области по делам указанной категории возрастает в частности ввиду значительного распространения через современные электронные телекоммуникационные средства информации и коммуникации, включая Интернет, радикальных религиозных идей экстремистско-террористического характера.

При расследовании убийств указанной категории следователям приходится сталкиваться с виртуальным пространством, которое образуют носители компьютерной информации, служащей по такого рода преступлениям источником сведений о совершенном противоправном деянии. Зачастую компьютерные сети в религиозных культах используются для создания веб-сайтов религиозного содержания, связи между ячейками и отдельными членами культа, пересылки контактной информации (например, адресов электронной почты), осуществления пропаганды собственного вероучения, обмена идеями и вероучительными документами, ведения переписки и личных дневников, вследствие чего должны подвергаться исследованию с использованием помощи соответствующих специалистов для получения доказательственной информации по делу.

При этом специалист в сфере компьютерной информации должен уметь выполнять следующие функции:

– применять имеющиеся технико-криминалистические средства – специализированные аппаратно-программные комплексы для поиска необходимой информации;

– осуществлять поиск, сбор и анализ компьютерных данных по заданным параметрам, их сохранение и копирование;

– участвовать в производстве осмотра компьютерных данных в зависимости от поставленных ему задач;

– восстанавливать зашифрованные, удаленные, поврежденные и недоступные компьютерные данные;

– давать разъяснения по вопросам, входящим в его компетенцию;

– выполнять иные функции.

В качестве наглядной иллюстрации эффективности использования специальных знаний в области компьютерных технологий при расследовании религиозно мотивированных убийств можно привести следующие примеры из судебно-следственной практики.

Так, по уголовному делу в отношении К., совершившего убийство двух лиц по мотивам религиозной ненависти и вражды, осмотру с участием специалиста подвергался принадлежащий последнему ноутбук, что позволило выявить содержащуюся в нем информацию о работе пользователя в сети Интернет, обнаружить и скопировать видеофайлы националистического содержания, данные о просмотре пользователем подобных фото- и видеофайлов, установить данные о регистрации пользователя в социальной интернет-сети «ВКонтакте», определить устройства, подключавшиеся к ноутбуку [3].

По этому же уголовному делу успешно подвергалась осмотру информация, содержащаяся на аналоговом видеорегистраторе, имевшемся на месте происшествия, позволившая следствию получить отображение произошедшего преступного события.

После участия в проведении соответствующего следственного действия специалист может быть допрошен по его существу, в том числе относительно необходимости дальнейшего назначения по делу компьютерно-технической экспертизы.

Интересующая следствие информация может быть обнаружена и при производстве следственного осмотра изъятых в религиозной группе или у лиц, самостоятельно исповедующих то или иное религиозное учение, электронных материалов (в том числе изображений) различного рода, содержащихся на материальных носителях информации, в том числе электронных, например, в мобильных телефонах.

Так, например, осмотр мобильных телефонных устройств по уголовному делу в отношении Б. и Г., совершивших ритуальное убийство Л. на почве верований в Сатану, позволил выявить в них файлы с изображением отдельных фрагментов проводимых виновными ритуальных церемоний, связанных с причинением смерти человеку [4].

По другому уголовному делу в отношении военнослужащего А., который, являясь приверженцем радикального течения ислама «ваххабизм», на почве религиозной ненависти и вражды причинил смерть троим сослуживцам, в мобильном телефоне последнего была обнаружена информация, содержащая видеоролики с призывами к экстремистской деятельности – противоправным дей-

ствиям (в том числе насильственным) в отношении человека или группы лиц по признакам отношения к религии, уничтожению европейской, христианской цивилизаций, что позволило подтвердить его приверженность радикальным религиозным взглядам [5].

Вместе с этим особую значимость в процессе исследования события убийства, совершенного по религиозному мотиву, приобретает использование цифровых технологий в области судебной медицины для идентификации личности погибших по материалам уголовных дел о культовых убийствах с массовыми человеческими жертвами, когда опознание жертв затруднено большим объемом подлежащих проведению идентификационных работ.

Случаи массовой гибели членов религиозных культов фиксировались, например, в 1978 году в Латинской Америке, где жертвами основателя культа «Народный Храм» стали 912 человек, многие из которых так и остались неопознанными.

В 1993 году лидер культа адвентистского толка «Ветвь Давида» Д. Кореш взорвал штаб-квартиру своей группы вместе с собой и всеми своими последователями в количестве не менее 100 человек.

Один из «рекордов» по численности жертв был поставлен в 2000 году в местечке Канунгу (Уганда), где лидерами культа «Движение за возрождение десяти заповедей Бога» и их приближенными были сожжены в храме и задушены более 600 последователей культа [6, с. 21–36].

Отмечается, что одним из самых распространенных способов такой идентификации является метод фотосовмещения с использованием компьютерной системы «TADD», при котором происходит сравнение проекционных соотношений черепа и головы человека путем наложения их одномасштабных и одноракурсных изображений для создания «виртуальной» пластической реконструкции внешности.

В настоящее время Российским центром судебно-медицинской экспертизы Министерства Здравоохранения и социального развития Российской Федерации совместно со 124 Центральной лабораторией медико-криминали-стической идентификации Министерства обороны Российской Федерации разработаны варианты экспертного применения информационных технологий в виде компьютерных автоматизированных аналитических систем, позволяющих обеспечить эффективный анализ больших массивов молекулярно-генетических экспертных данных для решения задач ДНК-идентификации при массовом поступлении неопознанных тел.

Судебными медиками накоплен значительный опыт работы в очагах массовой гибели людей, при этом, например, в России в целях выполнения указанной задачи используется мобильный комплекс судебно-медицинской экспертизы, частью которого является передвижной морг (на текущий момент времени имеется только в Свердловской области и Республике Саха-Якутия), позволяющий производить работу с массовым количеством тел погибших в местах, значительно удаленных от крупных населенных пунктов.

В разработке находится программный комплекс, позволяющий в случае большой фрагментации тел погибших произвести сопоставление имеющихся фрагментов по большому числу признаков для определения принадлежности каждого фрагмента конкретному телу. Ключевой задачей такого комплекса будет являться компьютерное составление графической модели тел, состоящих из совокупности фрагментарных останков, сходных по биологическим и идентификационным признакам.

Очевидно, что дальнейшее развитие техники и цифровых технологий предопределяет и необходимость разработки новых форм использования компьютерной и иной цифровой информации в процессе расследования убийств, обусловленных религиозной мотивацией. Для этого будут нужны квалифицированные специалисты в области компьютерной информации, способные эффективно противодействовать современным криминальным вызовам.

Библиографический список

1. Россинская, Е.Р. К вопросу о частной криминалистической теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия ТулГУ эконом. и юрид. науки. – 2016. – Вып. 3. – Ч. II. – С. 109–117.

2. Криминалистика: учебник для бакалавров / под ред. Л.В. Бертовского. – Москва: РГ-Пресс, 2018. – 960 с.

3. Уголовное дело № 2-3/15 // Архив Сахалинского областного суда.

4. Уголовное дело № 1-85/13 // Архив Шатурского городского суда Московской области.

5. Уголовное дело № 1.17.0200.0505.000077/18 // Архив военного следственного управления Следственного комитета Российской Федерации по Восточному военному округу.

6. Дворкин, А.Л. Сектоведение. Тоталитарные секты. Опыт систематического исследования. / А.Л. Дворкин. – Издание 3-е, переработанное и дополненное. – Н. Новгород: Издательство «Христианская библиотека», 2007. – 814 с.

УДК 343.3.7:342.76

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА АКТА ТЕРРОРИЗМА ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ КАЗАХСТАН

Сампиев Имран Ахатович
Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан

Общественная опасность акта терроризма состоит в том, что это одна из опасных форм преступного посягательства, основанная на стремлении субъекта посеять у окружающих страх, панику, парализовать общественно полезную деятельность людей, нормальное функционирование государственных органов и тем самым достичь своих антисоциальных целей. В статье рассмотрены особенности уголовно-правовой характеристики данного деяния по законодательству Казахстана.

***Ключевые слова**: преступление, террористический акт, терроризм, уголовное право, состав преступления, Республика Казахстан*

CRIMINAL-LEGAL CHARACTERISTICS OF THE ACT OF TERRORISM UNDER THE LEGISLATION OF THE REPUBLIC OF KAZAKHSTAN

Sampiev Imran Akhatovich
L.N. Gumilov Eurasian National University, Nur Sultan, Kazakhstan

The public danger of an act of terrorism is that it is one of the dangerous forms of criminal encroachment, based on the subject's desire to instill fear, panic among others, paralyze people's socially useful activities, the normal functioning of state bodies and thereby achieve their antisocial goals. The article discusses the features of the criminal legal characteristics of this act under the laws of Kazakhstan.

***Keywords**: crime, terrorist act, terrorism, criminal law, corpus delicti, Republic of Kazakhstan.*

Впервые уголовная ответственность за терроризм в Республике Казахстан была введена с принятием Уголовного кодекса от 16 июля 1997 года. В кодифицированном акте предусматривалась ответственность за терроризм *(ст. 233)*, заведомо ложное сообщение об акте терроризма *(ст. 242)* и посягательство на жизнь государственного или общественного деятеля *(ст. 167)*.

В настоящее время ответственность за акт терроризма предусмотрена ст. 255 Уголовного кодекса Республики Казахстан от 3 июля 2014 года *(далее – УК Республики Казахстан)*. Данная норма дважды изменялась и дополнялась в части увеличения наказания за данное деяние *(законы Республики Казахстан от 22 декабря 2016 года и от 11 июля 2017 года)*.

Согласно ст. 255 УК Республики Казахстан акт терроризма состоит в совершении или в угрозе совершения взрыва, поджога либо других действий, создающих опасность смерти гражданского населения, причинения значительного материального ущерба или наступления других социально опасных по-

следствий. Однако, для квалификации рассматриваемых действий по ст. 255 УК Республики Казахстан, необходимо их совершение в целях нарушения общественной безопасности, запугивания гражданского населения, оказания влияния на принятие решений отечественными государственными органами, иностранным государством либо международной организацией, а также провокации войны или ухудшения международных отношений.

Следует отметить, что понятие акта терроризма определено в п. 6) ст. 1 Закона Республики Казахстан от 13 июля 1999 г. № 416 «О противодействии терроризму», которое по своему содержанию не соответствует понятию, изложенному в ст. 255 УК Республики Казахстан с точки зрения целей этих действий.

Вместе с тем, согласно п. 7 ст. 23 Закона Республики Казахстан от 6 апреля 2016 года «О правовых актах» термины и определения, используемые в нормативном правовом акте, должны соответствовать дефинициям вышестоящего нормативного правового акта, регулирующего однородные общественные отношения. В связи с этим понятие акта терроризма, определенное в пп. 6) ст. 1 Закона Республики Казахстан от 13 июля 1999 года «О противодействии терроризму» необходимо привести в соответствие с понятие акта терроризма ст. 255 УК Республики Казахстан.

Отсутствие формулировок и их нечеткость приводят к смешению понятий, что, в свою очередь, неизбежно приводит к снижению эффективности правового регулирования, возникновению правовых конфликтов [1].

Общественная опасность акта терроризма состоит в том, что это одна из опасных форм преступного посягательства, основанная на стремлении субъекта посеять у окружающих страх, панику, парализовать общественно полезную деятельность людей, нормальное функционирование государственных органов и тем самым достичь своих антисоциальных целей [2].

Объективными признаками рассматриваемого преступления являются совокупность признаков, составляющих объект и объективную сторону данного противоправного деяния.

Структурно рассматриваемое террористическое преступление включено законодателем в главу 10 Особенной части УК Республики Казахстан, соответственно, его объектом являются общественные отношения, обеспечивающие общественную безопасность. В Законе Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» общественная безопасность определяется через «состояние безопасности жизни, здоровья и благополучия соотечественников, духовных и моральных ценности нашего общества и системы социального обеспечения от реальных и потенциальных угроз, при обеспечении стабильности и целостности казахстанского общества *(п. 1) ст. 4)*.

В качестве дополнительного объекта выступают жизнь и здоровье гражданского населения, собственность, существующий порядок управления и функционирования государственного органа, иностранного государства, международной организации и т.д. В связи с этим рассматриваемое деяние должно квалифицироваться как многообъектное противоправное деяние.

Для правильного понимания сущности и содержания указанного деяния, отграничения от других преступлений, правильной квалификации неоценима роль точного понимания объективной стороны.

С объективной стороны, это террористическое преступление является общественно опасным деянием в форме действия.

Основываясь на анализе рассматриваемого противоправного деяния, объективная сторона представляет собой сложных характер и проявляется в одном из следующих действий:

– совершение взрыва, поджога или других действий, создающих опасность смерти людей, влекущих значительный материальный ущерб или наступление других социально опасных последствий;

– угроза совершения взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий.

– угроза совершения взрыва, поджога или других действий, создающих опасность смерти людей, влекущих значительный материальный ущерб или наступление других социально опасных последствий.

Законодатель не определяет, что следует понимать под иными действиями в этом контексте. По нашему мнению, они должны включать те действия субъекта преступления, которые создают опасность смерти людей, причинения значительного материального ущерба или наступления других общественно опасных последствий. В качестве таковых следует рассматривать совершение аварий, катастроф, блокирование аэропортов, авто и железнодорожных станций и вокзалов, метрополитенов, путей сообщений и т. д.

Обязательным условием, выраженным в качестве альтернативы, является создание такой опасности, как гибель людей *(двух или более, независимо от гражданства, своих граждан, иностранцев, лиц без гражданства)*, причинения значительного материального ущерба или других социально опасных последствий.

Для привлечения к уголовной ответственности достаточно лишь создать опасность смерти людей, причинения значительного ущерба собственности или наступления других общественно опасных последствий. Оконченным составом рассматриваемого противоправного деяния является не только совершение этих действий, но и угроза их совершения. Однако угроза должна иметь такие качественные характеристики, как реальность *(т.е. имелись основания полагать, что она можно может быть реализована)* и действительность. В данном контексте не зависит какого содержания угроза *(устная или письменная)*, как она озвучена/передана *(напрямую или через кого-либо, или через различные средства связи)*.

Субъективные признаки рассматриваемого террористического преступления представляют собой совокупность признаков, составляющих субъект и субъективную сторону акта терроризма.

В отличие от объективной стороны, представляющей собой внешний акт преступного деяния виновного, субъективной стороной является внутреннее, психическое осознание сущности и направленности деяния. Она определяет психическое отношение субъекта к совершенному им социально опасному деянию и его последствиям.

Указанное деяние с субъективной стороны совершается только в форме прямого умысла. В данном контексте субъект преступления понимает, что он совершает или угрожает совершить такие действия, как взрыв, поджог или другие действия, которые создают опасность гибели граждан, причинения значи-

тельного материального ущерба или наступления других общественно опасных последствий, а также желает совершить такие действия. Исходя из содержания и конструкции рассматриваемого деяния оно не может быть совершено в форме неосторожности.

Исходя из своей конструкции, рассматриваемое деяние включает такие цели, как нарушение общественной безопасности, запугивание населения, оказание влияния на принятие решений отечественными государственными органами, зарубежным государством или международной организацией, а также провокация войны или ухудшения международных отношений.

Субъектом данного деяния является вменяемое физическое лицо *(гражданин Республики Казахстан, иностранец, лицо без гражданства)*, достигшее 14-летнего возраста *(ч. 2 ст. 15 УК Республики Казахстан)*.

Квалифицирующими признаками данного террористического преступления (ч. 2 ст. 255 УК Республики Казахстан):

1) неоднократность;

2) применение оружия или предметов, используемых в качестве оружия, взрывчатых веществ или взрывных устройств, создающие реальную угрозу жизни и здоровью людей.

Квалифицирующими признаками данного террористического преступления *(ч. 2 ст. 255 УК Республики Казахстан)* являются:

1) неоднократность;

2) применение оружия или предметов, используемых в качестве оружия, взрывчатых веществ или взрывных устройств, представляющих реальную угрозу жизни и здоровью людей.

Под неоднократностью в данном контексте следует понимать совершение двух или более актов терроризма, при этом если за ранее совершенное данное деяние виновный не был осужден или освобожден от уголовной ответственности по основаниям, установленным законом.

Под оружием понимаются «устройства и предметы, конструктивно предназначенные для поражения живой или иной цели, а также для подачи сигналов. Оружие по своему предназначению подразделяется на боевое ручное стрелковое и холодное, гражданское и служебное».

Предметами, используемыми в качестве оружия, являются предметы (средства), с помощью которых может быть нанесена реальная угроза жизни и здоровья людей, независимо от того, были ли они подготовлены заранее.

Под взрывчатыми веществами следует понимать порох, тротил, нитроглицерин, пироксилин, аммонал и другие химические вещества и их смеси, обладающие способностью к взрывчатым реакциям, на приобретение и хранение которых требуется специальное разрешение.

Под взрывными устройствами понимаются заводские или самодельные изделия, предметы (механизмы), предназначенные для производства взрыва.

Особо квалифицирующими признаками рассматриваемого деяния *(ч. 3 ст. 255 УК Республики Казахстан)* являются:

1) применение или угроза применения оружия массового поражения, радиоактивных материалов и совершение или угроза совершения массовых отравлений, распространения эпидемий или эпизоотий, а также других действий, которые могут привести к массовой гибели людей;

2) причинение смерти человека по неосторожности или других тяжких последствий.

Под оружием массового поражения понимается «химическое, бактериологическое (биологическое), радиологическое, ядерное и токсинное оружие».

Радиоактивными веществами признаются «любые материалы природного или техногенного происхождения в любом агрегатном состоянии, содержащие радионуклиды».

Под отравлением следует понимать «заболевание (состояние), возникающее при остром (одномоментном) или хроническом (длительном) воздействии на человека химических, биологических и иных факторов среды обитания».

Эпидемия – это «массовое распространение инфекционного заболевания, существенно превышающее обычно регистрируемый уровень заболеваемости».

Под эпизоотией понимается «массовое распространение особо опасных и других инфекционных болезней животных на территории соответствующей административно-территориальной единицы».

Под иными действиями в рассматриваемом контексте следует понимать такие действия, которые могут привести к массовой смерти людей. Обязательным является наличие такого признака как «массовость».

Причинение смерти человека состоит в наступлении биологической смерти физического лица в результате акта терроризма.

Под иными тяжкими последствиями акта терроризма следует понимать нанесение тяжкого вреда здоровью нескольким лицам или вреда средней тяжести многим лицам, а также причинение крупного имущественного ущерба.

Субъективная сторона преступления, предусмотренного п. 2) ч. 3 ст. 255 УК Республики Казахстан характеризуется виной с двойной формой. По отношению к акту терроризма вина характеризуется прямым умыслом, а по отношению к наступившим последствиям (смерть или другие тяжкие последствия) - неосторожностью. Однако в целом это преступление признается совершенным умышленно.

Объективная сторона ч. 4 ст. 255 УК Республики Казахстан состоит:

– из посягательства на жизнь человека, совершенного с целью нарушения общественной безопасности, запугивания населения, оказания влияния на принятие решений отечественными государственными органами, зарубежным государством или международной организацией, а также провокация войны или ухудшения международных отношений;

– посягательства на жизнь государственного или общественного деятеля, совершенное с целью нарушения общественной безопасности, запугивания населения, оказания влияния на принятие решений отечественными государственными органами, зарубежным государством или международной организацией, а также провокация войны или ухудшения международных отношений;

– посягательства на жизнь человека *(гражданина, иностранца или лица без гражданства)*, связанное с нападением на лиц или организаций, пользующиеся международной защитой, здания, сооружения, захватом заложника, зданий, сооружений, средств связи и сообщений, угон, а также захват воздушного или водного транспорта, железнодорожного подвижного состава или другого общественного транспорта.

Под посягательством на жизнь понимается умышленное противоправное причинение смерти (убийство) или покушение на убийство, то есть умышленные действия, непосредственно направленные на причинение смерти.

По конструкции состав противоправного деяния (ч. 4 ст. 255 УК Республики Казахстан) является формальным. Преступление считается оконченным с момента посягательства, независимо от наступивших последствий.

Следует отметить, что ст. 255 УК Республики Казахстан содержит примечание, в котором предусмотрены условия, при наличии которых лицо освобождается от уголовной ответственности. Так, согласно данной поощрительной норме физическое лицо (гражданин, иностранец или лицо без гражданства), участвующее в подготовке акта терроризма, освобождается от уголовной ответственности, если оно своевременно предупредило государственные органы или иными действиями помогло предотвратить акт терроризма, и, если в его действиях не содержится состав иного противоправного деяния.

Примечание к рассматриваемой статье предполагает наличие добровольной деятельности, направленной на информирование об обстоятельствах совершенного преступления – подготовке акта терроризма. О добровольности совершаемых действий должны свидетельствовать объективные (наличие у лица возможности продолжать преступную деятельность или скрываться от следствия и суда) и субъективные обстоятельства (осознание лицом этой возможности и желание ею воспользоваться).

Положительная роль данного примечания состоит и в том, что в настоящее время у сотрудников правоохранительных и специальных государственных органов имеется юридическое основание обещать виновным не привлекать их к ответственности в случае своевременного предупреждения государственных органов или иным способом содействовать путем добровольного информирования о подготовке акта терроризм, способствования выявления соучастников, осуществляющих такую подготовку, осуществляющих, организовавших или финансировавших подготовку акта терроризма, предоставления информации о месте ее проведения.

В качестве условий освобождения от уголовной ответственности за подготовку акта терроризма, следовательно, выступают следующие обстоятельства:

– добровольность сообщения о подготовке акта терроризма;

– способствование выявлению других лиц, осуществляющих такую подготовку акта терроризма, осуществляющих, организовавших или финансировавших такую подготовку;

– предоставление информации о месте проведения подготовки;

– отсутствие в действиях виновного иного состава противоправного деяния.

Библиографический список

1. Бачило, И. Л. Информационное право. Роль и место в системе права Российской Федерации / И. Л. Бачило // Государство и право. – 2001. – № 2. – С. 5–9.

2. Борчашвили, И. Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (том 2). / И. Ш. Борчпшвили. – Алматы: Жеті жарғы, 2015. – 504 с.

УДК 343.1

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ВИДЕОЗАПИСИ КАК СРЕДСТВА ФИКСАЦИИ РЕЗУЛЬТАТОВ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Селезнев Виктор Михайлович
Красноярский государственный аграрный университет, Красноярск, Россия

В данной статье рассматривается одна из актуальных проблем фиксации результатов следственных действий, как видеозапись. Изложены возможности, проблемы и пути их решения.

Ключевые слова: *криминалистическая видеозапись, фотограмметрия, протокол следственного действия, электронный носитель.*

TO THE QUESTION OF USING VIDEO RECORDING AS A MEANS OF RECORDING THE RESULTS OF INVESTIGATIVE ACTIONS

Seleznev Victor Mikhailovich
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article deals with one of the actual problems of fixing the results of investigative actions, such as video recording. Opportunities, problems, and ways to solve them are outlined.

Keywords*: forensic video recording, photogrammetry, investigative report, electronic media.*

Криминалистическая видеозапись находит все более широкое использование в современной следственной практике. Это объясняется, во-первых, ее несомненными достоинствами и, во-вторых, постоянным совершенствованием видеоаппаратуры.

Использование видеозаписи имеет большое значение для успеха расследования преступлений и может быть весьма эффективным способом фиксации практически при всех следственных действиях – от осмотра места происшествия до производства судебной экспертизы. Преимущества применения видеозаписи как технического средства фиксации заключаются в доказательственной информации, полученной с ее помощью, и отличается объективностью, наглядностью, отсутствием искажений с течением времени и многократного воспроизведения.

Использование технических средств фиксации, основанных на цифровых технологиях, позволяет фиксировать, хранить и передавать информацию в электронно-цифровой форме, т. е. в форме электронного документа. Данная форма предоставления информации обеспечивает хорошее качество фиксации, компактность, надежность, быстроту и удобство в использовании технических средств фиксации.

Расширенный анализ в прикладном, криминалистическом аспекте, современного состояния и возможностей использования технических средств цифровой видеофонограмм для обеспечения процесса производства криминалистических экспертиз, а также разработка методических рекомендаций по данной теме, представляются актуальными на современном этапе развития криминалистической науки и техники.

Видеофогограмма, как способ фиксации криминалистически значимой информации, на наш взгляд, является наиболее перспективным, доступным, качественным, универсальным в процессуальном и в техническом аспекте.

В настоящее время существуют определенные проблемы применения видеозаписи как средства фиксации результатов следственных действий, связанные с отсутствием (или недостаточном количестве) технических средств и возможностью качественной видеосъемки, так и допущением определенных методических нарушений (процессуальных и технических) [1].

К наиболее часто встречающимся типичным ошибкам можно отнести следующие:

– отсутствует четкое распределение ролей между участниками следственного действия (следователя и специалиста-криминалиста), съемка производится в хаотичном порядке, резкими движениями, и в кадре изображение получается слабовидимым или размытым. Это объясняется отсутствием четко разработанного сценария следственного действия;

– при выборе точек съемки оператор (специалист-криминалист) не учитывает направление световых потоков, что влечет за собой значительное затемнение кадра (т.е. производится лишь аудиозапись следственного действия);

– не учитывается определение композиции кадра (объект съемки фиксируется не полностью);

– отсутствует настройка экспозиции и фокуса (в кадре видны нечеткие изображения), нет грамотного определения направления съемки (фронтального, диагонального).

Для решения возникающих проблем предлагается:

– использовать дополнительные технические средства (штативы, выносные микрофоны, средства дополнительного освещения и т.п.);

– видеофонограмма должна вестись непрерывно (в случае вынужденного прерывания видеозаписи необходимо ранее установленными условными знаками сообщать причину остановки, а также точное время начала, окончания и возобновления видеозаписи);

– необходимы четкие комментарии событий, происходящих в кадре, или объектов съемки со стороны лица, производящего съемку;

– фиксировать результаты видеозаписи в протоколе следственного действия в соответствии с нормами УПК.

В протоколе следственного действия, при применении цифровой видеозаписи, следует отражать информацию, которая имеет определенное техническое и процессуальное значение:

а) тип и марка цифровой (аналоговой) видеокамеры;

б) название и характеристики объектива;

в) режим записи и степень сжатия видеозаписи (например, SP или LP);

г) тип, марка и емкость носителя информации, на который производилась видеозапись (HD, флеш карта, DVD-диск, мини DV и т. п.);

д) тип и марка внешнего микрофона и других средств (если они использовались);

е) условия, в которых осуществлялась цифровая запись (погодные условия и характер освещения);

ж) кем производилась видеосъемка;

з) при составлении планов и схем следователем на них должны быть указаны точки, с которых производилась видеозапись;

и) тип, марка устройства, при помощи которого осуществлялась демонстрация видеофонограммы;

к) при копировании зафиксированной информации на иной носитель следует указывать, что копирование осуществлялось без использования персонального компьютера, например посредством многофункционального записывающего устройства, на одноразовый диск DVD-R, либо с использованием персонального компьютера [2].

В протоколе следственного действия, возможно, внести и дополнительную информацию о носителе, для исключения подмены диска. При описании носителя (DVD ± R диска) для исключения возможности последующей его подмены или внесения каких-либо изменений в протокол необходимо занести следующую информацию о носителе:

а) тип (miniDV, digital 8, DVD, microMV), марка (производитель, название), емкость диска или носителя (Gb, Mb);

б) продолжительность записи (в секундах);

в) размер (контрольная сумма) записанной информации (например, 536 Mb, 1,3 Gb и т. п.);

г) индивидуальный номер производителя на внутреннем радиусе диска (например, 06/01/2012235:15.57).

В настоящее время существует проблема возможного редактирования цифровых видеозаписей [3]. Для исключения компьютерного редактирования, внесения каких-либо изменений и процессуального закрепления данных, полученных цифровыми видеокамерами, я предлагаю проведение следующих мероприятий в процессе производства следственных действий:

– продемонстрировать цифровую видеозапись участникам следственного действия;

– продемонстрированные данные зафиксировать на носителе (копировать, записать, отцифровать);

– удостоверить подписями участников следственного действия (упаковать, опечатать);

– приобщить к материалам дела в виде приложения.

На каждом из вышеперечисленных этапов существует определенная специфика, в зависимости от вида аппаратуры и типа носителя используемой видеокамеры.

Так, например, демонстрация цифровой записи участникам мероприятия в зависимости от места проведения следственного действия (открытая местность, кабинет следователя) возможна на таких средствах визуализации, как:

1) ЖК-дисплей видеокамеры;

2) монитор компьютера;

3) телевизионный экран.

В связи с вышесказанным можно сделать вывод, что объективное и полное исследование видеофонограмм, которые имеют значение для расследования уголовного дела, на современном этапе практически невозможно без использования научных знаний, средств специальной техники и разработанных на их основе криминалистических методик, которые являются необходимым и преимущественно единственным инструментом проведения расследования и оперативно-розыскных мероприятий.

Существует прямая связь между процессуальной значимостью доказательств и уровнем научных достижений, методик, технических средств, которые применялись для их получения и закрепления. Полученные экспертом (специалистом) данные опираются на научно-технические достижения и в результате этого приобретают силу доказательств.

В целом научно-прикладные и связанные с ними процессуальные вопросы использования информации, записанной на видеоносителях, могут быть решены лишь при условии комплексного подхода, который должен предусмотреть меры, направленные на совершенствование уголовно- процессуального законодательства, внедрение новых подходов и методик относительно применения средств записи видеоинформации на цифровые и иные носители, экспертного исследования полученных при этом результатов, выработки критериев, позволяющих учитывать информацию на видеофонограммах в качестве доказательств в процессе уголовного судопроизводства.

Библиографический список

1. Булгаков, А.Г. Судебная фотография и видеозапись: учебник / А.Г. Булгаков, В.А. Зотчев, А.А. Курин; Волгоградская академия. – Волгоград, 2006. – 849 с.

2. Селезнев, В.М., Криминалистика. Часть 1. Основы криминалистической техники: учеб. пособие / В.М. Селезнев, М.Э. Червяков. – Красноярск: Изд-во КрасГАУ, 2019. – 355 с.

3. Сильнов, М. К вопросу о допустимости использования цифровых технологий в доказывании при расследовании преступлений / М. Сильнов. – URL: www.silnov.newmail.ru (дата обращения: 22.02.2020).

УДК 343:004

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ПЕРЕСМОТР ИТОГОВОГО РЕШЕНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ, В СУДЕ С УЧАСТИЕМ ПРИСЯЖНЫХ ЗАСЕДАТЕЛЕЙ

Середа Ольга Викторовна
Аспирант
Красноярский государственный аграрный университет, Красноярск, Россия

Автор статьи рассматривает то, как информация, полученная присяжными из внесудебных источников, таких как социальные сети, электронные издания, телевидение и интернет, влияют на качество решения, принимаемого коллегией. Так же автор анализирует, какое количество решений, вынесенных с судом присяжных в дальнейшем обжалуется и можно ли говорить о том, что решения, которые подвергнуты изменениям, были приняты присяжными под давлением мнения извне.

Ключевые слова: *присяжные, приговор, обжалование, цифровые технологии, познавательная деятельность.*

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE REVIEW OF THE FINAL DECISION IN CRIMINAL PROCEEDINGS, IN COURT WITH THE PARTICIPATION OF JURORS

Sereda Olga Viktorovna
Postgraduate student
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

The author examines how information obtained by the jury from non-judicial sources, such as social networks, electronic publications, television and the Internet, affect the quality of the decision made by the panel. The author also analyzes how many decisions made by the jury are further appealed and whether it can be said that the decisions that were changed were made by the jury under the pressure of external opinion.

Keywords*: jury, verdict, appeal, digital technologies, cognitive activity.*

Развитие политики внедрения цифровых технологий в уголовное судопроизводство [1] и перспективы применения технологий «блокчейн» в данной сфере [2] распространяются на разные его институты, затрагивая и вопросы информационной безопасности [3], и особенности правового статуса участников судопроизводства [4], и вопросы собирания и использования цифровых доказательств [5] и многое другое [6]. Тем не менее, некоторые вопросы носят смежный характер. Остановимся на суде присяжных.

Говоря о суде присяжных в России, нельзя сравнивать его с той моделью, что принята, допустим, в США, где уголовные дела в обычном течении судопроизводства рассматриваются судом с коллегией присяжных, а не напротив, когда это становится исключением. Но, учитывая, что уголовное судопроизводство нацелено на расширение количества рассмотрения уголовных дел судом присяжных, нельзя оставлять без внимания те факторы, которые мешают принятию качественного решения и из-за которых они могут быть отменены или изменены после прохождения процедуры обжалования.

В современном мире люди ведут не только реальную социальную активность, но и виртуальную – в цифровом мире. Соответственно, воздействовать на мнение человека можно не только при личном контакте с ним, а посредством цифровых технологий, в его виртуальной жизни – через социальные сети, различные мессенджеры, информационные порталы. Если во время рассмотрения громкого уголовного дела присяжный захочет исследовать те мнения и доказательства, которые представлены в цифровом мире, а не в зале суда, будет ли он считаться беспристрастным? А если дело широко освещается СМИ и невозможно от такой информации «увернуться»?

«Присяжные не должны самостоятельно искать в интернете что-либо, относящееся к процессу, посылать запросы о «дружбе» или каким-либо еще образом связываться с участниками процесса, писать сообщения, размещать онлайн фото или видео, писать в блоге или писать в твиттере что-либо, относящееся к процессу», – говорится в докладе Нью-Йоркской ассоциации юристов, посвященном поведению присяжных в соцсетях [7, с. 457].

Не редки моменты, когда присяжные обсуждают дома с семьей или друзьями подробности рассматриваемого уголовного дела, и, если у данного присяжного есть авторитетный родственник или друг, то к его мнению он скорее всего прислушается. В США адвокаты защиты не редко пользуются не только своим ораторским мастерством, но и розыском влияния на определенный круг присяжных, что, в большинстве случаев помогает им склонить коллегию на свою сторону. И, если раньше, для таких действий было необходимо личное знакомство и личные встречи с человеком, то сейчас это можно сделать невзначай, через социальные сети или мессенджеры.

В России вопросом о том, насколько ответственно присяжные подходят к процессу, озабочены, казалось бы, меньше, чем на Западе. Больше волнует юридическую общественность вопрос, будет ли в стране вообще эффективный институт присяжных. Отвечая на вопрос журналистов о его перспективах, председатель ВС Вячеслав Лебедев отметил: «Я согласен с тем, чтобы присяжные были по более широкой категории дел. Если правозащитники считают, что надо ввести суды присяжных по всем абсолютно категориям дел – ради Бога, почему же я должен возражать?»[8]. Однако, несмотря на видимое отсутствие возражений у представителей властей, суд присяжных в России используется не слишком часто: по итогам 1 полугодия 2018 года судами присяжных рассмотрено 740 дел, в 4 % случаев вынесены оправдательные приговоры. Тогда как в 2014 году это было 308 уголовных дел и 14 % оправдательных пригово-

ров [9]. Надежда подсудимых о том, что «народные судьи» смогут проникнуться и разобраться в деле не оправдывается.

Когда в России совершается громкое уголовное преступление, то часто следователям приходится сталкиваться с журналистами, которые в своем желании поднять рейтинг своего информационного издания или личного блога, нередко освещают расследование, а потом и судебное разбирательство под своим углом понимания, что произошло и кто виновен в этом. И, при рассмотрении такого уголовного дела судом присяжных, присяжным нередко приходится сталкиваться с информацией, которая не относится к уголовному расследованию, но несет яркий эмоциональный окрас по фактам, изложенным в уголовном деле.

Согласно той же статье 333 присяжным запрещено собирать сведения по уголовному делу вне судебного заседания, в том числе нельзя этого делать с использованием социальных сетей или любых СМИ. Однако на практике весьма сложно проконтролировать поведение присяжных вне здания суда, поэтому на практике нередки случаи собирания ими информации на просторах цифровой сети. Некоторые эксперты приводят случаи отмены приговоров из-за чрезмерной активности присяжных в соцсетях. «Верховный Суд РФ отменил оправдательный приговор по делу О., поскольку был установлен факт создания девятью присяжными заседателями группы в социальных сетях, объединяющих присяжных заседателей по делу О., в которой они обсуждали вопросы, связанные с рассмотрением данного дела. По другому делу приговор был отменен Верховным Судом РФ, т. к. «…положение закона нарушено старшиной присяжных заседателей, который… счел своим гражданским долгом самому провести расследование, для чего неоднократно выходил на место преступления …» – указал Сергей Насонов, советник Федеральной палаты адвокатов России [8].

Рассмотрим статистику пересмотра уголовных дел в апелляционной инстанции по приговорам, вынесенным судом присяжных, всего их было рассмотрено 201:

– изменены без изменения квалификации 12, что равно 6 %,

– отменены оправдательные с передачей на новое судебное разбирательство 13, что равняется 6,5 %.

А эти статистические данные говорят нам о том, что 12,5 % вынесенных ранее решений судом присяжных заседателей оказались некачественными. Не исключено, что это произошло в связи с тем, что присяжные, вместо беспристрастного принятия решения по тем фактам, что были получены следствием и озвучены в ходе судебного разбирательства, подверглись влиянию информации, полученной посредством цифровых технологий о которым мы упоминали выше [9].

Чем же спасаются на Западе в данной непростой ситуации? Законы каждого штата решают это различными способами, но, как правило во всех содержится такая мера – как отстранение присяжного. Если была зафиксирована активность присяжного в деле отыскания новых фактов по рассматриваемому уголовному делу, или если присяжный или присяжные проводят обсуждение

материалов уголовного дела вне стен суда, то стоит рассматривать вопрос об отстранении такого присяжного или присяжных, дабы не подвергать подсудимого неоправданному осуждению или оправданию.

Библиографический список

1. Бертовский, Л.В. Цифровое судопроизводство: проблемы становления / Л.В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства: сб. мат-лов междунар. науч.-практ. конф. 2018. – С. 173–178.
2. Бертовкий, Л.В. Перспективы применения технологий «блокчейн» в уголовном судопроизводстве / Л.В. Бертовский, Г.С. Девяткин // Деятельность правоохранительных органов в современных условиях: сб. мат-лов XXIV междунар. науч.-практ. конф. – Иркутск, 2019. – С. 115–118.
3. Курбатова, С.М. Некоторые аспекты информационной безопасности личности в контексте права на свободу и «не насилие» / С.М. Курбатова. // Критика насилия: PRO RT CONTRA: мат-лы регион. науч. конф. – Красноярск, 2019. – С. 63–66.
4. Курбатова, С.М. Нормы модельного УПК СНГ как гарантия соблюдения правового статуса участников уголовного процесса с ограниченными когнитивными способностями / С.М. Курбатова // Енисейские политико-правовые чтения: сб. науч. ст. по мат-лам XII Всерос. науч.-практ. конф. / отв. ред. Г.Л. Москалев, Е.А. Акунченко. – Красноярск, 2019. – С. 146–151.
5. Щедрин, Д.Н. Проблемы собирания и использования цифровых доказательств в уголовном судопроизводстве / Д.Н. Щедрин, С.М. Курбатова // Актуальные проблемы уголовного права, уголовного процесса и криминалистики: сб. науч. тр. / под ред. В.Д. Зеленского. – Краснодар, 2019. – С. 196–200.
6. Уголовно-процессуальное право / под ред. Л.В. Бертовского, В.Н. Махова. – М.: Проспект, 2020. – 656 с.
7. David W. Neubauer, Henry F. Fradella, America’s courts. Cengage, 2017.
8. Правовой портал Право.ру. – URL: https://pravo.ru/story/view/126831.
9. Официальный сайт Судебного Департамента РФ. Судебная статистика. – URL: http://cdep.ru/index.php?id=79&item=4758.

УДК 004:34

НЕКОТОРЫЕ ПРОБЛЕМЫ АВТОРСКИХ ПРАВ НА МУЛЬТИМЕДИЙНЫЕ ПРОДУКТЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Силюк Татьяна Юрьевна
старший преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

Статья рассматривает проблемы авторских прав на мультимедийные продукты Российской Федерации. Таковое понятие, как мультимедийный продукт, не имеет закрепления в гражданском законодательстве и поэтому приводит к проблемам квалификации данного объекта. Автор рассматривает лишь несколько проблем в сфере авторских прав на мультимедийные продукты, а также возможные пути решения в нынешнем законодательстве.

***Ключевые слова**: авторское право, объект, мультимедийный продукт, интеллектуальная деятельность, сложный объект, квалификации.*

SOME COPYRIGHT ISSUES FOR MULTIMEDIA PRODUCTS IN THE RUSSIAN FEDERATION

Silyuk Tatyana Yuryevna
Senior lecturer of the Department of civil law and process of the Law Institute
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

The article considers the problems of copyright for multimedia products of the Russian Federation. Such a concept as a multimedia product is not fixed in civil legislation and therefore leads to problems of qualification of this object. The author considers only a few problems in the field of copyright for multimedia products, as well as possible solutions in the current legislation.

***Keywords**: copyright, object, multimedia product, intellectual activity, complex object, qualifications*.

Известно, что с развитием информационных и компьютерных технологий в Российской Федерации появляются новые результаты интеллектуальной деятельности, такие как мультимедийные продукты. Мировое господство компьютерных технологий всё больше захватывает все сферы жизни и деятельности нынешнего общества. Многочисленные интернет-магазины, социальные сети, интернет-каналы и компьютерные игры прочно связались с обществом, и являются неотъемлемой частью отношений в таком обществе. Мультимедийные продукты на сегодняшний день ведут к появлению новых форм творчества и являются средствами коммуникации.

Но, к сожалению, несмотря на обширное применение данного вида продукта, человеческие отношения, возникающие по поводу мультимедийных результатов в полной мере не урегулированы российским законодательством.

В юридической литературе такой вид объекта исследован не в полной мере и лишь изредка упоминается у таких авторов как Б.М. Гонгало, Ю.А. Жук и т.д. [1, 2]. Понятие мультимедийный продукт хоть и признан Гражданским кодексом РФ, но в нём отсутствуют нормы, которые регулируют создание и использование данного объекта. Все это привило к возникновению многих проблем, которые порождают не только противоречия между нормами права, но и влекут за собой разного рода правонарушения.

Важной проблемой является проблема законодательного закрепления понятия, а именно законодательного пробела, который влияет на квалификацию данного объекта. Сам термин мультимедийного продукта указан лишь в п. 1 ст. 1240 ГК РФ и то в качестве сложного объекта на ряду с такими объектами как кинофильм, театрально-зрелищное представление и база данных [3].

Для закрепления понятия предлагается, в подраздел 3, главу 6 ГК РФ после ст. 141.1. Цифровые права дополнить ст. 141.2 Мультимедийные продукты.

Мультимедийными продуктами признаются сложные объекты, под которыми понимаются компьютерные игры, презентации, учебники, энциклопедии, интернет-сайты, социальные сети, различные бизнес-приложения и т.п. Данный перечень объектов стоит оставить открытым, так как стремительно развивается наука и техника в нынешнем обществе. А если их ограничить, многим авторам будет сложно интерпретировать формы интеллектуальной деятельности, которые можно отнести к мультимедийным продуктам.

Так же предлагается главу 71 после параграфа 5 дополнить параграфом 5.1 Право на создание и использование мультимедийных продуктов. Закрепить в нём изготовителя мультимедийных продуктов, исключительное право изготовителя мультимедийных продуктов, срок действия исключительного права изготовителя мультимедийных продуктов и действие исключительного права изготовителя мультимедийных продуктов на территории РФ.

Изучая судебную практику, было найдено одно решение, связанное с нарушением авторских прав на мультимедийный продукт.

Две организации обратились к ряду юридических лиц с взысканием суммы компенсации за нарушение авторских прав на мультимедийную продукцию, а точнее за использование в продаже произведения на электронных носителях без согласия правообладателя.

Ответчиками в качестве доказательств был представлен лицензионный договор, в котором стороны пришли к согласию по передачи прав на использование названия, логотипа, название видео-клипов и записей концертов, сценарий, имена и изображения персонажей, фонограммы и исполнения, а также на иные объекты, оговоренные в приложениях к договору.

На основании изложенного суд приходит к выводу, что требования истцов являются не обоснованными и подлежащими отклонению в полном объеме как применительно к спорным фонограммам, так и к товарному знаку, в отношении всех ответчиков [4].

Проанализировав судебную практику Арбитражных судов РФ по авторским правам на мультимедийные продукты, 1216 дел, можно сделать следующие выводы:

– в решениях суды очень редко рассматривают термин мультимедийного продукта как самостоятельного объекта, лишь в одном деле фигурируют авторские права на мультимедийный продукт;

– мультимедийные продукты рассматриваются в совокупности со сложными объектами на основании п. 1 ст. 1240 ГК РФ.

Так из выше изложенного следует немедленное закрепление понятия, а так же создание и регулирование такого объекта как мультимедийный продукт.

Библиографический список

1. Гонгало, М.В. Гражданское право: учебник. В 2 т. / М.В. Гонгало. – Т. 1. – 3-е изд., перераб. и доп. – М.: Статут, 2018.

2. Жук, Ю.А. Информационные технологии. Мультимедиа / Ю.А. Жук. – М.: Лань, 2018.

3. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СПС Консультант плюс: законодательство.

4. Решение Арбитражного суда г. Москвы от 07.02.2014 по делу № А40-156369/2013 // URL: https://sudact.ru (дата обращения: 01.03.2020).

УДК 340.6:004

ОБЪЕКТ И ПРЕДМЕТ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Скобелина Галина Петровна
старший преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья посвящена преступлениям, указанным в гл.28 УК РФ. Особенности объекта и предмета этих преступлений вызывают много споров и дискуссий в науке уголовного права, что приводит к сложностям квалификации преступлений для правоприменителя. Хотя объем статьи не позволяет глубоко и детально исследовать объект и предмет преступлений, предусмотренный ст. ст.272,273 и 274 УК РФ, хотелось бы в общих чертах обозначить эти элементы состава преступления.

Ключевые слова: *преступления в сфере компьютерной информации, объект и предмет преступления, нарушение правил эксплуатации средств хранения, преступные последствия, определение имущественного вреда.*

OBJECT AND SUBJECT OF CRIMES IN THE COMPUTER SPHERE INFORMATION

Skobelina Galina Petrovna
senior lecturer of the Department of criminal law and criminology of the Law Institute
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article is devoted to crimes specified in Chapter 28 of the Criminal Code of the Russian Federation. The features of the object and subject of these crimes cause a lot of controversy and discussion in the science of criminal law, which leads to difficulties in qualifying crimes for the law enforcer. Although the volume of the article does not allow a deep and detailed study of the object and subject of crimes, provided for by Article Articles 272, 273 and 274 of the Criminal Code, I would like to outline in general terms these elements of a crime.

Keywords: *crimes in the field of computer information, object and subject of crime, violation of the rules for operating storage facilities, criminal consequences, determination of property damage.*

Важность исследования объекта преступления связана с тем, что его характер определяет общественную опасность деяния, систему Особенной части УК РФ, установление границ преступного, а также признаков состава преступления. Поскольку понятие «общественные отношения» являются абстрактными и неосязаемыми явлениями при квалификации это вызывает определенные трудности. Признание общественных отношений объектом преступления приводит к широкому применению норм уголовного права. Предмет преступления,

как часть объекта во многом определяется материальными признаками, т.е. обладает физическими единицами измерения [1].

В связи с бурным процессом научно-технической революции сформировался новый вид общественных отношений – информационные. Информационные отношения стали новым объектом, а информация – новым предметом преступного посягательства

Неизбежным следствием появления новых общественных отношений стали правонарушения в сфере компьютерной информации, в том числе и форме преступлений, которые представляют угрозу для нормального развития и течения общественной жизни.

Преступления в сфере компьютерной информации можно определить как умышленные общественно опасные деяния (действия и бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное хранение, использование или распространение информации и информационных ресурсов.

Уголовный Кодекс Российской Федерации установил нормы, устанавливающие уголовную ответственность за действия в сфере компьютерной информации. Такие нормы появились в российском законодательстве впервые. К ним отнесены 1) неправомерный доступ к компьютерной информации (ст.272 УК РФ), 2) создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ), и 3) нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст.274 УК РФ).

Когда речь идет о предмете, который представляет информацию, например, информацию об открытии, изобретении, а также сведения, составляющие коммерческую тайну, предложено рассматривать как предмет преступлений против собственности независимо от формы ее фиксации [2].

К рассматриваемой группе предметов относится также компьютерная информация (ст.272 УК), как неправомерный доступ к информации, повлекший за собой ее уничтожение, блокирование, модификацию либо копирование. Такие действия причиняют вред отношениям, обеспечивающим функционирование иных отношений. Представляется, что предметом преступления, предусмотренного ст. 272 УК РФ, является не любая охраняемая законом компьютерная информация, а только та, которая не содержит сведения о частной жизни (ст.ст.137,138,155 УК РФ), не является объектом авторского права (ст.ст.146, 147 УК РФ), имуществом в виде оплаты за доступ к логину и паролю (ст.165 УК РФ), коммерческой, банковской или налоговой (ст. 183 УК РФ) и государственной тайной (ст.275 УК РФ). Разглашение указанных сведений причиняет вред личным неимущественным отношениям, в сфере экономической деятельности, безопасности государства. И, во-вторых, получается, что если указанные сведения были выражены в компьютерной информации, то тогда действия виновного лица, скопировавшего ее с целью последующего разглашения или использования, надлежит квалифицировать по совокупности преступлений, предусмотренных ст. 272 УК РФ и соответствующими статьями. А если виновный завладел с этой же целью информацией, находящейся на материальном носителе, то только по соответствующей статье Особенной части УК РФ.

Предметом преступления, предусмотренного ст. 272 УК РФ, следует признавать не все программы, а программы-коды, позволяющие модифицировать ту или иную компьютерную информацию. Однако, в то же время, учитывая общественную опасность сбора сведений, являющихся предметом личных неимущественных отношений (ст.ст.137,138,155 УК РФ), имущественных отношений (ст.ст. 165,183 УК РФ), а также безопасности государства, существующих в форме компьютерной информации, представляется целесообразным дополнить указанные нормы таким квалифицирующим признаком, как совершение деяния с использованием компьютерной техники.

В настоящее время отмечается рост преступлений в сфере компьютерной информации и преступных деяний, совершенных в Российской Федерации с использованием информационных технологий, что причиняет значительный ущерб российской экономике и информационным общественным отношениям [3].

Законодателем в ч. 1 ст. 274 УК РФ установлена уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к таким сетям, повлекшим за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (свыше 1 мл. рублей).

Компьютерная информация может находиться в форме электронных денежных средств, т.е. являться имуществом и иметь конкретную стоимость. Для ч. 4 ст. 158 УК РФ установлено, что крупным размером признается стоимость имущества, превышающая двести пятьдесят тысяч рублей. Поэтому возникает вопрос, если предметом преступного посягательства, предусмотренного ст. ст. 146,158,159 и 274 УК РФ выступает компьютерная информация (компьютерные программы, базы данных и др.), находящаяся на различных носителях, то почему в первом случае сумма ущерба, причиненная правообладателю равна сто тысяч рублей , а для ст. 272 УК РФ эта сумма составляет один миллион рублей.

Такая правовая коллизия, относящаяся ко всем преступлениям в сфере компьютерной информации, ограничивает применение уголовно-правовых мер в борьбе с компьютерными преступлениями.

Так, Федеральным законом от 29 ноября 2012 г. №207-ФЗ уголовный закон был дополнен шестью новыми нормами о мошенничестве, одной из которых стала ст.159.9, предусматривающая уголовную ответственность за мошенничество в сфере компьютерной информации. Такое хищение чужого имущества совершается путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Особенности этого состава преступления заключаются в том, что диспозиция ст.159.6 УК РФ является бланкетной и отсылает нас к другим нормативным актам, например: Федеральному закону от 27.07.2006 г. №149-ФЗ « Об информации информационных технологиях и о защите информации». Данное преступление является

двухобъектным, так как посягает на отношение собственности и компьютерную информацию [4].

Таким образом следует сделать вывод, что видовым объектом преступлений в сфере компьютерной информации являются информационные отношения, т.е. отношения возникающие при формировании и использовании информационных ресурсов.

Следовательно, вышеуказанные обстоятельства выступают причиной для разработки системы противодействия преступлениям в сфере компьютерной информации. При этом степень уголовно-правовой защиты информации должна определяться ее содержанием, а не свойствами носителя [5].

Библиографический список

1. Зателепин, О.К. К вопросу о понятии объекта преступления в уголовном праве / О.К. Зателепин // Уголовное право. – 2006. – № 1. – С. 29.
2. Хилюта, В. Хищение интеллектуальной собственности / В. Хилюта // Уголовное право. – 2008. – № 2. – С. 54.
3. Быков, В.М. Преступления в сфере компьютерной информации: криминологические и уголовно-правовые проблемы: монография. / В.М. Быков, В.Н. Черкасов. – М.: Юрлитинформ, 2015. – С. 25–27.
4. Ермакова, О.В. Мошенничество в сфере компьютерной информации (ст.159-6 УК РФ): сложности толкования и квалификации / О.В. Ермакова // Уголовное право. – 2016. – № 3. – С. 36–39.
5. Айсанов, Р.М. Компьютерная информация как предмет преступления, предусмотренного ст.272 УК РФ / Р.М. Айсанов // «Черные дыры» в российском законодательстве. – 2007. – № 1. – С. 279–280.

УДК 378.147:004

ИНТЕГРАЦИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ В ВУЗЕ

Степанова Элина Вячеславовна
канд. эконом. наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В статье автор определяет возможность использования мобильного обучения, электронного и дистанционного обучения при использовании цифровых технологий. Представлены модели обучения и возможности интеграции цифровых технологий обучения. Определены ключевые критерии а интеграции m-learning, e-learning, массовых открытых курсов при смешанной модели обучения.

***Ключевые слова**: m-learning, e-learning, электронная образовательная среда, мобильное обучение, массовые открытые курсы.*

INTEGRATION OF DIGITAL LEARNING TECHNOLOGIES IN THE UNIVERSITY

Stepanova Elina Vyacheslavovna
candidate of economic science, aassociated professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The author in the article defines the possibility of using mobile education, electronic and distance education when using digital technologies. Training models and opportunities for integrating digital learning technologies are presented. Key criteria are defined for integration of m-learning, e-learning, mass open courses with mixed training model

***Keywords**: m-learning, e-learning, e-learning environment, mobile training, mass open courses.*

Технологии цифрового обучения активно используются в современных учебных заведениях. В рамках цифровизации образования государство возлагает большие надежды на высшее образование. Современное поколение студентов и преподавателей может обеспечить инновационный прорыв, который сделает Россию одной из ведущих стран научно-технического развития. Для этого в ближайшие годы российские вузы должны активно использовать цифровые технологии и менять методики обучения, подходы к организации учебного процесса с учетом перехода на цифру [1]. В результате Россия должна войти в десятку ведущих стран по применению современных технологий обучения в мировом рейтинге 500 лучших университетов мира. Каждый преподаватель и студент может внести свой вклад в процесс развития и модернизации российской высшей школы, стать активным участником этого процесса.

Современные вузы активно участвуют в процессе цифровизации образования и придерживаются порядка установления правил применения электронного обучения, дистанционных образовательных технологий организациями,

осуществляющими образовательную деятельность при реализации базовых образовательных программ и/или дополнительных образовательных программ [2].

Преподаватели системы высшего образования разрабатывают и реализуют цифровые технологии обучения Moodle, MOOC, m-learning в образовательный процесс [3]. Это позволяет оптимизировать и охватить большее количество обучающихся, расширить возможности доступа к информации активизировать студентов к участию в коммуникациях с помощью применения информационно-коммуникационных обучения. Со стороны студентов и многих преподавателей наибольший интерес вызывает мобильное обучение. Термин «мобильное обучение» (м-обучение) mobile learning (m-learning) относится к использованию мобильных и портативных ИТ - устройств, таких, как карманные компьютеры PDA (Personal Digital Assistants), мобильные телефоны, ноутбуки и планшетные ПК в преподавании и обучении [4]. Смартфон в образовательном процессе, по отношению к планшетным ПК, настольным компьютерам, позволяет быстро использовать удаленный доступ к интернету для повышения функциональности получения информации. Опыт двух лет применения мобильного обучения в вузе показывает, что студенты отказываются использовать настольные компьютеры в компьютерном классе в пользу смартфонов.

Успешной реализации курса дисциплины в Moodle способствует мобильное обучение [5]. Происходит интеграция e-Learning и m-learning, во многих случаях они используются взаимозаменяемо, несмотря на то, что эти два способа обучения различаются по многим аспектам. Чаще всего они представлены в смешанной учебной программе, где m-learning дополняет электронный курс дисциплины.

При разработке курса, с применением mLearning, следует учитывать, что он должен умещать контент в небольшом пространстве, и в одном экране обычно есть не более одной идеи. Разработка модулей дисциплины для m-learning является сложной задачей. Основное правило для создания успешных дисциплин для m-learning решающее значение имеет понимание контекста, и продолжительность. Для студентов, пользователей смартфонов необходимо использование меньше времени, поэтому для создания курса m-learning следует определить продолжительность модуля не более 20 минут. Рекомендуется, если каждый модуль будет меньше 15 минут, его можно считать идеальным для использования. Возможно использование видео для m-learning с продолжительностью не более 3 минут. Целесообразно создание простого контента, основанного на взаимодействии между одним и двумя пальцами, с областью, достаточно большой для одного пальца или большого пальца взрослого.

Дополнительным электронным ресурсом обучения студентов с применением дистанционных образовательных технологий является MOOC. MOOC может быть интегрирован в электронный курс дисциплины по следующим моделям:

Модель 1 «MOOC – поддержка дисциплины».

Модель 2 «Дисциплина + MOOC».

Модель 3 «MOOC + дисциплина».

Модель 4 «Исключительно MOOC».

Таблица 1 – Модель 1 «МООС – поддержка дисциплины»

Модель использования МООС	Преимущества модели	Недостатки/сложности модели	Риски в использовании данной модели
Модель 1 «МООС – поддержка дисциплины»	В рамках данной модели онлайн-курс используется в качестве дополнения к материалам очной дисциплины. Занятия по предмету проходят в традиционном формате, при этом преподаватель рекомендует студентам учебно-методические материалы МООС для подготовки к занятиям, выполнения домашних и курсовых работ, а также более углубленного изучения дисциплины	Для доступа к лекциям онлайн-курса студентам необходимо зарегистрироваться на платформе и записаться на МООС. Поэтому первое занятие можно провести в компьютерном классе, чтобы преподаватель проконтролировал наличие доступа к онлайн-курсу у всех студентов	При этом в вузе должны быть приняты положения, регулирующие политику университета в области онлайн-обучения. Это может быть зафиксировано в Образовательной политике вуза, в Положении об организации образовательного процесса с применением электронного обучения, дистанционных технологий или же иных нормативных документах, которые регулируют разработку и реализацию модулей образовательных программ

Ключевые критерии условия подбора «МООС – поддержка дисциплины»: в данном случае преподавателю необходимо предварительно оценить содержание МООС на платформе на его соответствие структуре очной дисциплины.

Таблица 2 – Модель 2 «Дисциплина + МООС»

Модель использования МООС	Преимущества модели	Недостатки/сложности модели	Риски в использовании данной модели
Модель 2 «Дисциплина + МООС»	В рамках данной модели только часть очного обучения переносится в онлайн-среду. Частным (и, пожалуй, самым распространенным) случаем применения модели является «перевернутый класс» (flipped classroom), когда студенты просматривают лекции на платформе, а семинарские занятия проводятся в университете очно	Сокращение часов контактной работы. Для доступа к лекциям онлайн-курса студентам необходимо зарегистрироваться на платформе и записаться на МООС. Поэтому первое занятие можно провести в компьютерном классе, чтобы преподаватель проконтролировал наличие доступа к онлайн-курсу у всех студентов	Объемы контактной работы преподавателя могут сократиться, так как он не ведет очные лекции по дисциплине

Ключевые критерии условия подбора «Дисциплина + МООС»:

– в данном случае преподавателю необходимо предварительно оценить содержание лекций на платформе на соответствие их структуре очной дисциплины;

– далее учебная программа должна быть согласована с руководителем образовательной программы и утверждена методическим советом вуза.

Таблица 3 – Модель 3 «МООС + дисциплина»

Модель использования МООС	Преимущества модели	Недостатки/ сложности модели	Риски в использовании данной модели
Модель 3 «МООС + дисциплина»	В рамках данной модели большая часть занятий по дисциплине переносится в онлайн-среду. При этом преподаватель проводит часть очных занятий, во время которых отвечает на вопросы студентов, разбирает сложные моменты, а также мотивирует студентов на прохождение курса	Незначительные часы контактной работы	Для реализации данной модели вузу необходимо заключить договор о сетевом взаимодействии двух образовательных организаций или договор о реализации образовательных услуг дополнительного образования с вузом-создателем МООС. При этом вуз-реципиент оплачивает стоимость сертификатов для студентов, которые осваивают онлайн-курс, как правило, она аналогична цене, указанной на платформе

Ключевые критерии условия подбора «МООС + дисциплина»:

– в данном случае учебная программа дисциплины должна быть трансформирована в соответствии с содержанием онлайн-курса;

– необходимо указать, что мероприятия по текущему и итоговому контролю проводятся онлайн.

Ключевые критерии условия подбора «Исключительно МООС» для реализации данной модели в вузе должны быть утверждены нормативные документы, которые регулируют организацию образовательного процесса с применением технологии электронного обучения:

1. Политика применения электронного обучения, дистанционных образовательных технологий в образовательном процессе.

2. Положение об организации образовательного процесса с применением электронного обучения, дистанционных образовательных технологий.

3. Документированная процедура «Разработка, экспертиза и использование в учебном процессе электронных образовательных программ».

4. Документированная процедура «Организация учебного процесса с использованием массовых открытых онлайн-курсов».

5. Типовые формы договора на создание произведений, являющихся электронными ресурсами, и соглашения об использовании.

Таблица 4 – Модель 4 «Исключительно МООС»

Модель использования МООС	Преимущества модели	Недостатки/ сложности модели	Риски в использовании данной модели
Модель 4 «Исключительно МООС»	В рамках данной модели обучение по дисциплине полностью переносится в онлайн- среду. Решение о включении онлайн-курса в учебную деятельность вуза принимается руководителем программы. В свою очередь, содержание обучения и ход учебного процесса будут определены структурой выбранного МООС	Отсутствие контактной работы	Для реализации данной модели вузу необходимо заключить договор о сетевом взаимодействии двух образовательных организаций или договор о реализации образовательных услуг дополнительного образования с вузом-создателем МООС. При этом вуз-реципиент оплачивает стоимость сертификатов для студентов, которые осваивают онлайн-курс, как правило, она аналогична цене, указанной на платформе

Реализацию представленных моделей целесообразно осуществлять последовательно. Наиболее результативной моделью является «МООС + дисциплина». Данная модель реализована на практике следующим образом:

– в рамках данной модели большая часть занятий по дисциплине переносится в онлайн-среду. При этом преподаватель проводит часть очных занятий, во время которых отвечает на вопросы студентов, разбирает сложные моменты, а также мотивирует студентов на прохождение курса;

– замена части лекций и практических занятий (несколько тем от 2 до 8);

– если МООС не освоен, экзамен в традиционной форме.

Мобильное обучение позволяет более эффективно реализовать технологию обучения тимбилдинг. При обучении в команде уделяется особое внимание «групповым целям» и успеху всей группы. Это может быть достигнуто только в результате самостоятельной работы каждого члена группы в постоянном взаимодействии с другими членами этой же группы при работе над темой/проблемой/вопросом. Студенты активно применяют мобильные средства коммуникации, так как задача каждого студента состоит не только в том, чтобы сделать что-то вместе, а в том, чтобы познать что-то вместе, чтобы каждый участник команды овладел необходимыми знаниями, сформировал нужные навыки и при этом, чтобы вся команда знала, чего достиг каждый учащийся. Вся группа заинтересована в усвоении учебной информации каждым ее членом, поскольку успех команды зависит от вклада каждого, а также в совместном решении поставленной перед группой проблемы [6].

Возможности мобильного обучения в вузе практически неограниченные. Мобильные устройства обеспечивают постоянно включенный доступ к соединению со студентами. С помощью этого подключения можно мгновенно отправлять быстрые сообщения и уведомления о новых дополнениях к мобильным учебным материалам и сегментам. Интеграция цифровых технологий обучения способствует эффективному обучению с применением кейс-стади [7]. По этой ссылке студентам могут быть направлены напоминания, например, о незаконченных модулях. Мобильные устройства также позволяют студенту легко отвечать на краткие опросы о содержании конкретного курса, а также предоставляют ему возможность вносить предложения или сообщать о любых проблемах с производительностью платформы урока [8].

Мобильные устройства используют сенсорный экран. Это означает, что способ взаимодействия пользователей очень отличается: вместо того, чтобы использовать мышь для щелчка, прокрутки или наведения мыши, пользователи нажимают на свой экран, чтобы взаимодействовать с различными элементами на экране. Поэтому при проектировании мобильного урока целесообразно разрабатывать его с использованием простых стилей меню, увеличивая пространственный размер кнопок и расширяя элементы интерфейса, такие как кнопки. Поэтому структуры mLearning должны умещать контент в небольшом пространстве, и в одном экране обычно есть не более одной идеи [8].

Несмотря на то, что eLearning развивается благодаря использованию мобильных устройств и, таким образом, создает новые проблемы для преподавателя, выступающего в роли дизайнера курса. Преподаватель вуза должен быть мобильным и быстро настраивать свою курс, используя цифровые технологии обучения и уметь адаптировать контент с учетом быстрых изменений.

Необходимость эффективного распространения образования обусловливает необходимость того, чтобы классные комнаты больше не помещались в четырех стенах. Современные студенты больше не привязаны к своим столам, обучение доставляется на их мобильные устройства, где они могут потреблять его в пути, без границ во времени в режиме 7/24.

Библиографический список

1. Belyakova G., Stepanova E. and Zabuga E. High Knowledge Level for an Innovation Cluster Environment Formation in the Russian Federation, 20th European Conference on Knowledge Management (ECKM 2019) Edited by Dr. Eduardo Tomé, Dr. Francisco Cesário Dr. Raquel Reis Soares Hosted By Universidade Europeia de Lisboa Lisbon, Portugal, 2019,VOLUME 1 pp.111-122

2. Zinina O.V., Antamoshkina O.I., and Olentsova, J. A. (2020) Methodology for Evaluating the Effectiveness of Investments in Distance Educational Services, 35th International Business Information Management Association (IBIMA), Madrid, Spain.

3. Степанова, Э.В. Возможности мобильного обучения в вузе / Э.В. Степанова // Ресурсосберегающие технологии сельского хозяйства: сб. науч. ст. Вып. 11. – Краснояр. гос. аграр. ун-т. – Красноярск, 2019. – 144 с.

4. Голицына, И.Н. Мобильное обучение как новая технология в образовании / И.Н. Голицына, Н.Л. Половникова //Образовательные технологии и общество, vol. 14, no. 1, 2011, pp. 241-252.

5. Kapsargina, S.A. and Olentsova, J.A. (2019) «Experience of using LMS MOODLE in the organization of independent work of bachelors in teaching a foreign language", «Far East Con» International Scientific Conference, Far East Federal University, Vladivostok

6. Stepanova, E.V., Rozhkova, A.V. and Dalisova, N.A. (2019) «Team building technology for the development of modern organizations», Science and education: experience, problems, development prospects materials of an international scientific and practical conference. Krasnoyarsk State Agrarian University. Pp. 297-301.

7. Rozhkova A.I., and Olentsova, J. A. (2020) Case-Study Method as an Educational Technology for Teaching Management Students, 35th International Business Information Management Association (IBIMA), Madrid, Spain

8. Макарчук, Т.А. Мобильное обучение на базе облачных сервисов / Т.А. Макарчук, В.Ф. Минаков, А.В. Артемьев // Современные проблемы науки и образования. – 2013. – № 2.

УДК 342.7

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ ОТ УГРОЗ В СОЦИАЛЬНЫХ СЕТЯХ

Тимофеев Константин Сергеевич
аспирант
Московский городской педагогический университет, Москва, Россия

В данной статье рассматривается вопрос использования несовершеннолетними социальных сетей в международной телекоммуникационной сети Интернет, как основного средства коммуникации. Обобщаются угрозы, исходящие из социальных сетей, влияющие и во многом детерминирующие поведение несовершеннолетнего. Проводится анализ становления государственного правового регулирования защиты несовершеннолетних от угроз в сети Интернет и в частности в социальных сетях, безопасного использования последних.
Ключевые слова: *кибербуллинг, интернет-травля, несовершеннолетний.*

LEGAL FRAMEWORK FOR THE PROTECTION OF MINORS FROM THREATS ON SOCIAL NETWORKS

Timofeev Konstantin Sergeevich
postgraduate student
Moscow City Pedagogical University, Moscow, Russia

The article discusses the issue of the use of social networks by minors in the international telecommunications network as the main means of communication. The paper systemizes the threats emerging from social networks that influence and largely determine the behavior of the minor. It contains the analysis of the formation of the state legal regulation of the minors' protection from threats in the Internet and, in particular, in social networks, with the safe use of the latter.
Keywords: *cyberbullying, cyberharassment.*

Ни для кого не секрет, что Интернет таит в себе много угроз. Исследование интернет-угроз Лаборатории Касперского показало, что Россия является одной из лидеров антирейтенга по доле опасного контента в сети. Большую часть угроз составляют: сайты «для взрослых», онлайн казино и другие сайты азартных игр, сайты с информацией об оружии [1].

В соответствии с ч. 1 ст. 63, ч.1 ст. 64 Семейного кодекса РФ, родители несут ответственность за воспитание и развитие своих детей, осуществляю защиту их прав. Однако воспитание и защита детей в сети интернет осложняется в связи с двукратным разрывом интернет-активностью детей и родителей. Зачастую использование сети интернет несовершеннолетними происходит бесконтрольно, что подтверждается открытой публикаций конфиденциальной информации: фамилия и имя, день рождения, город проживания, информации об образовательной организации, в которой проходят обучение, телефонов, фотографий и видео, информации об интересах. Учитывая изложенное, дети подвер-

гаются реальному риску стать жертвой интернет преступности, попасть под опасное или негативное влияние.

Основу правового регулирования защиты детей в сети Интернет составил Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» с учетом поправок в части 1, части 5 статьи 15_1, определил перечень информации, распространение которой в Российской Федерации запрещено, и ввела Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты, содержащие запрещенную информацию, в целях ограничения доступа к ним. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в статье 5 раскрыл виды информации, причиняющей вред здоровью и (или) развитию детей.

Согласно п.1 ст. 2 Федерального закона от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» основными задачами деятельности по профилактике безнадзорности и правонарушений несовершеннолетних являются: предупреждение безнадзорности, беспризорности, правонарушений и антиобщественных действий несовершеннолетних, обеспечение защиты прав и законных интересов несовершеннолетних; выявление и устранение причин и условий, способствующих этому; выявление и пресечение случаев вовлечения несовершеннолетних в совершение преступлений, других противоправных и (или) антиобщественных действий, а также случаев склонения их к суицидальным действиям.

В целях координации деятельности органов и учреждений системы профилактики безнадзорности и правонарушений несовершеннолетних созданы Комиссии по делам несовершеннолетних и защите их прав.

Для реализации основных задач Комиссии по делам несовершеннолетних и защите их прав района Савелки города Москвы (далее по тексту - КДНиЗП) по профилактике и предупреждению негативных тенденций среди несовершеннолетних в наиболее популярной социальной сети «Вконтакте», в 2016 выпущено Распоряжение управы «Об организации деятельности КДНиЗП района Савелки в социальных сетях». Подведя первые итоги работы в этом направлении и поделившись опытом на окружной коллегии Префектуры ЗелАО, выпущено распоряжение Префектуры. Данным актом закреплено поручение специалистам КДНиЗП районов проводить постоянный мониторинг социальных сетей, выявленные противоправные факты направлять по подведомственности.

Следует отметить, что на территории России, и даже города Москвы, случаи осуществления повсеместного мониторинга сети Интернет комиссиями не находит широкого применения. Проблематике недостаточно уделяется внимания. Как показывает практика, подросток, совершивший преступление, административное правонарушение, либо антиобщественное действие и впервые попавший на учет в Комиссию по делам несовершеннолетних и защите их прав ранее уже выставлял на своей страничке в социальной сети информацию о совершении им каких-либо противоправных действий. При помощи мониторинга социальных сетей можно успешно сработать на профилактику правонарушений, выявляя негативные тенденции в поведении несовершеннолетних.

На основе данных КДНиЗП можно выделить следующие негативные проявления при использовании подростками социальных сетей:

1. Желание похвастаться противоправной деятельностью, нарушением закона (курения сигарет, употребление алкоголя, совершение административных правонарушений, совершение преступлений). При мониторинге страниц в социальных сетях, выявляются группы (сообщества), на которые подписаны дети. Как правило современные подростки склонны к открытой демонстрации нарушения общественного порядка, норм и правил поведения, реализуемого посредством фотографий и видео. С целью затруднения идентификации личности многие подростки сохраняют свои имена, но при этом меняют фамилии.

После выявления подобных фотографий и видео происходит поиск несовершеннолетнего выложившего фотографию путём изучения подписчиков данного сообщества, а также на и подписчиков людей оставившего комментарии и к записи под заинтересовавшим его фото.

Имеют место случаи, когда подростки выкладывающие фотографии с нарушением общественного порядка, имеют свои интернет каналы на других сайтах, где можно обнаружить не только фотоотчеты с их «приключениями», а также видеоматериалы, где они подробно описывают свои «подвиги».

2. Ещё одной угрозой, с которой сталкиваются несовершеннолетние является «Кибербуллинг», иначе говоря: «интернет-травля — намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени» [2].

Жертвами данного негативного явления стали около ¼ подростков России, статистика говорит о том, что в 58% случаев решить проблему удалось лишь при вмешательстве родителей [3].

В практике комиссии были случаи, когда из агрессии и провоцировании конфликтов в сети, дело перерастало в реальное причинение вреда жизни и здоровью.

1. Вовлечение несовершеннолетних в противоправную деятельность.

Специалистами комиссии была выявлена группа, занимающаяся распространением материала, содержащего порнографический характер. Условием данного сообщества являлась конфиденциальность, то есть девушки, чьи фотографии были размещены в сообществе не должны были знать, о том, что их фотографии может просмотреть любой пользователь сети интернет, фотографии модератору сообщества присылали участники сообщества в основном из личных переписок. Охват каждого «поста» составлял более 5000 просмотревших. В дальнейшем в группе персональные данные несовершеннолетних девушек на фото продавались за заранее определенную плату. Деятельность данного сообщества была пресечена полицией, по сообщению комиссии.

2. К сожаленью в настоящее время существует мода на жестокость, что подтверждает участие несовершеннолетних в неформальных группировках антиобщественной направленности. («А.У.Е.», «фашисты», «около футбола», «поясни за шмот»). Идеология повсеместно распространяется в сети.

3. Оскорбление чести и достоинства личности, деловой репутации. Разглашение конфиденциальной информации.

Так же частым является демонстрация личной переписки, в которой может содержаться компрометирующая информация. Переписка является предметом обсуждения школы. Вместо учебы, в одной из групп, идет активное обсуждения взаимоотношений несовершеннолетних, где делаются ставки на различные аспекты их личной жизни.

4. Призывы и пропаганда действий суицидального характера.

5. При мониторинге социальных сетей, мы часто сталкиваемся с тем, что юные пользователи выкладывают фотографии абсолютно не задумываясь о том, что они находятся в общественном доступе. Достаточно часто, к фотографиям имеются сведения о местоположении. Данная информация, может нести вред самому несовершеннолетнему, но вместе с тем, она может стать хорошим подспорьем для тех, кто не может найти своего ребенка. Так, благодаря определенной геолокации удалось установить приблизительное местонахождение ребенка, находившегося в розыске.

Вместе с социальными страницами детей, в поле зрения так же попадаются и страницы родителей, и с сожалением хочется заметить, что дети, как правило стараются копировать своих родителей, но если старшему поколению не присуща культура поведения в сети интернет, чего нам стоит требовать от подрастающего поколения?

Делая выводы, стоит отметить необходимость уделять больше внимания мерам, направленным на обеспечение информационной безопасности детства:

– обучение детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию;

– блокирование информационных каналов проникновения через источники массовой информации в детско-подростковую среду элементов криминальной психологии, культа насилия, других откровенных антиобщественных тенденций и соответствующей им атрибутики.

– создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги «Родительский контроль», позволяющей устанавливать ограничения доступа к сети Интернет.

Библиографический список

1. Отчет Лаборатории Касперского: «Чем интересуются дети в Сети». URL: https://securelist.ru/what-are-children-doing-online/30779.

2. Лахмытко, Н. М. Интернет-травля. Миф или реальность? / Н. М. Лахмытко // Методист. – 2015. – № 6. – С. 21–24.

3. Исследование независимого агентства B2B International: «Угроза детям, о которой не знают взрослые: 52 % родителей не воспринимают кибербуллинг всерьез». – URL: https://www.kaspersky.ru/about/press-releases/2015_ugroza-detjam-o-kotoroj-ne-znajut-vzroslye.

4. Recommendation on the OECD Council Report on risks faced on children online and policies to protect them, C. 17. – URL: https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf.

УДК 343.13:347:8

ОСОБЕННОСТИ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВО СУДЕБНЫХ ЭКСПЕРТИЗ В РАМКАХ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ О НАРУШЕНИИ ПРАВИЛ ДВИЖЕНИЯ И ЭКСПЛУАТАЦИИ ВОЗДУШНОГО ТРАНСПОРТА ГРАЖДАНСКОЙ АВИАЦИИ

Трифонова Ксения Сергеевна
Средне-Волжский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийский государственный университет юстиции» в г. Саранске
Саранск, Россия

Использование специальных знаний в рамках предварительного расследования уголовных дел о нарушении правил безопасности движения и эксплуатации воздушного транспорта является одним из главных направлений в процессе доказывания по уголовным делам данной категории. Назначение и производство экспертиз направлено на установление обстоятельств, произошедшего авиационного происшествия, что позволяет в полном объеме исследовать все обстоятельства произошедшего.

***Ключевые слова**: экспертиза; нарушение правил безопасности движения и эксплуатации воздушного транспорта; криминалистика.*

FEATURES OF APPOINTMENT AND PRODUCTION OF FORENSIC EXAMINATIONS IN THE INVESTIGATION OF CRIMINAL CASES ABOUT VIOLATION OF TRAFFIC RULES AND OPERATION OF AIR TRANSPORT CIVIL AVIATION

Trifonova Ksenia Sergeevna
master's student
The Russian Law Academy of the Ministry of Justice of the Russian, Saransk, Russia

The use of specialized knowledge in the preliminary investigation of criminal cases involving violations of traffic safety rules and the operation of air transport is one of the main directions in the process of proof in criminal cases of this category. The appointment and production of examinations is aimed at establishing the circumstances of the aviation incident, which allows to fully investigate all the circumstances of the incident.

***Keywords:** expertise; violation of the rules of safety of traffic and operation of air transport; criminology.*

Одним из ведущих направлений доказывания, в процессе расследования уголовных дел о нарушении правил безопасности движения и эксплуатации

воздушного транспорта гражданской авиации, является применение специальных знаний, а именно назначение и проведение экспертиз.

Судебно-экспертная деятельность – это «организацинно-методическая деятельность государственных и негосударственных судебно-экспертных учреждений; производственная деятельность государственных судебных экспертов, а также иных экспертов из числа сведущих лиц, которые в соответствии с действующим процессуальным законодательством осуществляют судебно-экспертное исследование объектов экспертизы» [1].

Анализ следственной практики показывает, что в данном случае назначаются и проводятся следующие экспертизы: авиационно–техническая, судебно-медицинская и криминалистическая экспертизы.

На сегодняшний день особую трудность вызывает проведение экспертизы, направленной на определение качества обслуживания воздушного судна, управления данным транспортным средством, определение обстоятельств, связанных с пилотированием.

В силу того, что следователь не располагает специальными техническими знаниями в области авиации, а, следовательно, не имеет возможности самостоятельно установить причины авиационного происшествия, выявить конкретные нарушения правил безопасности движения и эксплуатации, определить субъект вышеуказанных нарушения данных правил. Так как, следствию самостоятельно не представляется возможным установить причинно-следственную связь между нарушениями и наступившими общественно опасными последствиями, появляется необходимость в проведении судебно-технической экспертизы, что представляет собой важное следственное действие.

Рассмотрим экспертизы, которые чаще всего назначаются при расследовании авиационных происшествий.

Так, одной из первых назначается авиационно-техническая (летная, летно-техническая) экспертиза. При проведении данной экспертизы перед экспертом ставятся следующие вопросы: установить причины авиационного происшествия; определить что послужило причиной выхода из строя отдельных частей самолета или иных средств управления (наемного управления и оборудования аэропорта); установить механизм происхождения следов на отдельных частях судна; определить координату начала разрушения судна; выявить качество соблюдения правил безопасности и движения воздушного судна сотрудниками воздушного транспорта и т. д.

Авиационно-техническая экспертиза по своей природе имеет комплексный характер. Так, в состав экспертов кроме специалистов по эксплуатации авиационной техники, радиотехнических и других средств аэродромного обеспечения полетов, также в области самолетовождения, могут быть включены специалисты по пожарному и взрывному делу, химики, металловеды и другие. С целью установления других обстоятельств назначаются также технические экспертизы узкого профиля, например, пожаротехническая, метеорологическая, летно-техническая, взрывотехническая, экспертизы по расшифровке фонограмм, данных автоматических и электронных устройств.

В рамках производства авиационно-технической экспертизы перед экспертами могут быть поставлены следующие виды вопросов: о техническом состоянии воздушного судна; об оценки действий работников управления воздушным судном; связанные с состоянием наземного авиационного оборудования; направленные на выяснения метеорологических условий полета [2].

Производство комплексных экспертиз в данном случае обусловлено тем, что чаще всего отказ авиационной техники, в результате нарушения правил безопасности, при ее обслуживании дополняются нарушениями правил безопасности полетов со стороны членов экипажа или работников службы управления воздушным движением. В практике известны случаи, когда причинами авиакатастрофы одновременно являются нарушения правил безопасности работниками диспетчерской службы и работниками аэродромной или метеорологической службы и др.

С целью установления причин смерти погибших, характера и тяжести прижизненных и посмертных повреждений, а также определения принадлежности отдельных фрагментов тел тем или иным трупам проводится судебно-медицинская экспертиза [3]. В рамках проведения данной экспертизы необходимо установить следующие обстоятельства: принадлежность останков частям тела человека; состояние здоровья работников воздушного транспорта перед полетом; механизм образования повреждений на трупах (останках) членов экипажа; поза пилота и иных членов экипажа в момент начала разрушения судна; состояние алкогольного и наркотического опьянения погибших и т.д.

В процессе проведения судебно-медицинской экспертизы осуществляется забор фрагментов тканей останков тел для проведения молекулярно-генетического исследования, а также для архивирования с целью последующего судебно-химического исследования (после идентификации фрагментов, принадлежащих членам экипажа) [4].

Молекулярно-генетическая экспертиза назначается по образцам, полученным в процессе судебно-медицинской экспертизы фрагментов тел погибших [5]. Так в рамках проведения данной экспертизы исследуются биологические образцы родственников погибших с целью проведения сравнительного исследования.

Практика расследования уголовных дел о нарушение правил безопасности движения и эксплуатации воздушного транспорта показывает, что если провести опознание тел погибших не представляется возможным из-за отсутствия признаков, позволяющих идентифицировать погибшего, то в таком случае назначается судебно-генетическая экспертиза.

По окончанию проведения молекулярно-генетической экспертизы, результаты исследования направляются следователю и судебно-медицинским экспертам для завершения судебно-медицинской экспертизы. На основании молекулярно-генетической экспертизы судебно-медицинские эксперты определяют принадлежность каждого фрагмента конкретному погибшему и заканчивают проведение судебно – медицинской экспертизы.

При необходимости в рамках проведения судебно-медицинской экспертизы дополнительно ставятся вопросы о наличии следов пожара, взрыва, резанных и огнестрельных ранениях, а также вопросы о кислородном голодании и отравлении угарным газом.

В процессе расследования уголовного дела об авиационной катастрофе проводятся криминалистические экспертизы, а именно трасологическая, пожарно-техническая, взрывотехническая, баллистическая, товароведческая, почерковедческая, технико-криминалистическая, фоноскопическая, биолого-орнитологическая и т.д.

Таким образом, проведение судебных экспертиз при расследовании преступлений о нарушение правил безопасности движения и эксплуатации воздушного транспорта является обязательным процессуальным действием. Так качественное и своевременное назначение и проведение судебных экспертиз оказывает положительное влияние на определение причин происшествий и установление виновных лиц, поскольку результаты экспертиз имеют существенное доказательственное значение.

Библиографический список

1. Россинская, Е.Р., Настольная книга судьи: судебная экспертиза / Е.Р. Россинская, Е.И. Галяшина. – М.: Проспект, 2014. – С. 36.

2. Расследование и предупреждение дорожно-транспортных происшествий, крушений железнодорожного транспорта и авиационныхкатастроф: научно-практ.пособие / Е. П. Ищенко [и др.]. – М.: Юрлитинформ, 2014. – С. 120.

3. Солодун Ю.В., Проблемы комплексной идентификации останков человека при расследовании авиационных катастроф. / Ю.В. Солодун, Д. Ю. Яковлев. – Иркутск: ИПКПР ГПРФ, 2004. – С. 85–86.

4. Митрофанова, А.А. Судебно-медицинская экспертиза по уголовным делам об авиационных происшествиях: некоторые актуальные вопросы / А.А. Митрофанова // Эксперт-криминалист. – 2016. – №3. – С. 15–17.

5. Иванов, П.Л. Практическое использование молекулярно-генетических технологий для решения задач судебно-экспертной идентификации неопознанных останков при чрезвычайных ситуациях с массовыми человеческими жертвами / П.Л. Иванов, Е.В. Щербакова, Ю.И. Пиголкин // Судебно-медицинская экспертиза. – 2004. – Т. 47. –№ 5. – С. 31–40.

УДК 343.13:347:8

МЕЖВЕДОМСТВЕННОЕ ВЗАИМОДЕЙСТВИЕ В РАМКАХ РАССЛЕДОВАНИЯ АВИАЦИОННЫХ КАТАСТРОФ С ВОЗДУШНЫМИ СУДНАМИ ГРАЖДАНСКОЙ АВИАЦИИ

Трифонова Ксения Сергеевна
Средне-Волжский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийский государственный университет юстиции» в г. Саранске, Саранск, Россия

В статье рассматривается вопрос межведомственного взаимодействия при осмотре места авиакатастрофы. Подчеркивается необходимость проведения широкого комплекса следственных действия, а также привлечения специалистов из различных государственных служб. Указываются проблемы, возникающие на первоначальном этапе расследования авиакатастроф, а также пути их решения.

Ключевые слова: *межведомственное взаимодействие, авиационная катастрофа, осмотр места происшествия*

INTERAGENCY COOPERATION IN THE INVESTIGATION OF AVIATION ACCIDENTS WITH CIVIL AVIATION AIRCRAFT

Trifonova Ksenia Sergeevna
The Russian Law Academy of the Ministry of Justice of the Russian, Saransk, Russia

The article deals with the interdepartmental cooperation during the inspection of the air crashes. It emphasizes the need for a wide range of investigative action, as well as the involvement specialists from different public authority. Indicates the problems during the initial phase of the investigation of air crashes and of addressing them.

Keywords: *interdepartmental cooperation, air crashes, scene inspection*

Одно из главных мест в транспортной системе перевозок пассажиров занимает воздушный транспорт.

За сутки самолеты перевозят в среднем более трёхсот тысяч человек, за год – более ста миллионов пассажиров. В среднем ежегодно в мире происходит шестьдесят авиакатастроф, причем в тридцати пяти случаях из которых гибнут все пассажиры и члены экипажа воздушного судна. Для сравнения: ежегодно на дорогах мира гибнет около трёхсот тысяч человек, в то время как в авиакатастрофах – менее двух тысяч человек.

В гражданской авиации случаи полного или частичного разрушения воздушного судна, имеющего на борту пассажиров, называются авиационными происшествиями. Авиационные происшествия в свою очередь подразделяются на катастрофы, аварии и инциденты.

Под авиационной катастрофой понимается авиационное происшествие, повлекшее за собой гибель хотя бы одного члена экипажа или пассажира, полное или частичное разрушение воздушного судна или его бесследное исчезновение. К авиационным катастрофам относятся также случаи гибели кого-либо из лиц, находившихся на борту, в процессе их аварийной эвакуации из воздушного судна.

Согласно данным Межгосударственного авиационного комитета (МАК), на территории государств-участников Межгосударственного соглашения о гражданской авиации и об использовании воздушного пространства в период с 2010 г. по 2018 г. с воздушными суднами гражданской авиации произошло 220 авиакатастроф, в которых погибло 931 человек.

Авиационные катастрофы с воздушными судами гражданской авиации отличаются своей масштабностью, труднодоступностью места происшествия, тяжестью последствий, а также опасностью не только для лиц, находившихся в воздушном судне, но и для лиц, находящихся в момент происшествия в районе места происшествия. Более того для авиационных катастроф характерным является наличие множества причин происшествия, как главных, так и вторичных.

Большое внимание при расследовании данной категорий преступлений уделяется техническим и специальным вопросам эксплуатации воздушного судна. Так на первоначальном этапе расследования преступлений, связанных с нарушением правил безопасности движения и эксплуатации воздушного транспорта (гражданской авиации), актуальным является вопрос межведомственного взаимодействия в рамках расследования данной категории преступлений.

Основными задачами первоначального этапа расследования авиационных катастроф с воздушными суднами гражданской авиации являются: 1) обеспечение спасательных работ; 2) ликвидация последствий происшествия (ликвидация розлива топлива, пожара и т. д.); 3) обнаружение, фиксация и изъятие следов на месте происшествия; 4) получение показаний свидетелей и очевидцев; 5) охрана места происшествия. Вышеуказанные задачи распределяются между всеми субъектами, уполномоченными участвовать в первоначальном этапе расследования катастроф с воздушными суднами гражданской авиации. На месте происшествия авиационной катастрофы работают: Федеральное агентство воздушного транспорта, Министерство внутренних дел Российской Федерации, Следственный комитет Российской Федерации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Межгосударственный авиационный комитет, а также местные органы исполнительной власти.

С целью обеспечения эффективной работы на месте происшествия необходимо четкое распределение обязанностей между всеми органами власти и

иными организациями, осуществляющими выезд на место происшествия, а также их полное взаимодействие.

Так на практике существует ряд проблем, затрудняющих быструю и эффективную работу в рамках первоначального этапа расследования авиационных катастроф.

Во-первых, в соответствии с законодательством, следователь обязан осуществлять предварительное следствие, с целью установления причин авиационного происшествия, а также установления виновных. Однако правительственные и ведомственные комиссии, так же нацелены на установление причин происшествия, что в результате оттесняет следователя на второй план.

Во-вторых, одновременно ведутся спасательные и ремонтно-восстановительные работы, в которых участвуют силы и средства МЧС, ФСБ, МВД, Минобороны России и медицинские спасательные службы, что значительно затрудняет поиск, фиксацию и изъятие следов возможного преступления.

В-третьих, ликвидация последствий авиационной катастрофы осуществляется поспешно, без учета задач, поставленных перед следствием.

В-четвертых, возникает вопрос относительно подследственности, которую невозможно определить сразу, ввиду отсутствия всех элементов расследуемого события в совокупности.

В виду наличия схожих целей и внешне аналогичных действий в рамках первоначального этапа расследования авиационных катастроф, в наиболее тесном взаимодействии находятся органы следствия и МАКа.

Порядок совместной работы МАКа и следственных органов урегулирован ПРАПИ-98, однако на практике встречается ряд проблем в рамках взаимодействия данных органов, которые обусловлены отсутствием норм, направленных на установление порядка совместной работы.

Так на практике возникают следующие проблемы в рамках взаимодействия МАКа и следственных органов: 1) не определен круг полномочий следственного органа до прибытия МАКа на место происшествия; 2) не установлен четкий порядок действий следователя при обнаружении бортовых самописцев; 3) нормативно не урегулирован порядок передачи изъятых следователем на месте происшествия следов членам МАКа и т.д.

Одной из важнейших проблем является следующее противоречие: поскольку предварительное следствие в своей работе опирается на выводы, содержащиеся в отчете МАКа, в ряде случаев работа предварительного следствия не может осуществляться своевременно и полноценно, так как, не смотря на то, что согласно п. 2.1.1. ПРАПИ-98, «срок расследования авиационных катастроф членами МАКа не должен превышать 30 суток, при необходимости срок расследования может быть продлён по ходатайству председателя комиссии», предварительное следствие в свою очередь ограничено в сроках проведения расследования, так согласно ч. 5 ст. 162 Уголовно-процесуального кодекса Российской Федерации «по уголовному делу, расследование которого представляет особую сложность, срок предварительного следствия может быть продлен руководителем следственного органа по субъекту Российской Федерации и иным

приравненным к нему руководителем следственного органа, а также их заместителями до 12 месяцев».

Следующей, немало важной проблемой, является противоречие принципам уголовного права Российской Федерации положению, закрепленного в Соглашении между Правительством Российской Федерации и Межгосударственным авиационным комитетом об условиях его пребывания на территории Российской Федерации. Так в соответствии с вышеуказанным Соглашением должностные лица МАКа не подлежат судебной ответственности за действия, совершенные ими при исполнении служебных обязанностей, что позволяет членам МАКа делать любые выводы о причинах возникновения авиационной катастрофы, более того заведомо ложные.

С целью всестороннего, полного и быстрого расследования авиационных катастроф, деятельность органов следствия и МАК должна строится на принципах полного взаимодействия, делового сотрудничества и своевременного обмена информацией.

Таким образом, возникает необходимость в нормативном урегулировании порядка взаимодействия следственных органов и МАКа, который закрепил бы в себе решение следующих проблемных вопросов: 1) установление задач и принципов работы органов следствия и МАКа; 2) определение конкретного перечня действий органов предварительного следствия, которые должны обязательно согласовываться с членами МАКа; 3) установление предельного срока расследования авиационных катастроф МАК, не превышающего предельных срок предварительного следствия; 4) установление определенного порядка передачи следов, изъятых следствием на месте происшествия должностным лицам МАКа; 5) определение четкого порядка распределения полномочии между МАК и следствием в процессе осуществления таких действий, как опросы, осмотры, изъятие и т.д.

Библиографический список

1. Китаева, В. Н. Актуальные проблемы осмотра места происшествия при расследовании авиакатастроф / В.Н. Китаева, А.А. Митрофанова // Известия Иркутской государственной экономической академии. – 2011. – № 4. – С. 163-166.

2. Вазюлин, С.А. Организация межведомственного взаимодействия при проведении осмотра места происшествия и неотложных следственных действий при авиакатастрофах / С.А. Вазюлин // Расследование преступлений: проблемы и пути их решения. – 2016. – № 2 (12). – С. 116–121.

3. Кравец, И. П. Правовое обеспечение взаимодействия следователя со служебной комиссией при расследовании авиационных происшествий / И. П. Кравец // Пробелы в российском законодательстве. –2016. – № 1. – С. 73–76.

4. Митрофанова, А. А. Тактические особенности осмотра места авиационного происшествия / А.А. Митрофанова // Сибирские уголовно-процессуальные и криминалистические чтения. – 2016. – Вып. 1 (9). – С. 95–105.

УДК 338.43

К ВОПРОСУ О ПРИМЕНЕНИИ ЦИФРОВЫХ ТЕХНОЛОГИИ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Фастович Галина Геннадьевна
старший преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

В статье рассмотрены вопросы повышения инновационного преобразования агропромышленного комплекса Российской Федерации. Представленное консолидированное исследование модели развития агропромышленного комплекса современной России – как технологической платформы и инновационного кластера совершенствования экономики государства, отражены вопросы внедрения цифровых технологий в АПК.

Ключевые слова: *агропромышленный комплекс, цифровые технологии, инновации, технологическая платформа, инновационный кластер, эффективность.*

TO THE QUESTION OF THE APPLICATION OF DIGITAL TECHNOLOGIES IN THE AGRICULTURAL COMPLEX OF THE RUSSIAN FEDERATION

Fastovich Galina Gennadevna
Senior Lecturer
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The article considers the issues of increasing the innovative transformation of the agricultural sector of the Russian Federation. The presented consolidated study of the development model of the agro-industrial complex of modern Russia - as a technological platform and an innovative cluster for improving the state economy, reflects the introduction of digital technologies in the agricultural sector.

Keywords*: agribusiness, digital technology, innovation, technology platform, innovation cluster, efficiency.*

В настоящее время российское агропромышленное производство является частью общемировой хозяйственной модели. Актуальность проведения исследования также обусловлена тем, что в XXI в. назрела потребность в обновленной теории, таких институтов, как «агропромышленный комплекс», «эффективность» [1], «отрасли народного хозяйства», но в тоже время происходит становление новых институтов, которые красной линией пронизывают все сферы государственного сектора, а именно: «инновационная модель развития», «технологическая платформа», «государственно-частное партнерство» и т. д. Учитывая, в целом, неоценимый вклад ученых-теоретиков и практиков в исследование вопроса эффективности агропромышленного комплекса Российской Фе-

дерации, стоит отметить на правовые коллизии в изучении инновационной модели развития АПК.

В формате всеобщей глобализации оно является частью жизненно необходимых интересов транснациональных компаний, которые непосредственно связаны с производством, переработкой и реализацией сельскохозяйственной продукции. Появились проблемные вопросы со стратегическим направлением развития сельскохозяйственного комплекса, экономической независимостью и продовольственной безопасностью. Требовалось и требуется решение вопросов на тему внешней и внутренней конкуренции, сбалансированности интересов участников рынка продовольствия [2]. Анализ факторов, способствующих снижению уровня эффективности АПК современной России, его участия в решении проблем государственного сектора, показывает, что они носят как объективный, так и субъективный характер. К объективным факторам можно отнести переход общества от ранее сложившейся системы социально-экономических и политических правил и установок к качественно новой модели общественных отношений, недостаточное государственное финансирование программ развития агропромышленного комплекса до 2015 года (стоит отметить, что за период 2015-2020 гг. вопросы финансирования государственных/национальных программ по развитию сельского хозяйства были увеличены в несколько раз, по сравнению с предыдущими периодами) [3]. Субъективные факторы включают в себя недостаточно оперативную и несистемную консолидацию государственных структур, научного сообщества и российской общественности. Одной из ключевых проблем современного периода, можно обозначить в непоследовательной международно-правовой политики мирового сообщества (политика санкций, экономического бойкота в отношении Российской Федерации). Функционирование экономики РФ в условиях санкций, нужно рассматривать как механизм развития отечественного сельского хозяйства и развития инновационных технологий для повышения производительности труда, а также как фактор обеспечения юридическую защиту и конкурентоспособность сельскохозяйственных товаропроизводителей.

Эти и другие обстоятельства обуславливают актуальность и политико-правовую значимость исследования состояния агропромышленного комплекса современной России. Агропромышленный комплекс является важной часть народного хозяйства страны. Он объединяет такие отрасли экономики как производство сельскохозяйственной продукции, переработку продукции и доведение её до потребителя. Развитие агропромышленного комплекса сильно отражается на экономике страны, поскольку его продукция составляет от всех товаров народного потребления.

Основной темой ближайших перспектив стало опережающее конкурентное развитие АПК на основе модернизации большинства его отраслей и возрождения отдельных направлений. Включились в активную практическую работу отраслевые институты агропромышленного комплекса для внедрения передовых, инновационных российских технологий.

Для развития агропромышленного комплекса в РФ является вопрос кадрового резерва в АПК. Кадровый резерв – это группа сотрудников (специалистов, руководителей), которые потенциально способны к руководящей деятельности, отвечают требованиям, предъявляемым должностью, прошли отбор и квалификационную подготовку, но еще не назначены на должность. Ведь создание кадрового резерва является инструментом эффективной управленческой политики, без которой невозможно реализовать такие важные сферы как сельское хозяйство и АПК в целом. Экономический мировой кризис и санкции стран запада относительно Российской Федерации требуют разработки и внедрения эффективных механизмов государственной поддержки производства в области сельского хозяйства, соответствующих условиям реализации стратегии импортозамещения. При этом важно использовать соответствующие информационные технологии в образовательном процессе [5], с учетом норм действующего законодательства [6].

В современных условиях частичной экономической изоляции является необходимым повышение конкурентоспособности российских производителей товаров сельского хозяйства [7]. Это является необходимым по причине того, что, в условиях импортозамещения спрос идет только на ту продукцию, которая соответствует высоким требованиям качества и чьи аналоги попали под эмбарго. Но помимо этого для успешной реализации заданной политики импортозамещения специалистам в аграрной сфере необходимо получать адекватную поставленным целям государственную поддержку, методы и формы которой должны активизировать агропромышленное производство путем дифференциации проводимых мероприятий с учетом условий производства у специалистов сельского хозяйства, их финансово-экономического положения, особенностей местонахождения и прочих факторов.

Эксперты отмечают, что большинство региональных АПК крайне заинтересовано в совершенствовании мероприятий государственной поддержки в рамках осуществления стратегического плана импортозамещения, особенно, касательно формирования экспертного потенциала.

В сложившихся условиях функционирования для Российской Федерации необходима подготовка, переподготовка и повышение квалификации кадров, способных обеспечить конкурентоспособность сельскохозяйственной продукции и продовольствия на внутреннем и внешнем рынках на основе инновационного развития агропромышленного комплекса, создания благоприятных условий для развития предпринимательства, повышения инвестиционной привлекательности отрасли. В этой связи необходимо выделить приоритетные задачи региональной аграрной политики по развитию кадрового потенциала сельского хозяйства. В качестве основных направлений, способствующих повышению эффективности аграрной экономики, следует обозначить совершенствование содержания и технологий непрерывного аграрного образования на основе взаимодействия образовательных учреждения, органов власти субъектов Российской Федерации и аграрного бизнеса, в том числе создание базы НПА, регулирующих вопросы трудоустройства, взаимоотношения образовательных уч-

реждений с работодателями, службой занятости, а также стимулирования закрепления молодых специалистов в аграрном секторе.

Органам местного самоуправления необходима поддерживать сельскохозяйственного производство, развивать соответствующую инфраструктуру: строить дороги, обеспечивать работников жильем, доплачивать из областного бюджета дополнительные выплаты к заработной плате в течение нескольких лет для мотивации специалистов. Внедрение системы мониторинга и управления обеспечением высококвалифицированными кадрами аграрного сектора экономики регионального АПК, создание механизмов для получения обратной связи от выпускников образовательных учреждений о качестве подготовки и трудоустройстве по специальности, так и от работодателей об уровне подготовки молодых специалистов.

Библиографический список

1. Тепляшин, И.В. Система взаимодействия общественности и органов местного самоуправления как условие развития предпринимательства на муниципальном уровне / И.В. Тепляшин, В.А. Власов // Муниципальная служба: правовые вопросы. – 2019. – № 2. – С. 25–28.
2. Бураева, Е.В. Аграрное образование: место и роль в кадровом обеспечении АПК / Е.В. Бураева // Вестник ОрелГАУ. – 2017. – № 6 (69). – С. 7.
3. Дорофеева, А.М. Совершенствование процесса подготовки кадров для агропромышленного комплекса / А.М. Дорофеева, Т.В. Шевченко // Международный журнал прикладных наук и технологий «Integral». – 2018. – № 2. – С. 6.
4. Морозов, В.А. Внешнеторговые проблемы развития АПК РФ / В.А. Морозов // Российский внешнеэкономический вестник. – 2018. – № 3. – С. 7.
5. Трашкова, С.М. Некоторые теоретико-правовые аспекты по использованию информационных технологий в образовании / С.М. Трашкова // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. науч.-практ. конф. / отв. за вып. В.Л. Бопп. – Красноярск, 2016. – С. 82–84.
6. Трашкова, С.М. Основы правового регулирования использования информационных технологий в образовании / С.М. Трашкова // Инновационные тенденции развития российской науки: мат-лы IX междунар. науч.-практ. конф. / отв. за вып. В.Л. Бопп. – Красноярск, 2016. – С. 27–30.
7. Шитова, Т.В. Современные проблемы санкций в международном праве // Аграрное и земельное право. – 2019. – № 3 (171). – С. 90–91.

УДК 34.6:004

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ РОССИИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Фастович Галина Геннадьевна
старший преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

В статье рассмотрены вопросы информационных технологий, применяемых в правоохранительной деятельности современной России. Представленное исследование в сфере информационных технологий позволяет судить о совершенствовании и эффективности государственного механизма в целом.

Ключевые слова: *цифровизация, правоохранительная деятельность информационные технологии, эффективность, государственный механизм.*

APPLICATION OF INFORMATION TECHNOLOGIES IN THE LAW ENFORCEMENT OF RUSSIA: QUESTIONS OF THEORY AND PRACTICE

Fastovich Galina Gennadevna
Senior Lecturer
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The article considers the issues of information technology used in law enforcement in modern Russia. The presented study in the field of information technology allows us to judge the improvement and effectiveness of the state mechanism as a whole.

Keywords*: digitalization, information technology, law enforcement, efficiency, state mechanism.*

Информационные технологии и компьютеризация выделяют вероятность усовершенствовать и облегчить правоохранительную деятельность, а полная или частичная его автоматизация рабочего процесса позволит облегчить труд специалистов в целом. Основная сущность и роль информационных технологий – это предоставление, хранение, обработка и восприятие информационных технологий. Информационная система в органах внутренних дел предназначена для передачи, сбора, обработки, регистрации, хранения, а также выдачи информации по запросам [2, с. 15]. Информация, которая подлежит защите в органах внутренних дел, как правило, являются документированные данные, которые образуются в результате профессиональной деятельности [4, с. 28].

Эффективность борьбы с преступностью находится в прямой зависимости от информационно-технологического обеспечения этой деятельности, однако, несмотря на достигнутые показатели в этом направлении, в настоящее время информационно-технологическое обеспечение правоохранительной дея-

тельности имеет ряд отраслевых и межотраслевых проблем.

В настоящее время использование информационных технологий в уголовном судопроизводстве позволяет представить в формальном виде, полезное для использования, научных познаний и практического опыта для реализации и организаций общественных процессов. С помощью технологий, внедряются специализированные системы принятия решений. Процедура принятия решений в уголовном судопроизводстве может быть характеризовано как мыслительно-интеллектуальный процесс, суть которого состоит в выборе цели, поступков и предварительном анализе фактической и правовой информации.

В настоящее время, можно считать общепризнанным то, что формализация процесса решения любого типа задачи, является алгоритмизацией. Пример: в судебном деле в Республике Казахстан энергично применяются электронные сервисы, направляемые на занимающие большое пространство процессы усовершенствования уголовного процесса [4]. Проводятся работы по включению новых решений для улучшения работы правоохранительной деятельности.

1. Целью данного судопроизводства является внедрение цифровых технологий в уголовном процессе, повышение его прозрачности, снижение сроков уголовного процесса, повышение эффективности затрат на бумажное делопроизводство, а также разрешение доступа к материалам дела в режиме реального времени [3].

Внедрение современных информационных технологий в правоохранительный процесс считается положительным аспектом, тем более что положительные факторы их использования уже известны. Цифровой формат ускорит принятие решений, сделает лучше защиту прав участников процесса, уменьшит коррупцию и злоупотребления. Цифровизация уголовного процесса дозволит решить ряд чувствительных для населения вопросов, а еще облегчит функцию сбора доказательств и составления процессуальных документов, понизит опасность фальсификации материалов дела.

Можно отметить, что в сфере информационных технологий появляются новые преступления, такие как нарушение целостности, доступности и конфиденциальности электронных данных, объектом которых выступают охраняемые законом интересы, возникшие в связи с развитием информационных технологий. То есть компьютерные преступления. Кроме того, Интернет-ресурсы все чаще выступают средством общения соучастников преступлений, а именно (сбыт наркотических средств и психотропных веществ, совершение различного рода хищений чужого имущества, и т.д.). По всему миру информационные сети используются для совершения деяний, ответственность за которые предусмотрена уголовным законодательством многих государств. Это обуславливает необходимость уделения внимания соответствующим вопросам в рамках криминалистики [1] и уголовного процесса [8].

Изученное позволяет отметить, что все недостатки и проблемы защиты информации в регистрационной деятельности органов внутренних дел, во-первых связаны с отсутствием развития системы ведомственного правового обеспечения, что соответственно приводит к противоречивости норм, а далее является и нарушением правил оборота регистрационной информации [6; с. 26].

Во-вторых, правовое регулирование деятельности органов внутренних дел, связанная с регистрацией, как правило, осуществляется, непосредственно ведомственными нормативными актами, поскольку действующие нормативно-правовые акты содержат в себе отсылочный характер. В-третьих, сотрудники органов внутренних дел часто могут оказаться субъектами разглашения регистрационной информации [7, с. 90].

Для наиболее полного осмысления проблем правового обеспечения защиты информации в рамках института регистрации, как правило, следует провести комплексный анализ регистрационной деятельности в органах внутренних дел. Неполноценность правового обеспечения в данной сфере во многом обусловлена отсутствием научной базы, и именно в связи с этим научная разработка указанного направления административно-правовой и информационной науки является весьма актуальной.

Таким образом, одной из важных проблем в сфере защиты информации в регистрационной деятельности органов внутренних дел считается установление административной ответственности за несанкционированный доступ к компьютерной информации. Однако в том случае если в качестве исходной посылки для цепи рассуждений принять во внимание тот факт, что в качестве уголовно-наказуемого деяния может рассматриваться ситуация, когда неправомерный доступ повлек уничтожение, модификацию либо блокирование, либо копирование информации, нарушение работы ЭВМ и т.д. К такому случаю можно отнести неправомерный доступ к компьютерной информации, в том случае если деяние повлекло блокирование, уничтожение, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ либо их сети.

Библиографический список

1. Антонов, В.П. Криминалистика: учебник / В.П. Антонов, И.И. Белозерова, Л.В. Бертовский [и др.]. – М.: РГ-Пресс, 2018. – 960 с.

2. Бабаш, А.В. Информационная безопасность / А.В. Бабаш. – М.: КноРус, 2013. – 136 с.

3. Бертовский, Л.В. Цифровое судопроизводство: проблемы становления / Л.В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства: сб. мат-лов междунар. науч.-практ. конф. 2018. – С. 173–178.

4. Гафнер, В.В. Информационная безопасность / В.В. Гафнер. – М.: Феникс, 2014. – 336 с.

5. Мельников, В.П. Информационная безопасность и защита информации. / В.П. Мельников. – М.: Академия, 2016. – 282 с.

6. Тепляшин, И.В. Система взаимодействия общественности и органов местного самоуправления как условие развития предпринимательства на муниципальном уровне / И.В. Тепляшин, В.А. Власов // Муниципальная служба: правовые вопросы. – 2019. – № 2. – С. 25–28.

7. Шитова, Т.В. Современные проблемы санкций в международном праве / Т.В. Шитова // Аграрное и земельное право. – 2019. – № 3 (171). – С. 90–91.

8. Уголовно-процессуальное право / под ред. Л.В. Бертовского, В.Н. Ма-

хова. – М.: Проспект, 2020 – 656 с.
УДК 343.1:347:004

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СУДЕБНОМ ПРОЦЕССЕ

Федотова Елена Леонидовна
кандидат педагогических наук, доцент
Гончаров Федор Юрьевич
Национальный исследовательский университет «МИЭТ», Москва, Россия

Статья посвящена анализу применения технологий искусственного интеллекта в сфере «электронного правосудия». Цифровые технологии способны резко сократить сроки рассмотрения и разрешения споров, оптимизировать судебные процедуры и повысить эффективность судопроизводства, исключить такие присущие человеку факторы как невнимательность и предвзятость. В статье описываются подходы к обработке и анализу судебных материалов, а также прогнозирования на их основе судебных вердиктов. Наиболее подходящими для этих целей являются технологии, основанные на искусственных нейронных сетях. В рамках статьи рассматриваются методы и способы построения искусственной нейронной сети, применяемой для решения данной задачи. Также рассмотрены этические вопросы использования искусственного интеллекта в области судебного права, сформулированы принципы, предъявляемые к автоматизированной обработке судебных решений и данных, и делается вывод, что современные технологии могут существенно облегчить и упростить доступ к правосудию. При этом важно понимать, что внедрение искусственного интеллекта в судебный процесс должно предусматривать взвешенный и осторожный подход.

Ключевые слова: *искусственный интеллект, автоматизация судебной деятельности, электронное правосудие, предиктивный анализ, большие данные, искусственная нейронная сеть.*

THE USE OF ARTIFICIAL INTELLIGENCE IN LITIGATION

Fedotova Elena Leonidovna
candidate of pedagogical Sciences, associate Professor
Goncharov Fedor Yuryevich
National Research University of Electronic Technology (MIET), Moscow, Russia

This article analyzes the use of artificial intelligence in the field of e-justice technologies. Digital technologies can drastically reduce the time for consideration and resolution of disputes, optimize judicial procedures and increase the efficiency of legal proceedings, and eliminate such inherent factors as inattention and bias. The article describes approaches to the processing and analysis of court materials, as

well as forecasting court verdicts based on them. The most suitable technologies for these purposes are based on artificial neural networks. The article discusses methods and of constructing an artificial neural network for solution of this problem. There are also considered the ethical issues of using artificial intelligence in the field of judicial law, formulates the principles for automated processing of court decisions and data, and concludes that modern technologies can significantly facilitate and simplify access to justice. At the same time, it is important to understand that the introduction of artificial intelligence in the judicial process should provide for a balanced and cautious approach.

***Keywords**: artificial intelligence, judicial automation, e-justice, predictive analysis, big data, artificial neural network.*

Развитие информационных технологий в России и переход к цифровой экономике предполагает повсеместное использование нейронных сетей или технологии искусственного интеллекта. При этом нельзя обойти вопрос о внедрении систем искусственного интеллекта в судебную систему Российской Федерации.

Искусственный интеллект стремится проникнуть во все сферы нашей жизни, понемногу догоняя человеческий. И если машина с успехом заменяет человека в различных сферах экономической деятельности: производстве, банковской и страховой деятельности, то почему не может сделать этого в зале суда? Ведь испокон веков говорят о предвзятости и невнимательности представителей этой ветви власти, а компьютер может сделать точный анализ и вынести разумное, верное и неподкупное решение, руководствуясь исключительно законом и неопровержимой математической логикой, а не эмоциями, которыми машина обладать не может. В последние годы в правоведческой среде все чаще обсуждается вопрос о том, можно ли автоматизировать весь процесс отправления правосудия, т.е. заменить судью искусственной нейросетью, которая будет способна на основе представленных доказательств и фактических обстоятельств дела, выносить соответствующее решение, и таким образом осуществлять «электронное правосудие».

Термин «электронное правосудие» используется в последние годы часто. За электронную судью выдаются компьютерные программы по составлению постановлений о привлечении к административной ответственности за правонарушения в случае фиксации их работающими в автоматическом режиме специальными техническими средствами, имеющими функции фото- и киносъемки, видеозаписи; зарубежный опыт вынесения решений компьютерной программой о выдаче лицензий, отказах в выплате компенсаций и т. п. [1]. В таких случаях вслед за фиксацией одного или двух-трех фактов без проверки обстоятельств, которые могут привести к иным выводам, выносится решение по юридическому делу. Для таких мер существует понятие "автоматические санкции" [2]. Споры об обстоятельствах, подлежащих установлению по делу, о соответствии обстоятельств дела юридическим фактам, признакам деяний, установленных применяемой в таком порядке нормой права, о коллизиях и пробелах

правового регулирования спорных отношений разрешаются уже при обжаловании решений, выносимых названным способом, которые являются итоговыми, если их не обжалуют. Таким образом, указанные программы оптимизируют правоприменительный процесс по бесспорным делам, но не решают задач перевода сущности правоприменительного процесса на язык информационных технологий.

Между тем задача определения вероятного решения суда на основе обстоятельств дела схожа по сути с задачей определения настроения документа на основании его содержания (Sentiment Analysis из области обработки естественных языков), ведь в обоих случаях суть заключается в бинарной классификации текста на основании его текста.

В последние годы благодаря фантастическому росту уровня обработки естественного языка NLP (Natural Language Processing) и машинного обучения, появились новые инструменты для построения прогностических моделей, в том числе моделей, способных раскрывать закономерности вынесения тех или иных судебных решений.

Наиболее сложными для типизации являются фрагменты судебного производства, которые обусловлены осмыслением прогноза как важнейшей фазы поведенческого контроля. В частности, суд, исходя из предвидения относительно юридически значимого поведения участников дела, принимает решение относительно применения мер судебного воздействия (обеспечительных мер, ареста, освобождения под залог, изменение меры пресечения и т.п.).

В этом направлении перспективно использование Big Data. Технология способна анализировать тысячи похожих дел, по ключевым словам, и выдавать свои прогнозы с учетом личности участника процесса.

Представляется, что сама по себе деятельность по предсказанию исхода дела является в значительной мере аналитической деятельностью, где логика как основной инструмент вполне освоена машинами, способными осуществлять такую работу на порядок глубже, детальнее и быстрее. Например, при помощи технологии Case Strategy, за короткое время анализирующей множество релевантной информации, можно получить прогноз даже с учетом личности судьи, который будет рассматривать дело (пример: сервис https://predictice.com/). E-discovery осуществляет поиск электронной информации путем обнаружения, сбора и представления сведений, хранящихся на цифровых носителях: в электронных письмах, презентациях, базах данных и любых других документах, способных быть доказательствами в судебном разбирательстве [3]. Данная технология наиболее развита в США и Великобритании в силу прецедентной правовой системы.

Для работы же суда с информацией субъективного элемента наиболее подходит искусственная нейронная сеть (ИНС). ИНС самообучаема. Предиктивные возможности нейронной сети обусловлены ее способностью к обобщению и выявлению скрытых зависимостей между исходными данными. После обучения сеть способна предсказать будущее значение некой последовательности на основе изучения прогнозного фона: существовавших в прошлом или су-

ществующих в настоящий момент факторов.

При обучении алгоритмы машинного обучения определяют зависимости в размеченном наборе данных. Для этого создается большой набор специально сконструированных из предложений признаков, который затем используется для обучения одного из алгоритмов классификации (например, SVM (Support Vector Machine) или Наивной Байесовской модели [4]). Большинство работ по этим методам фокусируются на построении вышеупомянутых признаков. Так, например, было показано, что использование последовательностей из заданного количества подряд идущих слов (N-gram) в качестве признаков позволяет добиться хороших результатов [5].

При решении задачи Sentiment Analysis многие алгоритмы используют так называемые словари окраски (Sentiment Lexicons) [6]. Эти словари, по сути представляют собой таблицы отображения слов в некоторую численную величину описывающую окраску слова. Часто эти словари создаются вручную, однако есть способы их построения на основе различной метаинформации. Однако данный подход плохо применим к решению задач юриспруденции, т.к. в формальных текстах не принято использовать слова, явно отображающие позицию автора.

В 2013 году был предложен способ векторизации слов Word2Vec основанный на нейронных сетях. В отличие от описанных ранее методов, данный подход строит семантическое представление слова. Для этого используется предположение о том, что контекст использования слов содержит информацию об их смысле. Для обучения модели, вокруг каждого слова выбирается контекст – набор окружающих его слов в окне заданной ширины (размер окна является гиперпараметром модели). Есть два основных способа использования контекста для построения отображения:

• **модель Skip-gram.** Перед обучениям всем словам корпуса присваиваются порядковые номера. На стадии обучения на вход нейронной сети подается onehot encoding слова w(t) – вектор, все компоненты которого равны нулю, кроме той, чей номер совпадает с номером слова: она равна единице. Данное представление является входными данными для полносвязного слоя с линейной активацией. Его задачей является построение искомого скрытого представления слов. Наконец, упомянутый полносвязный слой связан с выходным слоем, которой при помощи softmax активации определяет вероятности принадлежности слов контексту w(t). После обучения, можно использовать матрицу весов скрытого слоя для получения векторизации слов.

• **модель непрерывного мешка слов (CBOW).** Данный подход обладает архитектурой, схожей с моделью Skip-gram, однако противоположен по сути: он ставит своей задачей предсказание самого слова w(t) на основании onehot encoding контекста.

Таким образом, Word2Vec создает некоторое пространство семантического описания языка. При этом интересным является тот факт, что данное пространство обладает некоторой внутренней структурой: так, например, близкие по смыслу слова, зачастую, отображаются в близкие точки пространства. Более

того, в данном пространстве наблюдаются некоторые метрические соотношения: вектор разности слов «Россия» и «Москва» близок к вектору разности слов «Франция» и «Париж». Данный факт позволяет говорить об осмысленности использования средних Word2Vec векторов предложений в качестве их семантического описания. Используя модель Word2Vec можно построить классификатор, решающий задачу Sentiment Analysis при помощи простого мешка слов: документ представляется средним значением Word2Vec его слов, после чего это представление можно использовать для применения классического обучения с учителем.

Описанные выше подходы к решению задачи Sentiment Analysis используют лишь один из уровней абстракции: слов, предложений или документов. Однако одно и то же слово в разных контекстах может иметь разную окраску. Поэтому основной целью структурных моделей является создание многоуровневой модели, способной хотя бы частично отражать сложные семантические связи в тексте. Для достижения этой цели документ представляется графом, где решение об окрасе каждого предложения зависит от окраса его соседей, а также окраса всего документа. Т.е. выходом классификатора является набор решений (y^d; y^s_1; y^s_2; …; y^s_n), тут y^d – это окрас документа, а y^s_i — это окрас соответствующего предложения. По аналогии, данные модели могут быть расширены до уровня анализа слов, путем добавления в граф соответствующих им вершин и ребер [7].

Нейронные сети показали выдающиеся результаты в ряде задач обработки естественных языков (NLP). Например, они лежат в основе лучших на сегодняшний день решений не только задачи Sentiment Analysis, но и таких задач, как машинный перевод и семантический анализ текста. В частности, это стало возможно благодаря использованию рекуррентных слоев в архитектуре нейронных сетей (RNN) [8]. Данный метод позволяет учесть информацию о временной зависимости данных. В простейшем случае об RNN слое можно думать, как о нейроне, который хранит в своем внутреннем состоянии информацию о всех увиденных им данных. Для этого его внутреннее состояние в момент времени t добавляется ко входным данным в следующий момент времени t + 1. Данный механизм крайне важен при решении задач NLP, так как наличие внутреннего состояния позволяет учитывать последовательности слов в предложениях и предложений в документе.

С другой стороны, сам факт того, что RNN ячейки хранят в себе информацию обо всех предыдущих моментах времени, может оказаться не очень полезен: так, в длинных последовательностях данных внутренние представление смешивается и информация о ранних точках теряется. И чем длиннее цепочка данных, тем сильнее зашумление внутреннего состояния. Чтобы решить эту проблемы был предложен механизм LSTM ячеек [9]. Они построены таким образом, чтобы не было проблем с хранением информации, встреченной значительное число шагов назад. По сути – это схожая с RNN ячейка, передающая во времени свое внутреннее состояние, однако механизм этой передачи более сложен. Основными структурными деталями архитектуры LSTM ячейки явля-

ются внутреннее состояние, которое хранится отдельно от входных данных, а также механизмы добавления и удаления информации в это внутреннее состояние. Альтернативой механизму LSTM является схожий по сути механизм GRU, являющийся более современным аналогом.

Также стоит упомянуть такое понятие, как двунаправленные рекуррентные слои: RNN и LSTM в качестве внутреннего состояния хранят информацию о предыдущих данных. Однако при анализе текста стоит учитывать контекст, окружающий конкретное слово с обеих сторон. Чтобы преодолеть данное ограничение, можно использовать две LSTM ячейки: в одну подавать данные в прямом порядке, в другую – в обратном, а затем использовать конкатенацию их выходов в качестве конечного результата. Данный подход хорошо проявил себя в различных задачах NLP и применяется практически при любой обработке текста с помощью рекуррентных нейронных сетей.

Стоит отметить, что внутренние механизмы принятия решений нейронными сетями в данной задаче плохо поддаются интерпретации, что затрудняет определение вкладов отдельных слов и предложений. Однако в 2014 году был предложен механизм «внимания» для рекуррентных нейронных сетей [10] (если точнее – для машинного перевода). Он позволяет обойти данное ограничение. Суть механизма внимания Attention заключается в том, чтобы научить нейронную сеть «обращать внимание» на различные участки входных данных в зависимости от контекста. Идея состоит в том, чтобы добавить в нейронную сеть отдельный блок (Attention unit), задачей которого является генерация распределения весов входных данных на основании последовательности исходных точек (а также контекста). В общем случае архитектура Attention unit может быть сколь угодно сложной [11]. Однако в большинстве случаев (особенно при малом количестве данных) можно пользоваться простейшей моделью:

Пусть у нас есть некоторая последовательность точек hi: это может быть, например, результат применения двунаправленного рекуррентного слоя ко входным данным сети. Тогда их комбинированное представление st можно получить с помощью следующих формул:

$$u_i = \tanh(Wh_i + b); \qquad \alpha_{ti} = \frac{e^{u_i^T u_c}}{\sum_i e^{u_i^T u_c}}; \qquad s_t = \sum_i \alpha_{ti} h_i;$$

где W; b – внутренняя матрица весов и смещение внутри механизма внимания;

α_{ti} – веса входных данных, с точки зрения Attention unit;

u_c – вектор контекста. По сути – высокоуровневое представление фиксированного запроса «какие точки входных данных обычно несут полезную информацию». Он является одним из обучаемых параметров сети;

s_t – полученное представление входных данных, по сути – их взвешенная сумма.

Стоит подчеркнуть тот факт, что из построения механизма внимания следует семантика величины α_{ti} – это мера важности отдельных элементов после-

довательности данных. Также важно отметить, что в области обработки естественных языков, добавление к рекуррентной сети механизма внимания приводит к улучшению качества ее работы, что свидетельствует об осмысленности весов α_{ti}.

Стоит подчеркнуть тот факт, что из построения механизма внимания следует семантика величины – это мера важности отдельных элементов последовательности данных.

Также важно отметить, что в области обработки естественных языков, добавление к рекуррентной сети механизма внимания приводит к улучшению качества ее работы, что свидетельствует об осмысленности весов

Для построения действующей компьютерной модели необходима обширная информационная база судебных дел. В Российской Федерации существуют как коммерческие информационные базы (СПС Консультант+, Гарант), так и созданные государством в рамках программы «электронного правосудия» и создания Единого информационного пространства информационные системы ГАС «Правосудие», «Мой арбитр» и др. Хотя данные информационные базы слабо структурированы, все же они могут являться базой для создания программы для компьютерного прогнозирования судебных постановлений.

Стоит отметить, что доступность данных имеет первостепенное значение в сфере предиктивной судебной аналитики. К примеру, школа права Гарвардского университета оцифровала судебные дела с 1600-х годов и до наших дней. Создатели проекта не только выложили сами данные, но и дополнили их бесплатным API. С его помощью разработчики смогут создавать собственные продукты на базе судебных решений. В качестве успешного примера такой разработки можно привести компанию Ravel Law. Этот компания анализирует американские судебные прецеденты и, в отличие от многих других компаний, отталкивается от человека – судьи, а не от дела. Ravel Law структурирует все предыдущие процессы судьи и прослеживает скрытые закономерности его поведения. Таким образом, программа узнает, какие аргументы чаще всего влияют на судью, какая стилистика ведения процесса его раздражает, а какие прецеденты цитируются в его решениях чаще всего. Понимание этих аспектов позволяет адвокату быть более подготовленным на заседании, а клиенту – понимать, стоит ли вообще обращаться в суд.

Сложно сделать однозначный вывод о том, полезны или вредны для общества в целом и судебной системы в частности технологии предиктивной судебной аналитики. С одной стороны, анализ правовых данных поможет модернизировать и улучшить нынешнюю систему правосудия: государство может использовать данные, чтобы вычислять предвзятых и непоследовательных судей, судья – чтобы знать собственные недостатки, а истец – чтобы понимать, стоит ли ему вообще обращаться в суд, тратить собственные денежные ресурсы и время в ситуации, когда иск с большой долей вероятности не будет удовлетворен.

С другой стороны, обработка больших данных всегда влечет за собой проблему асимметрии информации – одна из сторон процесса в силу обладания большей информацией сможет знать почти точную вероятность выигрыша в

суде, а другая сможет полагаться лишь на собственные суждения. Большая проблема заключается в дилемме, которая возникнет, если мы дойдем до времени, когда цифры станут предсказывать исход дела – отзовете ли вы свой иск, основываясь только на данных предиктивной судебной аналитики? Это серьезная уже этическая, а не технологическая дилемма.

Этические вопросы использования искусственного интеллекта в правосудии беспокоят не только исследователей-правоведов, но и все мировое сообщество. Высказываются предположения о том, что использование в правосудии искусственного интеллекта таит опасность сделать человека, его права и свободы уязвимыми, а само правосудие бесчеловечным и формальным. Для того, чтобы развеять эти сомнения в мировом сообществе делаются первые шаги. Так, в декабре 2018 года Европейской Комиссией по эффективности правосудия одобрена «Европейская Этическая Хартия использования искусственного интеллекта в судебной и правоохранительной системах» [12] в которой изложены пять основных принципов, предъявляемых к автоматизированной обработке судебных решений и данных на основе методов искусственного интеллекта:

1. Принцип соблюдения основных прав: обеспечить разработку и применение инструментов и услуг, основанных на искусственном интеллекте, соответствующих основным правам.

2. Принцип недискриминации: а именно, предупреждать развитие или усиление дискриминации между отдельными лицами или группами лиц.

3. Принцип качества и безопасности: касательно обработки судебных решений и данных, использовать сертифицированные источники и нематериальные данные с применением моделей, разработанных на междисциплинарной основе, в безопасной технологической среде.

4. Принцип прозрачности, беспристрастности и достоверности: сделать доступными и понятными методы обработки данных, разрешить проведение внешнего аудита.

5. Принцип контроля пользователем: отказаться от предписывающего подхода и позволить пользователю выступать информированным участником и контролировать свой выбор.

Особый интерес вызывает «Принцип контроля пользователем», который позволяет судье не согласится с решением предложенным искусственным интеллектом и принять решение по собственному усмотрению, а участнику судебного процесса использовать возможность оспорить решение, принятое искусственным интеллектом или вообще отказаться от использования искусственного интеллекта в процессе и передать разрешение дела напрямую судье.

Несмотря на существующий в обществе скептицизм к применению искусственного интеллекта в судебном правоприменении, стоит отметить, что современные технологии при их умелом использовании могут существенно облегчить и упростить доступ к правосудию. При этом важно понимать, что внедрение информационных технологий в судебный процесс должно предусматривать взвешенный и осторожный подход, поскольку наряду с преимуществами, такие технологии могут нести риски.

Библиографический список

1. Patrick Gillespie. This AI Startup Generates Legal Papers Without Lawyers, and Suggests a Ruling: Bloomberg Businessweek - 2018. - URL: https://clck.ru/MFmgd.

2. Васильев, П. В. Автоматические санкции в российском праве (теория, практика, техника) / под ред. В.А. Толстика. - М.: ЮРЛИТИНФОРМ, 2016. - С. 48-56.

3. The Association for Intelligent Information Management. Intelligent Information Management Glossary: What is eDiscovery? – 2020. - URL: https://www.aiim.org/What-is-eDiscovery

4. Charlotte S. Vlek, Henry Prakken, Silja Renooij, Bart Verheij. A method for explaining Bayesian networks for legal evidence with scenarios: Artificial Intelligence and Law, volume 24, pages 285–324. - 2016. - URL: https://clck.ru/MFnC6.

5. Kushal Dave, Steve Lawrence, David M. Pennock. Mining the Peanut Gallery: Opinion Extraction and Semantic Classification of Product Reviews. — 2003. - URL: https://gate.ac.uk/sale/rnti-09/p519-dave.pdf

6. Saif M. Mohammad, Peter D. Turney. Emotions evoked by common words and phrases: using mechanical turk to create an emotion lexicon. - 2010. - URL: https://dl.acm.org/doi/10.5555/1860631.1860635

7. Ryan T. McDonald, Kerry Hannan, Tyler Neylon, Mike Wells, Jeffrey C. Reynar. Structured models for fine-to-coarse sentiment analysis - 2007. - URL: https://clck.ru/MFnGn.

8. Pengfei Liu, Shafiq Joty, Helen Meng. Fine-grained Opinion Mining with Recurrent Neural Networks and Word Embeddings. - 2015. - URL: https://www.aclweb.org/anthology/D15-1168.pdf.

9. Sepp Hochreiter, Jürgen Schmidhuber. Long short-term memory - 1997. - URL: https://clck.ru/MFnKA

10. Dzmitry Bahdanau, Kyunghyun Cho, Yoshua Bengio. Neural Machine Translation by Jointly Learning to Align and Translate. - 2015. - URL:clck.ru/JsTRj

11. Tang Duyu, Qin Bing, Liu Ting. Aspect level sentiment classification with deep memory network - 2016. - URL: clck.ru/JsTTi.

12. Европейская Комиссия по эффективности правосудия. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года). 2018. – URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4.

УДК 616

ДИАГНОСТИКА ДОМИНАНТ НЕОСОЗНАВАЕМОЙ ПАРАФИЛИИ

Черкасова Елена Сергеевна
кандидат психологических наук
Новосибирский филиал ФГКОУ ВО «Московская академия СК России»
Джафарова Ольга Андреевна
кандидат физико-математических наук, доцент
Федеральное государственное бюджетное научное учреждение «Федеральный исследовательский центр фундаментальной и трансляционной медицины»

Авторы представляют теоретико-экспериментальное обоснование комплексной методики диагностики и объективизации неосознаваемых (латентных) сексуальных побуждений человека, относящихся к половым девиациям. Диагностика неосознаваемых доминант восприятия невербальных знаково-символических объектов, измерение идеомоторных и психофизиологических реакций в качестве индикаторов субъективной значимости стимулов – знаков, являются востребованным направлением изучения противоправного сексуального поведения, в том числе в уголовном судопроизводстве и экспертной деятельности.

***Ключевые слова**: доминанта, парафилия, объективизация, неосознаваемая сфера, сексуальное поведение, половое преступление, девиация.*

DIAGNOSIS OF DOMINANT UNCONSCIOUS PARAPHILIA

Cherkasova Elena Sergeevna
candidate in psychology science
Novosibirsk branch of the «Moscow Academy of science of Russia», Novosibirsk, Russia
Jafarova Olga Andreyevna
candidate of physical and mathematical Sciences, associate Professor
Federal state budgetary scientific institution "Federal research center for fundamental and translational medicine", Novosibirsk, Russia

The authors present a theoretical and experimental substantiation of a complex method of diagnostics and objectification of unconscious (latent) sexual impulses of a person related to sexual deviations. Diagnostics of unconscious dominants of perception of nonverbal sign-symbolic objects, measurement of ideomotor and psychophysiological reactions as indicators of the subjective significance of stimuli-signs are a popular area of study of illegal sexual behavior, including in criminal proceedings and expert activities.

***Keywords**: dominant, paraphilia, objectification, unconscious sphere, sexual behavior, sexual crime, deviation.*

Психодиагностическая представленность в современных психологических исследованиях «мнимого знания» по принципу его сочетания с «болезненным» увлечением статистической психодиагностикой, заслуживает научного внимания по причине реализации результата этой психодиагностики в жизни и судьбе конкретного человека, особенно если речь идет об экспертной психодиагностике в рамках уголовного процесса.

Данная проблема приобретает объемное видение при анализе результатов комплексных психолого-сексолого-психиатрических экспертиз в уголовном судопроизводстве, когда очевидно, что реализуемые в экспертной деятельности критерии оценки вероятности нулевой гипотезы, заимствованные из математической статистики, не адекватны задачам экспертизы. Данное явление имеет место быть в ситуациях, когда подэкспертный и его актуальное состояние как в период реализации экспертизы, так и в предыдущий период (совершения противоправного деяния) никогда не являются «случайным элементарным» событием. Понимание того, что в основе деятельности сознания лежат определенные закономерности и наличие частично осознаваемых или неосознаваемых феноменов в психике подэкспертного, непосредственно влияет на объективность экспертного исследования. Неосознаваемые конструкты отличаются выраженной эмоциональной окраской, не предопределяющей облачение их в вербальную форму. Психодиагностические анкеты, тесты, опросники, включенные в исследовательские модели, предполагают искажение получаемой итоговой информации, предопределяя отсутствие объективности психодиагностического этапа экспериментального исследования. Слабо осознаваемые субъектом эмоциональные структуры имеют психологическую природу и непосредственно связаны с индивидуальностью личности. Их выражение в вербальную форму проблематично по причине недостаточной осознанности. Важно, что при попытке получение от подэкспертного информации о его аффективном уровне, следует реализация исключительно когнитивной информации, непсихологической, рациональной природы, определяемую социальными нормами и окружением. Сочетание в индивидуальном сознании подэкспертного двух реальностей: индивидуальной и отраженной требует обязательного учета при вынесении экспертного суждения. Имплицитная теория личности, представления о жизненном пространстве К. Левина, теория личностных конструктов Дж. Келли, теория личностных смыслов А.Н. Леонтьева, способны оказать неоценимую роль при анализе взаимосвязи индивидуальной и отраженной реальности подэкспертного.

Актуальность создания нового подхода к анализу неосознаваемых мотивов поведения человека, приводящих к совершению сексуальных преступлений лежит в плоскостях когнитивной психологии, клинической психологии, психологии личности, криминалистики, психофизиологии, компьютерных технологий и вызывает научный интерес в связи с включенностью в этот процесс неосознаваемых механизмов, необходимых для однозначной понятийной включенности в происходящее. Описанные в научной литературе сведения о том, что возникающее игнорирование части воспринимаемого имеет последствия

для дальнейшей обработки информации (Park J., Kanwisher N. G.), только отчасти доказывают положение о том, что выбор определенного значения воспринимаемой информации осознается, часто человек даже не подозревает о существовании конкурирующего значения, не ощущает его как недопустимое и игнорирования не происходит. Подобный феномен возможно наблюдать на примере противоправных расстройств сексуального влечения. В настоящее время важным является установление факта предпочтения одного и отвержение другого значения, осуществляемое до момента осознания одного из них. Гипотеза о существовании специальных механизмов, работа которых не осознается, что не исключает их влияния на идеомоторные механизмы человека, требует своего разрешения. Современная клиническая и когнитивная психология, несмотря на определенные разработки данного направления (И.Л. Соломин, П.В. Яньшин, Е.А. Петрова) до настоящего времени однозначно не выделила знаково-символические репрезентации латентных побуждений. Выявленный В. М. Аллахвердовым феномен неосознаваемого негативного выбора; возможность внезапного переключения внимания на ранее оставленный без внимания сенсорный канал в работе Greenwald A. G., Draine S. C., Abrams R. L.; возрастание показателей кожно-гальванической реакции при предъявлении угрожающей вербальной информации в недоступный для осознания период в работе С. Р.Мадди, до настоящего времени не дали ответ на вопрос о вербальной и невербальной семантике неосознаваемых компонентов мотивации. Выявленные закономерности влияния неосознаваемых значений, на результаты когнитивной деятельности, психофизиологические специфичные проявления (Р.В. Чернов, М. Г. Филиппов), в полной мере не доказывают целенаправленное игнорирование дистрактора (непроизвольного внимания), полагаясь на действие непроизвольного внимания с неминуемым последующем психофизиологическим реагированием.

Именно поэтому, целью научного проекта по диагностики несознаваемой парафилии, является обоснование комплексной методики анализа неосознаваемых (латентных) побуждений человека, а именно выявление: психологических, психофизиологических коррелятов обработки информации, что представляет собой как отдельный анализ процесса восприятия неосознаваемых значений, так и его сопоставление с попытками целенаправленного игнорирования объектов, создающих помехи для определенной цели деятельности (дистракторов).

Выявление неосознаваемых доминант латентных побуждений у лиц с расстройствами сексуальных необходимо, исходя из анализа статистических данных Главного управления правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации за период с января по июнь 2019 года совершено изнасилований и покушений на изнасилование 1 979. Важно, что в структуре преступлений непосредственное физическое сексуальное насилие реализовано в 21,4% случаев, а ненасильственные преступления с реализацией аномального сексуального поведения (сексуальные действия по обоюдному согласию с элементами фетишизма, вуайеризма, мазахизма, садизма, эксгибиционизма, раптофилии, гомицидомании и других) составляют

36, 3% от общего числа совершенных противоправных сексуальных действий по данным Следственного комитета Российской Федерации. В качестве дополнительных характеристик сексуальных преступлений, необходимо отметить «особую латентность и пролонгированность данных преступлений, инцестуозный характер их совершения (9% от общего числа), сокрытие этих преступлений как потерпевшими, так и членами их семей, осведомленными о совершенном сексуальном преступлении, но укрывающих факты во избежание наказания за его совершение» [5].

Актуальность объективизации психофизиологических и идеомоторных коррелятов субъективной значимости визуальных стимулов и выраженности доминант латентных неосознаваемых парафилийных побуждений, в контексте криминальной и клинической психологии представлено в работах иностранных ученых. Так, J. Bonta и D. Andrews, рассматривают психологические особенности лиц, совершающих противоправный сексуальный деликт, в контексте идеомоторной активности; G. Baranowski изучал поведенческие и психологические аспекты управления сексуальным преступником при прохождении опроса с использованием полиграфа; L. Berkowitz завершил исследования, посвященные изучению причин и последствий агрессии, включая и сексуальную агрессию. Работа L. Berkowitz не затрагивает психофизиологических методов исследования раптофилии, уделяя внимание созданию условий контроля агрессивного сексуального поведения. J. Bradford занимался исследованиями нейробиологии и нейрофармакалогии сексуально-аномального поведения, психофизиологические параметры при мониторинге не являлись целью его работы. C.R. Clipson исследовал вербальные семантические стимулы в качестве неэкспертной формы установления сексуального правонарушения. Использование психоаналитического подхода в анализе психической деятельности с точки зрения конструкции ассоциаций и смыслов, позволило устанавливают возможность экспертно оценивать расстройства ассоциативных связей в контексте значимости отдельных элементов психосемантической сферы, в целом данные аспекты исследовательской работы направлены на диагностику и экспертизу мотивационной основы девиантного поведения.

Учет ранее выявленных достоинств и недостатков при внедрении психофизиологических исследований диагностики неосознаваемых латентных побуждений человека, позволил расширить имеющийся отечественный опыт реализации взаимосвязи психологии и физиологии на этапе диагностики, исключив ранее выделенные негативные моменты в реализации. Психозондирование на основе системы MindReader, представленное в работе А.А. Ткаченко, Г.Е. Введенского и Н.В. Дворянчикова имеет объективное ограничение в применении в качестве экспертного метода. Наличие психиатрической патологии у лиц, проходящих исследование, в виде органического поражения головного мозга и различные степени умственной отсталости, не позволяют использовать данный вербально-семантический метод в отечественной экспертной практике. Указанная категория лиц адекватно воспринимать, понимать семантические стимулы, при двойном маскировании в системе MindReader не в состоянии именно по

причине органической деструкции. К сожалению, данная категория лиц при совершаемых преступлениях аномального сексуального поведения составляет, по мнению Т.В. Петиной, старшего научного сотрудника Отдела Судебно-психиатрических экспертиз ГНЦССП им. В.П. Сербского, значительное большинство. Перверсии, развивающиеся на фоне раннего или приобретаемого в процессе жизни органического поражения головного мозга, помимо стойкости (А.В. Арутюнян) обладают в значительной степени рецидивом в совокупности с утяжелением деликта. Важным негативным моментом, препятствующим реализации системы MindReader в отечественной практике, является не возможность диагностики идеаторного компонента до его реализации в идеомоторном акте.

Методика viewing time (VT) «измерение времени визуального восприятия», созданная и апробированная G.G. Abelem, J. Huffmanom, B. Warbergom, C. L. Hollandom позволяет устанавливать взаимосвязь между зрительной реакцией и психофизиологическим откликом плетизмограммы в области изучения мотивации, в том числе сексуально-первертной. Важно, что в рамках реализации проблемы экспериментального изучения неосознаваемого восприятия данные психофизиологические возможности сводится к попыткам выявить пороговую разницу между двумя индикаторами: один из них – показатель осознания стимула; другой – подпорогового (по отношению к осознанию) эффекта этого стимула. Разница в пороговой величине этих двух индикаторов составляет область бессознательного или неосознаваемого, в пределах которой внешний стимул может вызывать вегетативные и биоэлектрические реакции, а также влиять на поведенческие и психические функции человека. О факте осознания стимула субъект подэкспертный сообщает в словесном отчёте или с помощью произвольной двигательной реакции. Наибольшие теоретические и методические трудности связаны именно с этими индикаторами сознания, так как они существенно зависят от критериев, которые подэкспертный использует при принятии решения о наличии стимула и своей произвольной реакции на него.

Наиболее трудная и важная проблема экспериментального исследования бессознательных психических явлений заключается в том, что данные о реальности семантического анализа на неосознаваемом уровне не только в случаях психологической защиты при повышении порога осознания эмоционально значимых слов, но и в случаях действия вербальных стимулов вне поля фокусированного внимания субъекта, связаны с вербальной активностью и проблемами ее восприятия. Однако далеко не всегда приводятся твердые доказательства того, что словесный стимул хотя бы частично не осознаётся и, вследствие индивидуальных особенностей испытуемого, не сообщается им, так как испытуемый не полностью уверен в наличии данного стимула.

Положения психологии и психофизиологии неосознаваемых явлений психической жизни человека, дают возможность раскрыть механизмы и способы объективации неосознаваемых переживаний, отношений, мотивов в языке тела человека, идеомоторных актах, психофизиологических реакциях и т.п. [4, с. 228–232] данному вопросу посвящены известные научные публикации

К-Г. Юнга, Дж.Брунера, Дж. Леду, Н.Ф. Диксона, П.В, Симонова, Э.А. Костандова, Б.Ю . Александрова и других авторов.

Широкий круг психических явлений у человека в норме и патологии связан с неосознаваемым как подпороговым (по отношению к сознанию) восприятием эмоционально или мотивационно значимых, но физически слабых внешних сигналов, которые не достигают уровня сознания и не осознаются субъектом, однако вызывают вегетативные, биоэлектрические и эмоциональные реакции и могут влиять на процессы высшей нервной деятельности [3, с. 12].

Ещё одна форма неосознаваемого – это когнитивная установка, то есть состояние готовности субъекта к определённой активности, которое формируется на неосознаваемом уровне при наличии двух основных условий: актуальной потребности у субъекта и объективной ситуации её удовлетворения. В данном подходе планируется подтверждение с физиологической точки зрения положения З. Фрейда о консервативности подсознания и относительной стойкости влечений, эмоциональных переживаний и невротических реакций в случаях, когда их повод остается неосознанным для субъекта. Например, в ситуации противоправного сексуального поведения чрезвычайная стойкость влечения у обвиняемых, в соответствии с выдвинутой гипотезой, должна найти свое подтверждение поддержанием условно-рефлекторного механизма, а именно действием на сексуально-отклоняющуюся доминанту неосознаваемых условных стимулов, формирующих и поддерживающих её, а также создающих физиологическую основу «психической зависимости» от парафилийного поведения, четко «укладываясь» в профиль лица [8].

Описание базовых фреймов латентных побуждений и неосознаваемых мотивационных конфликтов. Фрейм – рамка (или фон) восприятия информации, которая дается параллельно или перед основной информацией, задавая логические или эмоциональные рамки ее восприятия для формирования определенного отношения. Визуальные фреймы при диагностике неосознаваемых мотивационных конфликтах и при латентных побуждений лишены отрицательных моментов, связанных с семантическим рядом, нивелируют негативное влияние сдерживающих механизмов (цензуры) и позволяют объективизировать диагностические признаки латентного побуждения, выходя на неосознаваемый уровень. Создавать визуальные фреймы и заменять один фрейм другим (техника невербального рефрейминга) позволит решить задачу превентивного реагирования при формировании социально-приемлемого побуждения, включая сексуальное. В дальнейшем преобразование техники в вербальный рефрейминг, как максимально мощного и способного менять убеждения и мировоззрение в формировании мотивационного поля личности применимо в воспитательных и образовательных задачах правосознания.

Идеомоторные и психофизиологические корреляты субъективной значимости знаковых объектов (стимулов) и выраженности латентных побуждений [2, с. 327], послужили основой разработки диагностического комплекса методов, направленных на определение неосознаваемых (латентных) побуждений человека, что позволяет решить важнейшую задачу при исследовании механиз-

мов возникновения и развития последующей идеомоторной активности, включая противоправные сексуальные деяния.

Установленные соматические, вегетативные, психологические, психофизиологические и кортикальные корреляты, связанные с направленностью внимания, активные в эмоционально-окрашенной стимуляции за счет базовых фреймов латентных побуждений, дадут прогностически- необходимые критерии для установления [5].

Доминанты и индикаторы интенсивности латентных побуждений и неосознаваемых мотивационных конфликтов в предлагаемом подходе позволят комплексно исследовать роль и функцию знаков (индикаторов), включая явления неосознаваемой установки [5]. Диагностированная неосознаваемая готовность субъекта к совершению определенного действия или к реагированию в определенном направлении, что непосредственно относится к идеоторной активности субъекта. Установление наличия неосознаваемого сопровождения совокупности сознательных действий, составляющих идеомоторный компонент и неосознаваемых латентных побуждений, составляющих идеоторный компонент, выраженные в: непроизвольных движениях, тоническом напряжении, психофизиологических реакциях, а также большой класс вегетативных реакций, сопровождающих действия и состояния человека при удовлетворении потребностно-мотивационной сферы, все это является итоговым продуктом диагностики посредством психофизиологического комплекса, созданного на базе ФГБНУ «Федеральный исследовательский центр фундаментальной и трансляционной медицины», в лаборатории компьютерных систем биоуправления [7]. Диагностика неосознаваемых компонентов парафилии в виде ассоциативного эксперимента, реализации метода атрибуции мотивов, неосознаваемого восприятия невербальных знаково-символических объектов, измерения психофизиологических реакций, идеомототорных компонентов и индикаторов субъективной значимости стимулов (знаков), с включенным психофизиологическим мониторированием состояния апробирована в: группе из 20 человек лиц мужского пола без расстройства влечений с целью определения диагностических и психофизиологических критериев необходимых для дальнейшей объективизации на выборке, состоящей из лиц с аномальным сексуальным поведением, реализуемым в противоправном деликте [5].

С целью определения психофизиологических коррелятов и субъективной значимости знаковых объектов (стимулов) и выраженности латентных побуждений проводятся аналитические исследования материалов завершенных уголовных дел, комплексных психолого-сексолого-психиатрических экспертиз по половым преступлениям, совершенным в отношении малолетних и несовершеннолетних в практике деятельности Следственного комитета Российской Федерации по Сибирскому Федеральному округу. За период с апреля 2017 года по декабрь 2019 года корреляты субъективной значимости выделены на выборке 872 человек, что позволило установить особенности психодинамической мотивационной базы для формирования аномального сексуального поведения. Объективизированы взаимосвязи между: особенностями семейной ситуации в

детский и подростковый период развития личности, впоследствии совершившей противоправное сексуальное деяние в отношении малолетнего или несовершеннолетнего; социальным статусом и социально-поведенческими особенности аномальных сексуальных мотивов; выявлены особенности психосексуального развития, кризисного развития, нарушений развития; изучены особенности эмоционально-волевой и когнитивной сфер развития; установлены особенности сферы полового самосознания личности [5]. Установлены корреляции следующих значимых характеристик личности: дизонтогенеза психосексуального развития, семейного воспитания и особенностей эмоционально-волевой сферы, а именно - конфликтность структуры самовосприятия и самоотношения, недостаточная интериоризированость нормативных полоролевых паттернов поведения, искажение когнитивного и эмоционального восприятия женского и/или мужского образов, недостаточная дифференцированность восприятия половозрастных качеств, в том числе объекта сексуального влечения, то есть реконструированы базовые фреймы латентных побуждений. Проведенный фрейм-анализ латентного побуждения, основанный на базовой когнитивной категории дискурса, позволил определить объектов в индивидуальном дизонтогенезе сексуального развития. Эмоциональное использование контекста в виде усиления или ослабления восприятия визуальных стимулов без вербального сопровождения, способного повлиять на потребностно-мотивационную сферу посредством знаково-символической репрезентации, зарекомендовал себя исключительно положительно, что является значимым с позиции реализации исследовательских задач.

Невербальные компоненты закрепляются в виде тезауруса, в знаках, в когнитивных моделях сознания, скриптах, фреймах, позволяя объективизировать восприятие [6], что и достигнуто в ходе реализации апробирования методики предъявления в диагностике неосознаваемых парафилийных компонентов. Результаты фрейм-анализа латентного побуждения, на примере противоправных расстройств сексуального влечения, в виде косвенного информирования на данном этапе проводимого исследования, рассматриваются как инструмент классификации различных точек зрения и выступают способом выявления признаков данного косвенного информирования, с целью выявления и объективизации индикаторов интенсивности латентных побуждений и неосознаваемых мотивационных конфликтов сексуальной сферы, реализованных или «готовых» к реализации в виде сексуально-прессинговых преступлений.

Диагностика с выделением конкретных психофизиологических коррелят субъективной значимости позволяет повысить эффективность психологической и экспертной диагностики в целом, а также представляется необходимой в решении прикладных задач. Способ повышения эффективности и объективности диагностики за счет реализации психофизиологического исследования, позволит проводить анализ реагирования в контексте изучения конкретных идеомоторных паттернов во взаимосвязи с мотивационной значимостью, детерминированной избирательностью внимания при конкретизации отклоняющегося поведения.

Библиографический список

1. Криминалистика / под ред. А.И. Бастрыкина. – М., 2014. – 559 с.
2. Психофизиология / под ред. Ю.А. Александрова. – 3-е изд. – СПб., 2012. – 34 с.
3. Ратинова, Н.А. Саморегуляция поведения при совершении агрессивно-насильственных преступлений: дис. … канд. психол. наук / Н. А. Ратинова. – М., 1998. – С. 12.
4. Ткаченко, А.А. Судебная сексология. / А.А. Ткаченко, Г.Е. Введенский, Н.В. Дворянчиков. – М., 2014. – 648 с.
5. Черкасова, Е.С. Противоправные сексуальные действия в отношении детей: ретроспективный анализ общей характеристики и идеаторно-идеомоторной активности / Е.С. Черкасова // Вестник Московской академии Следственного комитета Российской Федерации. – 2018. – № 4. – С. 189–194.
6. Черкасова, Е.С. Возможности психофизиологического исследования в целях объективизации данных аномального сексуального поведения / Е.С. Черкасова, А.Н. Алехин, А.В. Букин // Вестник Московской академии Следственного комитета Российской Федерации. – № 1. – 2018. – С. 138–142.
7. Черкасова, Е.С. Разновидности идеальных следов в диагностике устанавливаемого события в рамках криминалистической полиграфологии. Материалы международной научно-практической конференции. / Е.С. Черкасова. – М., 2016. – С. 544–547.
8. Черкасова, Е.С. Профайлинг – психологический портрет лица, совершившего насильственное преступление на этапе организации предварительного расследования / Е.С. Черкасова // Расследование преступлений: проблемы и пути их решения. – 2013. – № 2 (2). – С. 411–415.

УДК 347.9:004

ИНФОРМАЦИОННЫЕ СЕРВИСЫ КАК ОДИН ИЗ ЭЛЕМЕНТОВ ЦИФРОВЫХ ТЕХНОЛОГИЙ В АРБИТРАЖНОМ СУДОПРОИЗВОДСТВЕ

Шейко Полина Анатольевна
руководитель секретариата председателя Арбитражного суда Красноярского края, государственный советник юстиции РФ 3 класса
Дадаян Елена Владимировна
кандидат юридических наук, доцент
Сторожева Анна Николаевна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В настоящей статье авторами раскрываются вопросы применения информационных (электронных) сервисов в арбитражных судах Российской Федерации, которые значительно упрощают деятельность не только работников суда, но и участников арбитражного процесса. Делается вывод, что указанные сервисы получили положительные отзывы среди пользователей - участников арбитражного процесса, так как позволяют максимально оперативно, с соблюдением процессуальных сроков удаленно не только подавать исковые заявления, но и обжаловать вынесенные судебные акты.

Ключевые слова: *Арбитражный суд, усиленная квалифицированная электронно-цифровая подпись, арбитражное судопроизводство, участники арбитражного процесса, судебные акты, информационные сервисы, информационные технологии.*

INFORMATION SERVICES AS ONE OF THE ELEMENTS OF DIGITAL TECHNOLOGIES IN ARBITRATION LITIGATION

Sheiko Polina Anatolyevna
head of the secretariat of the chairman of the Arbitration Court of the Krasnoyarsk Territory, state adviser of justice of the Russian Federation 3 classes
Dadayan Elena Vladimirovna
Candidate of law, assistant professor,
Storozheva Anna Nikolaevna
Candidate of law, assistant professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

In this article, the authors disclose the use of information (electronic) services in the arbitration courts of the Russian Federation, which greatly simplify the activities of not only court employees, but also participants in the arbitration process. It is concluded that these services received positive feedback among users - participants

in the arbitration process, as they allow as quickly as possible, in compliance with the procedural deadlines, to remotely file claims and appeal judicial decisions.

Keywords: *Arbitration court, enhanced qualified digital signature, arbitration proceedings, participants in the arbitration process, judicial acts, information services, information technology.*

Вопросы информационных технологий в судопроизводстве поднимаются в трудах не только ученых, но и практикующих юристов. Так, О.А. Капустин полагает, что использование информационных технологий приводит к высвобождению части судебных ресурсов, расходы которых становятся экономически нецелесообразными [1]. Шарифуллин Р.А., Бурганов Р.С., Бикмиев Р.Г. рассматривают технологические, правовые и этические проблемы, возникающие в ходе внедрения современных информационных технологий в процесс отправления правосудия [2]. Брановицкий К.Л. к информационным технологиям в контексте оптимизации арбитражного судопроизводства относит применение судьями при подписании электронного документа усиленной квалифицированной электронной подписи.

В настоящей статье рассмотрим такой информационный как «Мобильная картотека арбитражных дел», «Электронный страж», который позволяет осуществить подписку и отслеживать информацию по делам либо по номеру дела, либо по названию участника. Для получения информации через сервис необходимо пройти процедуру регистрации (наименование, ИНН, ОГРН, адрес, номера телефонов, адрес электронной почты и т.д.) и создать «Личный кабинет», используемый впоследствии также для подачи документов в суд в электронном виде через систему «Мой арбитр». Последний сервис пользуется активнейшим спросом среди участников арбитражного процесса, позволяя максимально оперативно, с соблюдением процессуальных сроков, удаленно подавать исковые заявления (заявления), заявления о выдаче судебных приказов, а также иные дополнительные документы по делам и апелляционные, кассационные, надзорные жалобы по делам, рассматриваемым арбитражными судами. Так, по данным статистики Арбитражного суда Красноярского края в 2019 году количество и доля исковых заявлений (заявлений), поступающих через сервис «Мой арбитр», выросли и составили 29% от общего числа поступивших в суд исковых заявлений (заявлений) (в 2018 году – 23%). Для сравнения, в 2017 году через сервис «Мой арбитр» зарегистрировано 62208 электронных документов, из них 7123 исковых заявления (заявления) или 22% от общего количества поступивших в суд исковых заявлений (заявлений). Таким образом, следует отметить последовательный рост исков (заявлений), подаваемых в суд в электронном виде.

Техническая возможность подавать не только первоначальные исковые заявления, но и дополнительные документы в материалы дела в электронном виде позволяет лицам, участвующим в деле, избежать расходов по изготовлению копий документов и их доставке в арбитражный суд, а Арбитражному суду Красноярского края, в связи с автоматической загрузкой документов в электронном виде в КАД, – сократить затраты по сканированию документов по де-

лам упрощенного производства в целях их размещения в сети Интернет. Кроме того, по делам, рассматриваемым в порядке упрощенного производства, у лиц, участвующих в деле существует и возможность в режиме ограниченного доступа (т.е. только с получением кода доступа к конкретному делу) удаленно знакомиться и с материалами дела, представленными другой стороной по делу.

Хочется обратить внимание еще на одно из последних информационных внедрений в рамках реализации комплекса программ электронного правосудия как обеспечение технической возможности подписания всех публикуемых судебных актов арбитражных судов усиленной электронно-цифровой подписью. Так, абсолютно все публикуемые судебные акты Арбитражного суда Красноярского края, принимаемые судом, выполняются в форме электронного документа, подписанного усиленной квалифицированной электронно-цифровой подписью. Опубликованные в КАД в формате PDF электронные образы судебных актов имеют равноценную силу судебных актов, выполненных на бумажных носителях, и дополнительного заверения не требуют, за исключением случаев, прямо предусмотренных Инструкцией по делопроизводству [4]. Данное нововведение позволяет существенно сократить бюджетные расходы суда на отправку почтовой судебной корреспонденции, поскольку судебные акты, выполненные в форме электронного документа, считаются направленными лицам, участвующим в деле, посредством их размещения на официальном сайте арбитражного суда в информационно-телекоммуникационной сети «Интернет» в режиме ограниченного доступа не позднее следующего дня после дня их принятия, вынесения (часть 1 статьи 177 АПК РФ, часть 1 статьи 186 АПК РФ) и считаются полученными ими на следующий день после дня их размещения на сайте [5].

В заключение нельзя не отметить, что все перечисленные информационные сервисы в арбитражных судах направлены на реализацию положений Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [6]. Поэтому сегодня открытость правосудия давно уже не является частным делом судей, а стала направлением государственной политики. В этой связи огромную значимость приобретают такие революционные инструменты, как прозрачность, доступность отправления правосудия, а также своевременное информирование общественности о ходе и результатах того или иного судебного разбирательства.

Библиографический список

1. Капустин, О.А. Влияние использования информационных технологий в федеральных судах общей юрисдикции на перспективы изменения территориальной судебной организации / О.А. Капустин // Администратор суда. – 2019. – № 2. – С. 3–8.

2. Шарифуллин, Р.А. Проблемы и перспективы внедрения информационных технологий в деятельность судебной системы России / Р.А. Шарифуллин, Р.С. Бурганов, Р.Г. Бикмиев // Российский судья. – 2018. – № 8. – С. 49–53.

3. Брановицкий, К.Л. Использование информационных технологий в контексте оптимизации гражданского судопроизводства / К.Л. Брановицкий // Закон. – 2018. – № 1. – С. 59–70.

4. Постановление Пленума ВАС РФ от 25.12.2013 № 100 (ред. от 11.07.2014) «Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)» // Информационно-поисковая система «Консультант плюс».

5. Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // Информационно-поисковая система «Консультант плюс».

6. Федеральный закон от 22.12.2008 № 262-ФЗ (ред. от 28.12.2017) «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Информационно-поисковая система «Консультант плюс».

УДК 347.9:004

АКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АРБИТРАЖНОМ СУДОПРОИЗВОДСТВЕ

Шейко Полина Анатольевна
руководитель секретариата председателя Арбитражного суда Красноярского края, государственный советник юстиции РФ 3 класса
Дадаян Елена Владимировна
кандидат юридических наук, доцент
Сторожева Анна Николаевна
кандидат юридических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В настоящей статье авторами раскрываются актуальные информационные технологии в Арбитражных судах Российской Федерации. Делается вывод, что современные информационные технологии совершенствуют систему арбитражного судопроизводства, которая отвечает современным информационным технологиям.

Ключевые слова: *Арбитражный суд, информатизация, информационные технологии, интернет-трансляция, арбитражное судопроизводство, открытость, гласность.*

CURRENT INFORMATION TECHNOLOGIES IN ARBITRATION PROCEEDINGS

Sheiko Polina Anatolyevna
head of the secretariat of the chairman of the Arbitration Court of the Krasnoyarsk Territory, state adviser of justice of the Russian Federation 3 classes
Dadayan Elena Vladimirovna
Candidate of law, assistant professor,
Storozheva Anna Nikolaevna
Candidate of law, assistant professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

In this article, the authors reveal current information technologies in the Arbitration courts of the Russian Federation. It is concluded that modern information technologies improve the system of arbitration proceedings that meets modern information technologies.

Keywords: *Arbitration court, Informatization, information technologies, Internet broadcasting, arbitration proceedings, openness, publicity.*

Основополагающим для начала цифровизации судебной системы в России стало Постановление Президиума Совета судей Российской Федерации от 19 февраля 2015 года № 439 «Об утверждении Концепции развития информатизации судов до 2020 года» [1].

В соответствии со статей 11 Арбитражного процессуального кодекса Российской Федерации разбирательство дел, в арбитражных судах отрытое [2]. В современной судебной системе особое значение приобретает совершенствование процедуры судопроизводства, расширение доступа граждан к правосудию и гласность разбирательства дел в судах. Этому способствует повышение степени информатизации судов, расширение области применения компьютерных технологий, создание на этой базе современных и надежных систем отбора, хранения информации, доступа к ней, а также ее использование и распространение.

Так, например, в Арбитражном суде Красноярского края уделяется большое внимание внедрению современных информационных технологий в рабочий процесс обеспечения судопроизводства и делопроизводства, что, безусловно, способствует повышению эффективности и качества отправления правосудия.

Автоматизированные рабочие места работников аппарата суда оснащены технологическим оборудованием, в том числе, сканерами и компьютерной техникой, объединенной в локальную информационную вычислительную сеть суда (серверные диски).

Арбитражные суды первыми в российской судебной системе внедрили техническую возможность проведения судебных заседаний посредством использования систем видеоконференц-связи (далее - ВКС), обеспечивая реализацию прав граждан и представителей организаций на непосредственное и беспрепятственное участие в судебном разбирательстве. На сегодняшний день, с учетом внесенных изменений в Арбитражный процессуальный кодекс Российской Федерации и Гражданский процессуальный кодекс Российской Федерации, возможно проведение судебных заседаний посредством ВКС между арбитражными судами и судами общей юрисдикции.

Системы видеоконференц-связи установлены практически во всех залах судебных заседаний, кроме того по всем судебным заседаниям ведется аудиопротоколирование, а после вступления в силу соответствующих изменений в Арбитражный процессуальный кодекс Российской Федерации будет обеспечена и техническая возможность осуществления и сохранения видеозаписи судебных заседаний.

Данные автоматизированные системы позволяют осуществлять высококачественную аудио- и видеозапись в ходе заседания, а также вести трансляцию судебного заседания в отложенном режиме. Аудиопротокол судебного заседания как отдельный файл в формате mp3 позволяет фиксировать все процессуальные действия в хронологической последовательности, синхронизировать эти действия с полученными записями. Ведение архива аудио- и видеозаписей протоколов судебных заседаний позволяет говорить о возможном переходе на электронный архив хранения дел и документов к судебным делам, обеспечивающее надежное хранение всей полученной информации. При необходимости возможен полнотекстовый поиск по протоколам и реквизитам записей.

Актуальной на сегодня является и возможность интернет – трансляция судебных заседаний. Так, в соответствии с внутренним локальным актом суда и приказом Судебного департамента при Верховном Суде Российской Федерации от 17.10.2017 № 182 «Об утверждении Порядка организации и проведения в су-

дах трансляции судебных заседаний по радио, телевидению и в информационно-телекоммуникационной сети «Интернет» [3] на официальном сайте Арбитражного суда Красноярского края по адресу: www.krasnoyarsk.arbit.ru имеется соответствующий раздел, в котором размещается информация о проведении трансляции предварительных судебных заседаний, судебных заседаний в сети «Интернет» со ссылками на наименование истца, ответчика и СМИ, как источника публикации. В частности, указаны сайты таких телекомпаний, как www.tvk6.ru, www.trk7.ru, www.afontovo.ru, а также www.youtube.com.

Конечно, необходимо отметить, что информационные технологии в Арбитражных судах используются в рамках Федерального закона от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [4]. Поэтому сегодня открытость правосудия давно уже не является частным делом судей, а стала направлением государственной политики. В этой связи огромную значимость приобретают такие демократические инструменты, как прозрачность, доступность правосудия, а также своевременное информирование общественности о ходе того или иного разбирательства. Однако по рейтингам, проводимым на предмет информационной открытости можно отметить, что открытость Арбитражных судов не имеет еще 100 % для всех судов Российской Федерации.

В связи с этим «Правительством РФ намечена реализация до 2024 года концепции комплексного правового регулирования отношений, возникающих в связи с развитием цифровой экономики. Планируется, что в этот период на основе принятых нормативно-правовых актов регуляторная среда в полном объеме обеспечит благоприятный правовой режим для возникновения и развития современных технологий и экономической деятельности, связанной с их использованием в цифровой экономике» [5].

Библиографический список

1. Постановление Президиума Совета судей Российской Федерации от 19 февраля 2015 года № 439 «Об утверждении Концепции развития информатизации судов до 2020 года».

2. Арбитражно-процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (ред. от 02.12.2019) // Консультант Плюс: Законодательство.

3. Приказ Судебного департамента при Верховном Суде Российской Федерации от 17.10.2017 № 182 «Об утверждении Порядка организации и проведения в судах трансляции судебных заседаний по радио, телевидению и в информационно-телекоммуникационной сети «Интернет» // Консультант Плюс: Законодательство.

4. Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Консультант Плюс: Законодательство.

5. Вайпан, В.А. Правовое регулирование цифровой экономики / В.А. Вайпан // Предпринимательское право. Приложение «Право и Бизнес». – 2018. – № 1. – С. 12–17.

УДК 343.9:316.1

АНАЛИЗ СЛЕДОВАТЕЛЕМ СОЦИАЛЬНЫХ МЕДИА В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Шеметов Алексей Константинович
старший преподаватель.
Екатеринбургский филиал ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», Екатеринбург, Москва

В статье рассмотрены основные направления использования информации, имеющейся в социальных медиа. Выделены трудности, с которыми сталкивается следователь при исследовании персональных страниц пользователей в социальных сетях. Автором определены направления повышения эффективности указанной работы.

Ключевые слова: *расследование преступлений, социальные сети, сеть Интернет, аккаунты, анализ информации*

INVESTIGATOR'S ANALYSIS OF SOCIAL MEDIA IN CRIME INVESTIGATION

Shemetov Alexey Konstantinovich
senior teacher
Yekaterinburg branch of the Moscow Academy of the Investigative Committee of the Russian Federation, Yekaterinburg, Russia

The article considers the main directions of using information available in social media. The author highlights the difficulties that the investigator faces when examining users ' personal pages in social networks. The author defines the ways to improve the efficiency of this work.

Keywords: *crime investigation, social networks, Internet, accounts, information analysis*

Развитие технического прогресса в наши дни делает все более доступным использование информационно-коммуникационных сетей каждым человеком. Современный представитель общества практически не мыслим без профилей, личных страниц, аккаунтов в сетевых ресурсах Интернет пространства. Отдельные, наиболее активные в этой сфере пользователи, имеют несколько персональных страниц в разных социальных сетях.

В этой связи становятся все более актуальными вопросы использования информации, содержащейся в сети Интернет, в различных сферах человеческой жизни. Так, совсем недавно в некоторых Европейских и заокеанских странах не утихали скандалы, связанные с использованием технологий анализа информации социальных медиа в целях повышения эффективности избирательной политики отдельными кандидатами. Активно используется информация подобного рода рекаламными компаниями и поисковыми системами.

Используются указанные сведения и правоохранительными органами ряда зарубежных стран. В наибольшей степени это направление получило развитие в США, Германии, Великобритании и др.

К сожаленью, представители российских правоохранительных органов практически не задействуют столь эффективный инструмент поиска и анализа информации об отдельных людях и событиях [3, с. 30].

При этом, использование подобного рода сведений из социальных медиа имеет актуальность при расследовании не только уголовных дел о преступлениях в сфере высоких технологий, но и грамотного для грамотного планирования расследования любой категории, подготовки к проведению отдельных следственных действий, поиска пропавших лиц и субъектов преступлений, выдвижения и проверки версий о других обстоятельствах преступного события.

Несомненно, одной из основных причин столь нечастого обращения к данным, содержащимся в социальных сетях, является сложность поиска, вызванная ограниченностью знаний субъектов расследования об объеме названной информации, месте хранения и отсутствием методик работы с ней.

Думается, что для преодоления указанной проблемы требуется обратиться к многочисленным исследованиям, посвященным проблемам социологического изучения личности в социальных сетях, составления и использования профайлинга.

Некоторые авторы предпринимали попытки подготовки методики использования социальных сетей в работе следователя [2]. Однако подобные рекомендации не раскрывают направлений исследования той или иной информации на персональных страницах пользователя, приводя лишь последовательность обращения к ней самим следователем. При этом субъектом расследования должны быть задействованы методы общей, социальной, юридической психологии, социологии и других отраслей знаний.

При подготовке к следственному действию следователь имеет возможность, изучив страницу в социальных сетях, связи и активность пользователя, получить более подробное представление о свойствах личности участника процесса, запланировать использования определенных тактических приемов для эффективного производства запланированного мероприятия. Особую актуальность это приобретает в ситуациях подготовки к встрече с несовершеннолетним участником уголовного процесса.

Хранящаяся в сети Интернет информация позволяет полно отражать интересы, хобби, психотип конкретного пользователя, накапливает данные о его действиях и поступках в течение долгого времени, а результаты ее анализа могут быть использованы в качестве доказательств [6, с. 202].

Изучение личности пользователя социальной сети способствует не только получению общего представления о психотипе изучаемого, но и установлению конкретных данных о его нахождении в определенном месте в интересующий период времени, знакомстве с отдельными участниками события, характере поддерживаемых с ними отношений и других данных.

Позже, результаты подобного исследования могут применяться для выработки наиболее оптимальной тактики производства следственного действия с его непосредственным участием [1, с. 4; 4, с. 97]. Однако это не единственное направление возможного использования полученных сведений.

Видится вполне эффективной и ситуация формирования на основе полученных данных психологического, рисованного, комплексного либо другого иного портрета неизвестного лица, которому принадлежит персональная страница под вымышленным именем.

Например, в условиях отсутствия данных о лице, призывающем к террористической, экстремистской, суицидальной, и иной антиобщественной деятельности, могут использоваться результаты психологического, лингвистического, криминалистического исследования содержащейся на используемой им странице в социальных сетях информации.

Определенное распространение в судебно следственной практике имеет выяснение склонности к самоубийству у отдельных пользователей сети, а также действительного содержания призывов к определенной деятельности. В этих условиях возможно также привлечение специалистов Минюста, частных сведущих лиц для производства осмотра следователем аккаунтов социальных сетей и Интернет-контента.

Данные, полученные из социальных сетей, могут также позволить отыскивать свидетелей и очевидцев интересующих событий, установить обстоятельства преступного события, организовать поиск субъекта преступления [5, с. 426].

Конечно ввиду недостаточной достоверности некоторых данных, которые могут содержаться на персональной странице пользователя, следователю порой трудно получить реальное представление о выясняемых обстоятельствах. Однако в форме предположения, определенные выводы могут существенно помочь в установлении истины.

Например, анализ участников отдельных сообществ и групп в социальных сетях, увлечение их схожими интересами, факты взаимного общения могут позволить следователю значительно сузить круг проверяемых лиц, определиться с возможными местами сбора представителей отдельных сообществ, приобретения предметов и средств, используемых в преступной деятельности.

Все это требует наличия у следователя специальных навыков аналитической деятельности, работы со столь специфичной информацией, налаживания взаимодействия с отдельными специалистами, которых он будет привлекать.

Требуется помощь следователю и со стороны представителей различных отраслей знаний, с участием которых будут подготовлены методические рекомендации по сбору, обобщению и анализу названных сведений. Еще более удачным видится изготовление автоматизированных программных средств, позволяющих исследовать значительные объемы цифровых данных, располагающихся на разных сетевых ресурсах.

Библиографический список

1. Богданова, Т.В. Методика анализа диалогов в судебной психолингвистической экспертизе по материалам следственных действий и оперативно-розыскных мероприятий на предмет определения наличия и приемов оказываемого воздействия / Т.В. Богданова // Эксперт криминалист. – 2018. – № 3. – С. 3–5.

2. Гамбарова, Е.А. К вопросу о методике использования социальных сетей в работе следователя / Е.А. Гамбарова // Юридический вестник Самарского университета. – Т. 3, № 3. – 2017. – С. 137–141.

3. Гамбарова, Е.А. К вопросу об использовании информации из социальных сетей в работе следователя / Е.А. Гамбарова // Вектор науки ТГУ. Серия: Юридические науки. – 2017. – № 1 (28). – С. 30–31.

4. Иванов, Н.А. Цифровая информация в уголовном процессе / Н.А. Иванов // Библиотека криминалиста. Научный журнал. – 2013. – № 5. – С. 93–102.

5. Цимбал, Н.Г., Использование информации социальных сетей Интернет в ходе предварительного расследования / Н.Г. Цимбал, В.Н. Цимбал // Теория и практика общественного развития. – 2013. – № 10. – С. 425–427.

6. Чернышов, В.Н., Проблемы собирания и использования цифровых доказательств / В.Н. Чернышев, Е.С. Лоскутова // Социально-экономические явления и процессы. – 2017. – Т.12, № 5. – С. 199–203.

УДК 343.1

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ВЫСОКИХ ТЕХНОЛОГИЙ НА ДОСУДЕБНЫХ СТАДИЯХ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Щедрин Денис Николаевич
Красноярский государственный аграрный университет, Красноярск, Россия

В данной статье рассматриваются основы государственной политики в области информационной безопасности методы обеспечения информационной безопасности, а также уделяется внимание организационной и технической защите информации и информационных процессов.

***Ключевые слова**: уголовный процесс, цифровые технологии, основы информационной безопасности, защита информационных ресурсов.*

TO THE QUESTION OF THE USE OF HIGH TECHNOLOGIES IN THE PRE-JUDICIAL STAGES OF CRIMINAL PROCEEDINGS

Shchedrin Denis Nikolaevich
Krasnoyarsk State Agrarian University, Krasnoyarsk, Russia

This article discusses the basics of state policy in the field of information security, methods for ensuring information security, and also focuses on the organizational and technical protection of information and information processes.

***Keywords**: criminal process, digital technologies, the basics of information security, the protection of information resources.*

В соответствии с приказом № 1157 МВД России от 29 декабря 2012 г [1]., для эффективного выполнения следователями и дознавателями своих служебных обязанностей рабочие места должны быть оснащены: персональным компьютером, имеющим доступ к правовым ресурсам и консультационным порталам, а также интернет для организации электронной почты; принтером, сканером, ксероксом (либо МФУ). Как правило, в персональном компьютере следователя содержится вся информация, начиная от шаблонов протоколов, и заканчивая обвинительными заключениями с фотографиями места происшествия, которые содержат конфиденциальную информацию. Как было выше сказано, персональный компьютер должен иметь доступ интернет для организации электронной почты. Но, сейчас интернет используется не только для выхода электронной почты, но и для получения необходимой информации, например, какие объекты находятся непосредственно около места происшествия. Или адрес, куда необходимо направить запрос по тому или иному вопросу.

В настоящее время технология построения локальных компьютерных сетей «Интернет» стала самым распространённым решением. Обычная сеть «Интернет» является одной из самых дешевых в построении из когда-либо разрабо-

танных стандартов локальных сетей. Данный стандарт создан на базе экспериментальной сет Интернет Нетворк, предложенный фирмой Xerox в 1975 году. В сетях «Интернет» все компьютеры имеют непосредственный доступ к обычной шине, поэтому она не может быть использована для передачи данных между двумя узлами сети. Одновременно все компьютеры имеют, возможно, немедленно получить данные, который любой из компьютеров начал передавать на общую шину. Иногда указанное построение сети называют методом коллективного доступа.

Сети «Интернет» завоевали огромную популярность благодаря хорошей пропускной способности, простоте установке, передачи информации приемлемой стоимости сетевого оборудования. Участки сети, для которых скорости данных 50 Мбит/с недостаточно. Легко модернизировать, чтобы повысить эту скорость вплоть до 1 Гбит/с. Однако технология «Интернет» не лишена существенных недостатков. Основной из них – передаваемая информация не защищена. Компьютеры сети оказываются в состоянии перехвата информацию, адресованную соседям. Основной причиной тому является принятый в сети «Интернет» так называемый широковещательный механизм обмена сообщениями. Компьютеры сети, как правило, совместно используют один и тот же коаксиальный кабель, который служит средой для пересылки сообщений между ними. Компьютер сети, желающий передать какое-либо сообщение по общему каналу, должен удостовериться, что этот канал в данный момент свободен [6].

В начале передачи компьютер сканирует несущую частоту сигнала, определяя, не произошло ли искажения сигнала в результате возникновения взаимодействия с другими компьютерами, которые ведут передачу одновременно с ним. При наличии коллизии компьютер начинает прерывать передачу и в итоге замолкает. По истечении некоторого случайного периода времени он пытается повторить передачу. Если компьютер, подключенный к сети «Интернет», ничего не передает сам, он, тем не менее, продолжает сканировать все сообщения, передаваемые другими компьютерами. Заметив в заголовке поступившей порции данных свой сетевой адрес, компьютер копирует эти данные в свою локальную память.

Существует два основных способа объединения компьютеров в сети «Интернет». В первом случае компьютеры соединяются при помощи коаксиального кабеля, а кабель соединяется с сетевым адаптерами Т-образным разъемом (сеть Интернет 10 Base2). В этой сети «Все слышат всех». Любой компьютер, как было сказано ранее, способен перехватывать данные, посылаемые другим компьютером. Во втором случае, каждый компьютер соединён кабелем типа витая пара с отдельным портом центрального коммутирующего устройства – концентратора или коммутатора. В таких сетях, которые называются сетями «Интернет» 10 BaseT, компьютеры поделены на группы, именуемые доменами коллизий. Домены коллизий определяются портами концетратора или коммутатора, замкнутыми на общую шину. В результате коллизии возникают не между компьютерами сети, а по отдельности – между теми из них, которые входят в один и тот же домен коллизий, что повышает пропускную способность сети. В по-

следнее время в крупных сетях стали появляться коммутаторы нового типа, которые не используют широковещание и не замыкают группы портов между собой. Вместо этого все передаваемые по сети, данные буферизируются в память и отправляются по мере возможности. Как уже отмечалось, сетевой адаптер каждого компьютера в сети «Интернет», как правило, слышит все, но обрабатывает и помещает в свою локальную память только те порции (так называемые кадры) данных, которые содержат его уникальный сетевой адрес. В дополнение к этому подавляющее большинство современных Интернет – адаптеров допускают функционирование в особом режиме, называемом беспорядочным. При использовании данного режима адаптер копирует в локальную память компьютера все без исключения передаваемые по сети кадры данных. Специализированые программы, переводящие сетевой адаптер в беспорядочный режим и собирающие весь трафик сети для последующего анализа, называются анализаторами протоколов. Администраторы сетей широко используют анализаторы протоколов для осуществления контроля за работой этих сетей и определения их перезагруженных участков. К сожалению, анализаторы протоколов используются и злоумышленниками, которые с их помощью могут перехватить чужие пароли и другую конфиденциальную информацию. Анализаторы протоколов представляют серьезную опасность. Присутствие их в сети указывает на брешь в защитных механизмах. Установить анализатор протоколов мог посторонний человек, который проник в сеть извне (к примеру, если сеть имеет выход в интернет). Специалисты в области компьютерной безопасности относят данные атаки к так называемым атакам второго уровня. Это значит, что взломщик сумел проникнуть в сеть и теперь стремится развить свой успех, при помощи анализатора протокола он может перехватить как финансовые данные, так и пароли пользователей. Имея достаточные ресурсы, в принципе, он может перехватывать всю информацию, передаваемую по сети.

Анализаторы протоколов существуют для любой платформы. Они исследуют не конкретный компьютер, а протоколы. Поэтому анализаторов протоколов может обосноваться в любом узле сети и оттуда перехватывать сетевой трафик. В результате актуальным является вопрос о об обеспечении информационной безопасности [7]. В качестве мер защиты, необходимо установить сетевой адаптер, который принципиально не может функционировать в беспорядочном режиме. Такие адаптеры существуют. Одни адаптеры не поддерживают беспорядочный режим на аппаратном уровне, а другие снабжаются драйвером, не допускающим работу в беспорядочном режиме. Хотя этот режим и реализован в них аппаратно. В результате надобность в «прослушивании» сетевым адаптером всего трафика для того, чтобы выбирать из него сообщения, адресатом, который является данный компьютер, отпадает [8].

В свою очередь, технологии не стоят на месте и все время двигаются вперед, применяясь в разных сферах, и, что немаловажно, – в системе образования, которая и готовит специалистов, должных применять эти современные технологии, а значит, овладеть ими [11, 12]. Однако очень актуальным является вопрос об их использовании в уголовном процессе [14], о внедрении криминали-

стических методик в правоприменительную деятельность [2], в том числе в профилактических целях [10], учитывая серьезность и специфику общественных отношений, возникающих в данной области. Одним из путей решения вопросов по совершенствованию безопасности компьютеров, на которых содержится информация по материалам проверки, а также уголовного дела, это использование системы «блокчейн» [4].

Технология «блокчейн» (транслитерация с англ. blockchain) - децентрализованная база данных, содержащая информацию о выстроенной по определенным правилам цепочке блоков транзакций.

Применение технологии «блокчейн» возможно практически везде. Сельское хозяйство, бухгалтерский учет, логистика, образование, медицина – в любой сфере возможно транслировать данную технологию. В том числе и в рамках уголовного судопроизводства [3].

С точки зрения эффективности внедрения технологии «блокчейн» при ведении уголовного судопроизводства необходимо ответить на вопрос: позволит ли технология «блокчейн» оптимизировать процессы, безопасно хранить данные либо нет. Например, при сборе цифровых доказательств [13], при фиксации хода и результатов осмотра места происшествия при раскрытии и расследовании преступлений, совершенных с применением информационных компьютерных технологий [5]. В большинстве случаев ответ – «да, возможно». И сейчас зарубежные коллеги стали применять это в сфере уголовного судопроизводства.

В конце ноября 2019 года стало известно, что Шаосинский суд впервые вынес приговор, используя доказательства, которые хранятся в Блокчейн - системе. Народный суд района Шанюй успешно использовал технологию распределенного реестра, чтобы удостовериться в подлинности доказательств и ответить на иск.

Дело касалось ряда мошеннических случаев, совершенных ответчиком. Обвиняемый действовал в нескольких китайских провинциях и заработал около $1400. Благодаря тому, что часть доказательств попала в блокчейн-систему и была успешно сохранена, прокурор сумел доказать судье справедливость претензий истцов, а обвиняемый был приговорен к 14 месяцам тюремного заключения.

В сообщениях местных СМИ, цифровые доказательства, хранящиеся на жетском диске, могут быть утрачены в любой момент, поскольку сам диск может быть поврежден или утерян, в то время как сохранение данных в децентрализованной системе позволяет не только сохранить их, но и быстро проверить достоверность.

Глава Апелляционного суда района Шанюй отметил, что возможность использования блокчейна для шифрования и хранения судебных данных была подтверждена Верховным народным судом Китая еще в 2018 году. Тогда же блокчейн впервые использовался в судебных разбирательствах по гражданским и коммерческим делам, однако в отношении уголовного дела новые технологии использовались впервые [14].

Специалисты напоминают, что хотя блокчейн гарантирует неприкосновенность данных после внесения в систему, стоит учитывать возможность манипуляций с информацией до загрузки. Как и в случае с компакт-диском, источник доказательств должен быть заслуживающим доверия. Впрочем, с развитием технологий этот вопрос тоже постепенно канет в Лету, ведь данные все чаще фиксируются напрямую с датчиков благодаря интернету.

Подводя итог вышесказанному, хочется отметить, что цифровые технологии в Российской Федерации не стоят на месте. При использовании зарубежного опыта и практики применения, такого как в Китае, мы сможем добиться больших высот и быть на шаг впереди при использовании технологий блокчейн на досудебных стадиях уголовного процесса. Это остается лишь делом времени.

Библиографический список

1. Приказ МВД России от 29.12.2012 № 1157 «Об утверждении норм положенности специальной техники для отдельных подразделений центрального аппарата МВД России и средств связи, вычислительной, электронной организационной и специальной техники для территориальных органов МВД России, медицинских (в том числе санаторно-курортных) организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел Российской Федерации» (ред. 30.03.2016). – М., 2012.
2. Антонов, В.П. Криминалистика: учебник / В.П. Антонов, И.И. Белозерова, Л.В. Бертовский [и др.]. – М.: РГ-Пресс, 2018. – 960 с.
3. Бертовский, Л. В. Цифровое судопроизводство: проблемы становления / Л. В. Бертовский // Проблемы применения уголовного и уголовно-процессуального законодательства: сб. мат-лов междунар. науч.-практ. конф. – Симферополь, 2018. – С. 173–178.
4. Бертовкий, Л.В. Перспективы применения технологий «блокчейн» в уголовном судопроизводстве / Л.В. Бертовский, Г.С. Девяткин // Деятельность правоохранительных органов в современных условиях: сб. мат-лов XXIV междунар. науч.-практ. конф. – Иркутск, 2019. – С. 115–118.
5. Девяткин, Г.С. Способы фиксации хода и результатов осмотра места происшествия при раскрытии и расследовании преступлений, совершенных с применением информационных компьютерных технологий / Г.С. Девяткин, П.В. Малышкин, Н.Г. Балашкин // Трансформация социальных систем: проблемы и поиски путей решения: сб. науч. тр. по мат-лам всерос. науч.-практ. конф. (с междунар. участием). – Саранск, 2017. – С. 477–482.
6. Карлин, С. Математические методы в теории игр, программировании и экономике: пер. с англ. / С. Карлин. – М.: Мир, 1964.
7. Курбатова, С.М. Некоторые аспекты информационной безопасности личности в контексте права на свободу и «не насилие» / С.М. Курбатова // Критика насилия: PRO RT CONTRA: мат-лы регион. науч. конф. – Красноярск, 2019. – С. 63–66.

8. Новиков, В.К. Информационное оружие – оружие современных и будущих войн: монография / В.К. Новиков. – М.: Горячая линия – Телеком, 2014;

9. Трашкова, С.М. Некоторые вопросы понимания криминалистической профилактики на современном этапе / С.М. Трашкова // Бизнес. Образование. Право. – 2018. – № 2 (43). – С. 308–312.

10. Трашкова, С.М. Некоторые теоретико-правовые аспекты по использованию информационных технологий в образовании / С.М. Трашкова // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. науч.-практ. конф. / отв. за вып. В.Л. Бопп. – Красноярск, 2016. – С. 82–84.

11. Трашкова, С.М. Основы правового регулирования использования информационных технологий в образовании / С.М. Трашкова // Инновационные тенденции развития российской науки: мат-лы IX междунар. науч.-практ. конф. / отв. за вып. В.Л. Бопп. – Красноярск, 2016. – С. 27–30.

12. Щедрин, Д.Н. Проблемы собирания и использования цифровых доказательств в уголовном судопроизводстве / Д.Н. Щедрин, С.М. Курбатова // Актуальные проблемы уголовного права, уголовного процесса и криминалистики: сб. науч. тр. / под ред. В.Д. Зеленского. – Краснодар, 2019. – С. 196–200.

13. Уголовно-процессуальное право / под ред. Л.В. Бертовского, В.Н. Махова. – М.: Проспект, 2020. – 656 с.

14. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain).

УДК 316:004

CYBERSOCIALIZATION OR MIXED SPACE LIFE

Aisner Larisa Yurievna
candidate of cultural studies, Associate Professor
Naumov Oleg Dmitrievich
candidate of philosophy, Senior Lecturer
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The end of XX and beginning of XXI century accelerated the pace of modern life by means of Informatization, computerization and internetization of all fields of science, education and production. The article aims to analyze the period which is characterized by the fact that information and computer database is the main and most important product. The article argues that the processes of storing, processing and transmitting information, creating, updating, and protection of computer databases, etc. become the leading types of human activity.

Keywords: *information, Informatization, information and communication technologies, socialization, cyberspace.*

КИБЕРСОЦИАЛИЗАЦИЯ ЧЕЛОВЕКА ИЛИ ЖИЗНЬ В СМЕШАННОМ ПРОСТРАНСТВЕ

Айснер Лариса Юрьевна
кандидат культурологии, доцент
Наумов Олег Дмитриевич
кандидат философский наук, ст. преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

Конец XX и начало XXI века дало старт ускорению темпа жизни современного человека на рубеже, вызванные, в частности, во всем мире наращивающимися оборотами процессов информатизации, компьютеризации и интернетизации всех областей науки, образования и производства характеризуются тем, что основным и наиболее значимым продуктом становится информация и компьютерные базы данных, а ведущими видами деятельности современного человека становятся процессы хранения, обработки и передачи информации, создания, обновления и защиты компьютерных баз данных и т. п.

Ключевые слова: *информация, информатизация, информационно-коммуникационные технологии, социализация, киберпространство*

The socio-cultural and economic transformations taking place in modern world influence various spheres of personal life. In this regard, the problems of human socialization have acquired an increasing importance [3].

Obviously, socialization is a multi-faceted process, during which an individual is introduced to "universal social" and constantly discovering and asserting oneself as a subject of social world culture. The world in which we live in today is being transformed and changing. As a result, the factors of human socialization change.

With the development of computer technology, especially due to the dynamic cyberevolution of global Internet, modern person as Homo Sapiens at the turn of XX-XXI centuries turns, in fact, into a unique new species – "Homo Cyberus" (person cybersolidaires). Consequently, psychological and pedagogical sciences have been enriched by the emergence of innovative social and pedagogical phenomenon – a process of cybersocialization of the person [10].

Socialization in cyberspace is particularly evident in the younger generations – children, adolescents and young people – cybersocialization in general, media socialization and Internet socialization, in particular.

Modern youth, who are active users of social networks and other Internet resources, have a different way of organizing their life activities, developing intellectual and cognitive abilities. They contact the outside world and their environment in a different way, in different social and temporal network dimension. The matter is not only in skills of modern information and communication technologies and computer technology; it is about changes in the fundamental spiritual and cultural structures, conceptual basis and diverse views, the whole worldview [1, 2, 4].

The need to develop a personality in cyberspace and the need to organize life activities in the Internet environment is becoming more relevant and real every day, being almost an obligatory criterion of socialization and, directly, cybersocialization of the individual in modern society. A person of the XXI century, almost regardless of age, who has embarked on the path of cybersocialization, has to be a registered user of at least one social network, has to have a personal website and operate a blog. E-mail and cell (mobile) phone are just necessary conditions for the success of a modern person.

In the world "global web", which took a key position in the XXI century in the continuum of cyberspace – the new human living space – one can observe a whole "galaxy" of services and resources that have become a real polygon of social education of a modern person in the context of cybersocialization [11].

Based on the above, one can easily see that human cybersocialization, on the one hand, is a relatively innovative phenomenon, on the other hand, has long been the actual reality of our world, an integral part of the socialization of a modern individual, as well as the engine of scientific, technical, economic and social progress of human society in general. Speaking about Internet socialization, it is necessary to emphasize that the Internet environment itself has become a new level of social network (and popular, the fact which is proved by the permanent growth in the number of users) interaction of modern people of almost all ages, from children to the elderly, in the process of their cybersocialization [8].

In the new millennium, modern information and communication, computer and digital technologies offer tremendous opportunities to reduce the gap between the level of socio-economic development of different countries. Modern technologies al-

low for better exchange of knowledge and experience, and they can enhance the dialogue between cultures [9]. Bridging the digital divide between developed and developing countries should be a major strategic challenge for many international educational organizations, especially the United Nations educational, scientific and cultural organizations (UNESCO).

In the twenty-first century, there is every reason to believe that the efforts of UNESCO and other international organizations will jointly provide the necessary conditions for the sustainable development of the world information society. UNESCO is actively pursuing the policy to strengthen the capacity of nations through:

- expanding access to useful information;
- improving the professional skills of people who are involved in the process of education;
- encourage research and exchange of scientific knowledge through the development of network structures, communication tools [7] and information systems.

Thus, we believe that today's experts in the fields of social, psychological and pedagogical sciences naturally face the prospect of creating a cyberontological concept of personal development and life activity of a modern person.

The cyberontological concept of personal development and life activity of a modern person is designed to justify the potential of using socializing, training and educational opportunities of ICT [6], computer, Internet and digital technologies, based on socio-cultural, psycho-age, gender, ethno-confessional, personal and individual characteristics of a person.

Educators and psychologists need to know and take into account the fact that the generation of humanity at the turn of the XX-XXI centuries – the generation of cybersocialization – the generation of "Homo Cyberus" who grew up in close contact with computer and media technologies, cell (mobile) communication – differs in their worldview, structure of self-consciousness and motivational sphere in social, psychological, spiritual and moral terms [5].

Библиографический список

1. Aisner L.Yu. "Smart" education system for digital society // Проблемы современной аграрной науки: мат-лы междунар. заоч. науч. конф. – Красноярск, 2019. – С. 368–371.
2. Айснер Л.Ю. Развитие цифровой грамотности как условие формирования современной цифровой образовательной среды / Л.Ю. Айснер, С.М. Курбатова // Приоритетные векторы развития промышленности и сельского хозяйства: мат-лы II Междунар. науч.-практ. конф. – Макеевка, 2019. – С. 12–17.
3. Айснер, Л.Ю. Генеалогия личностно-социального со-бытия человека: экзистенциальный аспект / Л.Ю. Айснер, О.Д., Наумов, М.Э. Червяков // Контекст и рефлексия: философия о мире и человеке. – 2019. – Т. 8. – № 4-1. – С. 11–19.

4. Бершадская, С.В. Особенности реализации технологического подхода в образовании / С.В. Бершадская // Наука и образование: опыт, проблемы, перспективы развития: мат-лы междунар. науч.-практ. конф. – Красноярск, 2019. – С. 254–256.

5. Bershadskaya, S.V. Supportive social networks as driving force of educational performance // В сборнике: Проблемы современной аграрной науки. Материалы международной научной конференции. Красноярск, 2018. – С. 238-240.

6. Bershadskaya S.V., Aysner L.Yu. ICT as a tool to develop students' communicative competence in a foreign language // В сборнике: Проблемы современной аграрной науки. Материалы международной заочной научной конференции. Красноярск, 2016. – С. 162-165.

7. Bershadskaya S.V., Aisner L.Yu. Individual barriers to cross-cultural communication // В сборнике статей VI международной научной конференции: Концепт и культура: диалоговое пространство культуры. Языковая личность. Текст. Дискурс. 2016. – С. 114-116.

8. Brand M. Integrating psychological and neurobiological considerations regarding the development and maintenance of specific internet-use disorders: An interaction of person-affect-cognition-execution (i‑pace) model // Neuroscience & Biobehavioral Reviews. 2016. Vol. 71. P. 252-266.

9. Курбатова, С.М. Экосистема образования как фактор цифровизации российской экономики / С.М. Курбатова, Л.Ю. Айснер // Международный научный мультидисциплинарный журнал: The Scientific Heritage. – Будапешт, Венгрия. – 2020. – № 43-5 (43). – С. 3-4.

10. Плешаков, В.А. Киберсоциализация человека: от Homo Sapiens’а до Homo Cyberus’а: монография / В.А. Плешаков. – М.:Прометей, 2012.

11. Хазиева, Н.О. Виртуальная реальность как пространство социализации (социально-философский анализ проблемы): автореф. дис. … канд. психол. наук / Н.О. Хазиева. – Казань, 2014. – 19 с.

УДК 378.147:004

USING THE MULTIMEDIA TECHNOLOGIES IN TEACHING UNIVERSITY STUDENTS A FOREIGN LANGUAGE

Agapova Tamara Vadimovna
PhD in Culturology, Associate Professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

In the context of the transition of educational institutions to the Federal state educational / professional standards of the (new) generation, the content and nature of the teacher's professional activity have changed significantly. The article presents interactive methods of teaching a foreign language using multimedia technologies. The possibilities and practical significance of these methods in the system of higher professional education are considered.

Keywords: *higher professional education, interactive teaching methods, multimedia technologies, foreign language.*

ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИЙНЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ ИНОСТРАННОМУ ЯЗЫКУ СТУДЕНТОВ ВУЗА

Агапова Тамара Вадимовна
кандидат культурологии, доцент
Красноярский государственный аграрный университет

В условиях перехода образовательных учреждений на Федеральные государственные образовательные / профессиональные стандарты (нового) поколения существенно меняются содержание и характер профессиональной деятельности преподавателя. В статье представлен обзор интерактивных методов обучения иностранному языку с использованием мультимедийных технологий. Рассматриваются возможности и практическое значение данных методов в системе высшего профессионального образования.

Ключевые слова: *высшее профессиональное образование, интерактивные методы обучения, мультимедийные технологии, иностранный язык.*

At present, when the need for knowledge of foreign languages is realized by many groups of society, modern communicative-oriented education prepares students for using a foreign language in real life, for cultural, professional and personal communication with representatives of other social systems.

In this regard, the question of finding new, more effective methods, methods and techniques of teaching foreign cultures to keep students interested in studying a foreign language is especially relevant.

Modern methodological innovations are connected with the use of interactive teaching methods. The essence of interactive teaching is that all students are involved

in this process, they have the opportunity to understand and reflect on what they know and think. Many interactive teaching methods are related to multimedia technologies.

Multimedia technologies involve the use of audio visual and interactive teaching tools such as [5], [1]:

1) software (multimedia boards, presentations, video and audio materials, Internet resources);

2) equipment (PC, audio, video equipment, projector, interactive whiteboard).

Modern information and communication technologies provide a whole range of tools for teaching foreign languages: multimedia training programs ("Oxford platinum", "English platinum"), dictionaries (http://spravki.net/), electronic versions of foreign newspapers and magazines (http://www.onlinenewspapers.com/) and so on. Access to computer technologies and telecommunications, as well as their proper use, is the key to success in the information society. It is very efficient for students to perform independent creative or project work using computer programs and Internet resources.

The system of testing as a method of final or intermediate verification is developed now. Students are offered to be tested, for example, on the Moodle platform. There is a computer processing, when they can see their results and, if necessary, work on some material again [2].

Today, the most universal technical training tool is interactive whiteboards. The lesson material clearly emerges on the screen of the interactive whiteboard and target students to active work. Pre-prepared thematic texts in a foreign language, teaching and verification exercises, colorful pictures, audio and video materials help to introduce or activate the lesson material, repeat or consolidate the lexical units and the grammatical structure of the language, for control and self-control of knowledge. The interactive whiteboard allows you to work without using a keyboard, mouse and computer monitor. All necessary actions can be done directly on the screen with a special marker or even a finger.

There is some special software for interactive whiteboards. It allows you to create records that can include various types of information (texts, videos, diagrams, tables, figures). The software has the following features:

1) When explaining grammatical material, the use of multi-colored pencils helps to highlight the main thing, to focus on the use of the desired form.

2) On the screen you can show the train of your thought, fix the order of work and, if necessary, return to the beginning of the presentation.

3) The "drag and drop" function helps to move pictures and words when performing tasks such as: "make up sentences", "correlate".

4) On one slide, you can place a few elements of the lesson and follow the train of your thought.

A variety of styles, communication, and teaching in the lesson, the use of multimedia interactive technologies - all this enriches the content of the lesson, speeds it up, increases interest in learning a foreign language.

Those, who decide to work with interactive technologies, need to remember some of the rules for organizing interactive teaching [4]:

1) All participants of the educational process should be involved in the work.

2) It is necessary to take care of the psychological preparation of the participants. Not everyone who came to the lesson is psychologically ready to be involved in certain types of the work [3]. They can be embarrassed and shy. In this regard, warm-ups, constant encouragement of students for active participation in the work are useful.

3) There should be not many participants.

4) It is necessary to divide all of them into groups.

Interactive teaching can solve some educational problems. It develops communication skills, helps to establish contacts between students, teach teamwork.

The use and implementation of modern technologies and multimedia equipment enrich the content of the educational process, increase the motivation to learn a foreign language.

References

1. Анисимова, Н.С. Мультимедиа-технологии в образовании: понятия, методы, средства: монография / Н.С. Анисимова; под ред. Е.А. Бордовского. – СПб.: Изд-во РЕПУ, 2002. – 89 с.
2. Воронов, М.В., Мультимедийные технологии и дистанционное обучение / М.В. Воронов, В.И. Пименов // Университетское управление. – 2000. – № 1 (12). – С. 67-69.
3. Психолого-педагогическое сопровождение реализации инновационных образовательных программ / под ред. Ю.П. Зинченко, И.А. Володарской. – М.: Изд-во МГУ, 2007. – 120 с.
4. Ступина, С.Б. Технологии интерактивного обучения в высшей школе. / С.Б. Ступина. – Саратов: Издательский центр «Наука», 2009. – 52 с.
5. Цветков, В.Я. Управление потоками мультимедиа в образовательном процессе / В.Я. Цветков, А.Е. Тюрин // Информатизация образования и науки. – 2014. – № 1. – С. 170–178.

УДК 343

THE IMPORTANCE OF THE RESEARCH OF PERSONALITY OF THE CRIMINAL IN FORENSIC SCIENCE

Ashimova Elnara Ashimovna
candidate of legal sciences, associate professor
L.N. Gumilov Eurasian National University, Nur-Sultan, Kazakhstan

The article considers a number of aspects related to the study of the identity of the offender. Attention is drawn to a number of issues of relevance to this topic. Some recommendations are made for this kind of research.

***Keywords**: personality, forensics, science, forensics, personality traits.*

ВАЖНОСТЬ ИССЛЕДОВАНИЯ ЛИЧНОСТИ ПРЕСТУПНИКА В СУДЕБНОЙ НАУКЕ

Ашимова Эльнара Ашимовна
кандидат юридических наук, доцент
Евразийский национальный университет им. Гумилова, Нур-Султан, Казахстан

В статье рассмотрен ряд аспектов, связанных с исследованием личности преступника. Обращено внимание на ряд вопросов, имеющих значение для этой темы. Сделаны некоторые рекомендации для данного рода исследований.

***Ключевые слова**: личность, преступник, наука, криминалистика, свойства личности.*

The criminal identity in forensic science is considered as an element of the criminalistic characteristics of the crime. Such criminologists as R.S.Belkin, A.N. Kolesnichenko, S. I. Konovalov, V. G. Tanasevich, V. A. Obraztsov, N. A. Selivanov, N. P. Yablokov, A. G. Filippov, I.A. Vozgrin, V.K. Gavlo, G.G. Zuykov, V.I. Shikanov, I.M. Luzgin and many others devoted their research to the problems of the essence and content of the criminalistic characteristics of the crime.

Nowadays, scientists often mean the ideal informational model of a crime, where the leading role is given to information as a source for obtaining forensic informationwhen speaking about the forensic characterization of a crime.

The research of the problem of the information approach in forensic science should be supplemented by the semantic aspect of information. The necessity for a semantic approach in the analysis of forensic information is associated primarily with he human factor.

In the process of substantiation in a criminal case, it is important to consider:

1. Socio-demographic characteristics of the defendant's personality (place of residence, nationality, income level, social status, status, education, marital status, relationships in the family and work collective).

2. Psychophysiological characteristics of the personality of the accused person (emotional state, characteristics of the character, motivational sphere, somatic diseases, heredity).

3. Materials characterizing a person in everyday life and at work [1].

There is a problem of classification of the identity of the offender and the features of the identity of the violent offender.

Human personality is one of the most difficult problems of philosophy, anthropology, psychology and other sciences of the humanitarian direction. The problem of the personality must be considered through the prism of its internal structure, organization and functioning of its mental processes. A person's personality can be represented as a system, the elements of which are divided into bodily, mental and attributive properties.

When we talk about the identity of the offender, as an element of the criminalistics characteristics of the crime, we mean a stable forensically significant set of psychophysiological properties and qualities, motivational attitudes, emotional and rational spheres of human consciousness, reflected in the traces of a crime in the process of preparing, committing and hiding the traces of a crime, as well as its post-criminal behavior [2].

There are such types of personality such as the personality of the recidivist, the personality of the minor, etc. in forensic science. A special category includes the type of criminals who have committed violent crimes.

There is the most significant classification of violent criminals: by the method of committing a crime, the mechanism of criminal activity, the motive for the crime, based on the relationship of the criminal with the victim.

There is an ongoing debate about which factors are key to evolution, patterns and acts of violence: heredity, psychopathological or socio-psychological, cultural factors. However, whatever the balance between them, ultimately, violence manifests itself in a social context.

Violence manifests itself in a social aspect, while aggression is an internal psychological state of an individual. Along with other factors, the emergence of aggression is facilitated by the constant growth of conflicts in modern society, which, in turn, causes the transfer of aggression, in particular, to inanimate objects, animals, random passers-by.

According to the research of N.N.Demidov, violent actions are accompanied by verbal aggression in 58.1% of cases against a background of a pronounced interpersonal conflict, while 17.2% of violent criminals are prone to commit aggressive acts. These actions are expressed in inflicting cuts on oneself, attempting suicide, and committing other actions destructively aimed at causing harm to one's body [3].

Violent crimes are based on personal motives (revenge on the basis of personal hostility; on the basis of jealousy; hatred, bitterness, self-affirmation, resolution of internal conflicts)as a rule. The role of personality factors is often decisive in decision making in the competition of motives. The goal of a violent crime is primarily the desire to resolve personal conflicts and remove obstacles to meeting current or potential needs.

These features of the mechanism of violent crimes indicate that the motivation stage is the most important for this category of crimes. The phenomenon of the unconscious is currently not fully understood. Unconscious mental processes, giving rise to heated debate, were the subject of research by representatives of various philosophical and psychological schools, various directions of scientific thought. This problem was the focus of G.V. Leibniz, I. Kant, G. Hegel, A. Schopenhauer, 3. Freud, E. From, C. Jung, J. Lacan, I. M. Sechenova, I.P. Pavlova and many other sci-

entists. The offender may be completely unaware of the true motives of his behaviour due to the action of protective psychological mechanisms (crowding out, substitution, rationalization), which squeeze out from the consciousness undesirable information about the true motives if it is painful, traumatic for the subject. In the consciousness of a person, rational foundations of his behaviour are often developed, actions are given a noble meaning.

There is an internal tension associated with the acute experience of guilt in psychological research of criminals who have committed serious violent crimes. This personality factor is pronounced in 68% of individuals. This circumstance can be explained from the standpoint of classical psychoanalysis as an internal conflict between the "Super Self" and the "Ego".

The general psychological characteristics of violent criminals include increased emotional instability (25.3%), emotional stress (30.2%), the need for self-esteem (26.9%), primitive personality (35.7%), low intelligence (39.2%), while the main logical operations are developed (75.4%), resentment (27.4%), protest reactions (24.6%) irritability (33.7%), high motivation to achieve the goal (22.6%), a tendency to respond directly to an irritation reaction (25.6%), authoritarianism (29.7%), egocentrism (33.1%), demonstrativeness (26.2%), the desire to make oneself better (32.1%), social activity (33.1%), independence of behavior (29.9%), a tendency to outward accusation (32.9%), high self-esteem (27.9) [4].

The relationship of the identity of the criminal with other elements of the forensic characteristics is traced. This relationship of the elements of the forensic characteristics is a correlation (probabilistic-statistical).

The most adequate and significant dependence is revealed on the basis of the analysis of the elements of the criminalistic characteristics of a certain type of crime, for example, violent crime.

A special group of properties that determine the way a criminal is acting (his behavior) is made up of special abilities, skills and habits. Forensic significant and determining when choosing a method of committing and concealing a crime are the general properties of a person: character traits and abilities, as well as mental deviations [5].

The concepts of the method of committing a crime and the method of criminal behavior can be distinguished on a teleological basis. Only those actions that are aimed at preparing, committing and concealing a crime can be considered as a way of committing a crime.

An analysis of the practice of investigating violent crimes indicates that the most common methods of committing a crime are: striking the entire body with arms, legs, and hard blunt objects (46, 3%), wounding with sharp-cutting objects (44.3%), strangulation (5.2%), the use of firearms (4.2%) [6].

It was also established that the methods of concealing a crime and opposing an investigation vary in certain categories of cases.

Speaking of trace information as an element of the forensic characteristics, it is necessary to note its connecting role for all other elements of the forensic characteristics. Trace information is present in all elements of the forensic characteristics as a necessary means (information signal) to display reality, through which we learn such a complex phenomenon as a crime.

Thus, relying on the existence of a macrostructure common to external and internal activities, we can talk about the individual's ability to leave his "imprint" at the scene in the material environment in the form of a "complex personality-regulatory trace". This "trace" is no less suitable for identifying the identity of the offender than the trace of his finger.

It seems important the relationship of the identity of the offender with the situation of the crime. The content of information on the situation in which the crime was committed can vary dynamically depending on the specific crime.

According to statistics, 76.2% of crimes against the person are committed on household grounds against relatives and close friends, 34.9% of them are in the victim's apartment (house), usually in the evening and late evening hours (17-22 hours) - 47, 7%. A certain relationship is most often traced between the criminal and the victim, as a result of which the criminals usually do not randomly select individuals as objects of their criminal assault. Therefore, the identification of the offender is often carried out according to the scheme "victim - suspect - accused" [7].

50% of criminals who committed violent crimes were previously familiar with the victim, 26.2% of criminals were relatives of the victims, and only 22.2% of criminals were not familiar with the victim. It is important that 33.7% of violent crimes were committed in the conditions of provocation by the victim. These provocative actions resulted in attempts by the victim to commit crimes, physical aggression against the offender, pronounced verbal aggression, immoral behavior, behavior that did not meet the standards accepted in the social group, etc. [8].

There are two areas in the criminalistic study of the identity of the criminal: the study of an unknown criminal by material traces at the scene of the incident, based on the identification of the relationship between the criminal and the victim, and the study of the detained suspect, accused.

The general requirements for all forensic methods of personality research should be defined. The methods that can be used to investigate the accused must be primarily scientific and legal. The ethical side of such studies is also important.

Special (particularly scientific) methods are used to cognize and study individual phenomena, events, and facts. In this regard, modelling as a forensic method is also used to search for an unidentified person who has committed a crime. A probabilistic psychological portrait of an unidentified criminal means a combination of forensically significant information about his personality traits, socio-demographic data about him, his characteristic behavioural characteristics. The process of compiling a likely psychological portrait of an unidentified criminal is called forensic profiling.

The purpose of using the techniques of forensic profiling is to determine the strategy of the preliminary investigation.

The process of forensic profiling is defined as a technique for identifying the unique and typical psychophysiological characteristics of the person who committed the crime in conditions of non-obviousness.

The methodology of forensic profiling basically uses the already accumulated personal information about persons who have committed various types of crimes.

One of the main objects of research in compiling a psychological portrait is the "handwriting" (autograph) of the offender. It is important to study the learned behavior: how the criminal acts to commit a crime; it manifests itself in dynamics and can

change. An autograph is how a criminal acts in order to realize himself in a criminal act, that is, to achieve the necessary goal in criminal behavior [9].

The methodology for compiling and using a probabilistic psychological portrait of an unidentified criminal in the investigation process includes the following steps: obtaining and analyzing the initial trace information from the scene, analyzing the relationship of the elements of the criminalistic characteristics of a crime of this type; reconstruction of a crime event; forensic profiling and putting forward a search version; development of recommendations on the identification and search of the offender, as well as the forensic forecast of post-criminal behavior of the offender.

When compiling a probabilistic psychological portrait of an unidentified criminal, special methods of cognition are used, in particular, forensic psychiatric and forensic psychological methods.

Based on the analysis of the results of studying acts of a comprehensive forensic psychological and psychiatric examination, specialists compiled an average probabilistic psychological portrait of a violent criminal. Often used methods of qualitative and quantitative analysis (content analysis) of documents.

The motivational sphere of criminals is characterized by the following features: in 44.2% of cases, a sudden intention is revealed, which characterizes the actions of this category of persons as disorganized. A selfish motive was detected in 12.2% of cases; revenge - in 16.9%; jealousy - in 2.9%; personal hostility - in 21.5%; hooligan - in 16.3%; sexual - in 9.9%; desire to hide another crime - in 2.3%; self-defense - in 13.5%; indefinite motive - in 5.8% [9].

Correlation dependencies between the age of the offender, the method and nature of the crime committed, the localization of bodily harm, the motives of criminal acts and social relationships with the victim of the crime are established.

There are features of the nomination of versions of the identity of the criminal in a situation of non-obviousness of the crime.

Speaking about the correlation of the concepts of the investigative version and the forensic model, it should be noted that in science there is no consensus on whether these concepts are identical. However, it should be noted that a specific feature plays a special role in determining the content of the version and the direction of the investigation. The most important for the identification and search of an unknown criminal are the search signs of the criminal: - 1. The method of committing a violent crime; - 2. The nature of the actions of the offender (organized, disorganized); - 3. The sex of the offender; - 4. The age of the offender; - 5. Education of the offender; - 6. The scope of the offender; - 7. The presence or absence of a criminal record; - 8. Information about the relationship with the victim before committing the crime.

In the investigation of any crime, an initial investigative situation arises, which develops mainly as a result of the initial investigative actions, often only when examining the scene of the incident. Three types of such situations can be distinguished: a) there is no (or incomplete) information about the offender; b) there is incomplete information about the crime event; c) there is incomplete data on the crime event and the offender. One of the typical investigative situations at the initial stage of the investigation is the initial investigative situation: the detection of a crime committed in conditions of non-obviousness. According to statistics, in 68.2% of cases, crimes were committed in conditions of non-obviousness. That is, at the initial stage of the

investigation, at the stage of initiating a criminal case, the person who committed this crime was not established.

Based on the forensic characteristics of the crimes in question, in the absence or deficit of information about the identity of the offender, work to establish it should be based on the use of a system of source models.

It should be noted that often at the initial stage of the investigation of crimes committed in conditions of non-obviousness, the only source of forensic information is an examination of the scene of the incident. In this regard, the examination of the scene of the incident and traces found at the scene of the incident should be considered as sources of information on the physical, psychological, social and personality traits of the criminal.

Therefore, we can talk about an ideal reconstruction of the crime event, which should be understood as the mental restoration of events at the time the crime was committed. During this reconstruction, the careful and competent study of material traces at the crime scene becomes important.

In the process of studying material traces found at the scene, the person conducting the investigation faces the complex problem of analyzing the traces and identifying their significance for investigating the crime and identifying the offender. This work can be defined as the forensic diagnosis of material traces of a crime.

To identify the offender and solve other tasks of the investigation, it is important to clarify and use in the process of putting forward investigative versions and checking data that characterize the situation directly at the scene of the incident: climatic conditions at the time the crime was committed, time of day, degree of illumination of the area, remoteness from settlements, roads, landscape features and other circumstances.

There is always a certain relationship between the behavior of the criminal and the victim. Investigation of the identity of the victim and his actions immediately before the crime is a necessary part of the investigation since the victim's behavior in some cases is provocative, provocative, or frivolously careless.

The issues of predicting the behavior of a criminal in order to find him are important. Forensic forecasting is the activity of the investigator (or other persons conducting the investigation) aimed at obtaining and analyzing forensic information on a criminal case in order to model the behavior of an unidentified criminal in the future.

Prediction of criminal behavior is possible in the context of modelling his lifestyle. Thus, the forensic forecast of the alleged behavior of a person is compiled after he commits a crime. The behavior of an unidentified offender is seen as an information model.

The information model of the behavior of a criminal after committing a crime includes information that contains data:

– about a person committing a second crime (relapse);

– about whether the offender escaped from the scene and in what direction he left;

– the presence of the criminal (with himself, in his home or other places) of the crime, personal belongings of the victims;

– the alleged opposition to the investigation by the offender or other interested parties.

Modelling the behavior of violent criminals after their detention, during the production of urgent investigative actions, the psychological characteristics of this category of persons should be taken into account.

Specialists note the following characteristic personal features of this category of persons: a clear tendency to external accusation (accusation of the current circumstances or those surrounding their failures) was detected in 39.2% of the criminals; 32.1% had the desire to put themselves in the best light, while 53.1% did not repent of the crime and positively assessed their actions. For comparison, only 22.1% of criminals formally repented of the crime.

It should be noted such a psychological feature as a pathological tendency to lie, which was diagnosed in 15.7% of criminals. Criminals of this category rarely repent of a crime, usually at the initial stage they don't give true evidence, they are inclined to oppose the investigation, they don't immediately contact the investigation, which can adversely affect the entire course of the investigation.

On the other hand, one should pay attention to such psychological characteristics of the group as excessive self-esteem detected in one-third of the examined persons (27.1%). At the same time, this category of persons showed a decrease in critical abilities (14.6%), and mainly in men. The need for approval was identified in 19.5% of criminals [10].

Consequently, the identity of the offender has significant specifics, which must be taken into account in the work of collecting and researching information about the crime.

References

1. Criminology: Textbook / Ed. V. D. Malkova. M .: CJSC Justicinform, 2006.
2. Criminology: Textbook for universities / Under total. ed. A. I. Dolgovoy. M .: NORMA Publishing House, 2001. S. 335.
3. Demidov N.N. The study of the identity of the criminal in the investigation process, Author. diss ... cand. legal Sciences, Volgograd 2003, p.15.
4. Simakova E.S. Reflection in the handwriting of psychological properties and states of personality (forensic, criminal procedural and psychological aspects), Author. diss.cand. legal Sciences, Tomsk, 2003, p.10.
5. Criminology: Textbook / Ed. V.N. Kudryavtseva and V.E. Eminova. M.: Lawyer, 2004.S. 55-56.
6. Criminology: Textbook / Ed. V.N. Kudryavtseva and V.E. Eminova. M., 2005.S. 50-52.
7.Http://web.archive.org/web/20100215152520/http://www.mvd.ru/files/u281KzbmtHplrXo.pdf
8. Criminology: Textbook / Ed. N.F. Kuznetsova, V.V. Luneeva. M., 2004.S. 126.
9. Criminology: Textbook / Ed. V.N. Kudryavtseva and V.E. Eminova. M., 2005.S. 159.
10. Gnatenko E. Problems of studying the identity of the criminal in the domestic criminological science // Sociology in a situation of social negligence. - X .: KhNUimeni V.N. Karazina, 2009 . - S. 177.

УДК 378.1:004

INFORMATION AND COMMUNICATION TECHNOLOGIES IN SOLVING PROBLEMS OF TEACHING FOREIGN LANGUAGE GRAMMAR IN NONLINGUISTIC UNIVERSITIES

Kapsargina Svetlana Anatolyevna
candidate of pedagogical Sciences, associate Professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The article considers the possibilities of using modern information and communication technologies in the process of teaching the grammatical aspect of a foreign language. The use of new information and communication technologies in teaching is one of the most important aspects of improving and optimizing the educational process, it allows activating the cognitive activity of students; providing positive motivation for learning; a high degree of differentiation of learning; improving the control of knowledge, skills and abilities.

Keywords: *student, foreign language, information and communication technologies, grammatical aspect, nonlinguistic university.*

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В РЕШЕНИИ ЗАДАЧ ОБУЧЕНИЯ ИНОЯЗЫЧНОЙ ГРАММАТИКЕ В НЕЯЗЫКОВЫХ ВУЗАХ

Капсаргина Светлана Анатольевна
кандидат педагогических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В статье рассмотрены возможности использования современных информационно-коммуникационных технологий в процессе преподавания грамматического аспекта иностранного языка. Использование новых информационных технологий в преподавании является одним из важнейших аспектов совершенствования и оптимизации учебного процесса, позволяет активизировать познавательную деятельность студентов; обеспечить положительную мотивацию обучения; высокую степень дифференциации обучения; усовершенствовать контроль знаний, умений и навыков.

Ключевые слова: *студент, иностранный язык, информационно-коммуникационные технологии, грамматический аспект, неязыковой вуз.*

Today, it is impossible to imagine the educational process without modern information technologies. With the development of information technologies the process of teaching foreign languages is changing and the need to meet modern requirements and to apply new forms and methods of teaching foreign languages confirm the relevance of the broad introduction of means of informatization of education in the

modern educational process that enhances the didactic possibilities, providing clarity, audio and video support, control, and increases the efficiency of the organization of independent language learning, contributing to improving teaching. Based on practical experience, it can be argued that linguistic information resources have advantages over traditional means of teaching a foreign language, since they contribute to the implementation of an individual approach and increase the independence of students.

The main advantages of using ICT include the intensification and individualization of training, which give a positive result, because they create conditions for the successful activity of each student, causing positive emotions in students, and thus contributes to increasing interest in the subject of students. New information technologies ensure high quality of material delivery by using various communication channels, and help to fill the shortage of sources of educational material. The undoubted advantages of using ICT are also the acceleration of replication and access to the achievements of pedagogical practice, reducing the time of obtaining and assimilation of information without loss of quality, and ensuring the flexibility of the learning process. In addition, the use of computers and digital educational resources in teaching a foreign language helps students overcome the psychological barrier to using a foreign language as a means of communication, develops their communicative, cognitive, creative abilities and information culture [1–3].

Recently, scientific research and publications examining the experience of teachers and methodologists show that the effectiveness of teaching grammar can be significantly improved by introducing new pedagogical technologies, in particular, the use of information and communication technologies.

The use of ICT can be effective at all four main stages of working on grammatical material, highlighted by N. I. GEZ, M. V. Lyakhovitsky, and A. A. Mirolyubov. At the stage of introduction of grammatical material, ICTs have a wide range of tools for presenting grammatical phenomena and creating an indicative basis for the subsequent formation of the skill. ICTs can provide a visual representation of the material being studied.

A significant advantage of using modern technologies in teaching grammar of a foreign language is the ability to generalize grammatical material in tables, diagrams, that can be interactive, which allows you to reduce significantly the amount of text information, favorably affecting the figurative memorization of grammatical material. Information and communication technologies make it possible to diversify the process of getting acquainted with a new grammatical phenomenon. An example of such a task is a text for listening or reading, in which a new grammatical structure is highlighted in color or font [3].

Existing modern computer programs offer a variety of grammar exercises, the main advantage of which is instant verification of correctness of execution, while errors are highlighted in color and sound signal, which significantly improves memorization. If there are difficulties, the student can return to performing certain points in the exercise. Often programs include grammatical reference books. Thanks to hyperlink technology, you can move from a specific topic in the reference book to the corresponding exercise and vice versa.

The use of ICT in a grammar lesson is possible when studying any topic and at any stage of working on grammatical material. With the correct location, successful color design, use of diagrams and tables, and voice guidance, the rules will be perceived easier and faster by students. Moreover, using new information technologies, it is possible to control the level of formation of grammatical skills in an interesting way on the basis of test programs and a system for detecting grammatical errors at the morphological and syntactic levels.

Research in recent years has highlighted the great potential of modern technologies for more effective organization of student learning, including the use of various electronic educational platforms, such as LMS Moodle. The teacher can also use this platform to work on grammatical material, since the platform has an extensive toolkit and actively use such elements of the course as a forum, glossary, page, lecture, test, and crossword.

Teachers of the Department of foreign language of Krasnoyarsk State Agrarian University widely use the tool "Lecture" of the electronic system, both during the classroom work of students and for the organization of independent work and homework. Element of the system "Lecture" is used to organize independent work of students on new theoretical material, such as grammar. The use of this tool gives a positive result in the work of students in the assimilation of grammatical material. As example, lectures on grammatical topics such as "Article", "Present Simple", "Past Simple", etc. Thanks to the settings set by the teacher of the lecture, students have the opportunity at their own pace (the time of the lecture and the number of attempts are unlimited) step by step to pass and learn new material. In order to increase active interaction and control the understanding of the studied material, the teacher uses different questions and tasks at the end of each section (page) of the lecture. It is impossible to continue studying the topic without understanding the material read and checking the quality of the knowledge gained. Depending on the answer chosen by the student and the strategy developed by the teacher, students, correctly answering the questions, go to the next page or in case of an incorrect answer return to the previous page, having the opportunity to read the theoretical material again and reanswer the control questions [4–11].

Different combinations of course elements are possible to achieve certain tasks. In addition, it is important to note the fact that the content of the course, editing its content is carried out by the authors in any order and can easily be carried out directly in the learning process.

Thus, the use of ICT in teaching a foreign language significantly increases the effectiveness of teaching students grammar in non-linguistic universities, since the resources of these technologies are quite diverse. Learning becomes person-oriented due to the variability and flexibility of learning the course material based on individual pace. In addition, ICTs allow for high-quality continuous monitoring of material assimilation. Monitoring of results is available not only to the teacher, but also to the student himself, which contributes to the implementation of the technology of self-assessment of individual achievements.

References

1. Тимофеева, Е. В. Использование информационно-коммуникационных технологий при обучении иностранному языку / Е.В. Тимофеева, Ю. А. Кайль // Известия АлтГУ. – 2014. – № 2 (82). – URL: https://cyberleninka.ru (дата обращения: 25.02.2020).

2. Брезгина, О. В. Об использовании информационно-коммуникационных технологий при обучении иностранному языку / О. В. Брезгина // Вестник НВГУ. – 2014. – № 4. – URL: https://cyberleninka.ru (дата обращения: 26.02.2020).

3. Шаранов, К. Е. Способы преподавания аспектов немецкой грамматики при помощи современных информационно- коммуникационных технологий / К. Е. Шаранов // Преподаватель XXI век. – 2012. – № 2. – URL: https://cyberleninka.ru (дата обращения: 27.02.2020).

4. Kapsargina, S.A. The use of LMS Moodle to intensify the independent work of students in teaching a foreign language in a non-linguistic university / S.A. Kapsargina // Азимут научных исследований: педагогика и психология. – 2018. – Т. 7, № 4 (25). – С. 120–123.

5. Khudoley, N.V. New use of MOODLE tools for distance English language learning (experience of Krasnoyarsk state agrarian university) / N. V. Khudoley, J. A. Olentsova // 18th International Multidisciplinary Scientific GeoConference SGEM 2018, www.sgem.org, SGEM2018 Conference Proceedings, ISBN 78-619-7408-49-2 / ISSN 1314-2704, 2 July - 8 July, 2018, Vol. 18, Issue 5.4, 225–232 pp.

6. Khramtsova, T.G. The role o f information technologies in modern educational institutions / T.G. Khramtsova, Yu.A. Olentsova // Образование: традиции и инновации: мат-лы XIV международ. науч.-практ. конф. – Прага: World Press, 2017. – P. 289–291.

7. Худолей, Н. В. Использование LMS Moodle при обучении иностранному языку в вузе (опыт ФГБОУ ВО «Красноярский ГАУ») / Н. В. Худолей // Вестник РУДН. Серия: Информатизация образования. – 2018. – № 4. – URL: https://cyberleninka.ru (дата обращения: 28.02.2020).

8. Шмелева, Ж. Н. Из опыта внедрения платформы Moodle в преподавании иностранного языка в аграрном вузе / Ж. Н. Шмелева // Успехи современной науки. – 2017. – Т. 1, № 1. – С. 60–62.

9. Shmeleva, Zh. N. The use of modern software on LMS Moodle in teaching listening and speaking in a foreign language at the non-linguistic university / Zh. N. Shmeleva, S. A. Kapsargina // АНИ: педагогика и психология. – 2019. – № 1 (26). – URL: https://cyberleninka.ru (дата обращения: 01.03.2020).

10. Волкова, А. Г. Использование онлайн-словарей как инновационный метод обучения иностранным языкам / А. Г. Волкова // Проблемы современной аграрной науки: материалы международной заочной научной конференции, 15 октября 2016г. – Красноярск: КрасГАУ, 2016. – С. 202–204.

11. Волкова А. Г. Инновации в образовательных технологиях: современные мировые тенденции / А. Г. Волкова // Аллея науки. – 2018. – № 7 (23). – С. 855–859.

УДК 378.1:004

INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE PROCESS OF TEACHING ENGLISH IN NONLINGUISTIC UNIVERSITIES

Kapsargina Svetlana Anatolyevna
candidate of pedagogical Sciences, associate Professor
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The role of information and communication technologies (ICT) in teaching, including foreign languages, is becoming increasingly important. The use of ICT in the educational process makes the learning process more accessible and flexible and the effectiveness of the perception of the material increases with such training.

Keywords: *student, foreign language, educational process, information and communication technologies, nonlinguistic university*

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ОБУЧЕНИИ АНГЛИЙСКОМУ ЯЗЫКУ В НЕЯЗЫКОВЫХ ВУЗАХ

Капсаргина Светлана Анатольевна
кандидат педагогических наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

Роль информационно-коммуникационных технологий (ИКТ) в обучении, в том числе иностранному языку, становится все более значимой. Использование ИКТ в образовательном процессе позволяет сделать процесс обучения более доступным, гибким и эффективность восприятия материала при таком обучении возрастает.

Ключевые слова: *студент, иностранный язык, учебный процесс, информационно-коммуникационные технологии, неязыковой вуз.*

Experience in the agrarian university indicates that the teacher of a foreign language often has to work under the conditions of: a) reduction of contact hours devoted to the study of language and the increase in hours of independent study; b) lack of availability of modern textbooks, special dictionaries, technical means of training; c) low or almost complete lack of learning and cognitive competence of students with weak skills to work with a book, encyclopedia, dictionary, text, including text with a degree in native language; d) low motivation, lack of interest in the subject of students. Despite such difficulties, the teacher must prepare a specialist who is ready for future professional activity in the conditions of modern society. To do this, it is necessary to solve the following tasks: a)to find new ways, techniques and means of teaching a foreign language to fill the shortage of classroom hours; b) to organize the educational process for mastering the foreign language professional vocabulary in

such a way as to compensate for the lack of provision of textbooks, dictionaries; c) to create motivation for students to learn a foreign language.

To solve these tasks, it is advisable to introduce information and communication technologies (ICT) into the educational process.

Information and communication technologies (ICTs) are widely used in all areas of social life, including all levels of education. The use of information and communication technologies in the educational process helps to intensify and individualize learning, increases interest in the subject, and makes it possible to avoid subjective evaluation. Using a computer and digital educational resources to teach English helps students overcome the psychological barrier of using a foreign language as a means of communication[1–2].

The main goals and objectives of ICT are: a significant increase in motivation for language learning (creativity, novelty, autonomy, and competence in solving problems, personal growth, and positive emotional factor), development of language competence, skill development self-study of English; the development of creative abilities of the students.

ICT is both a means of delivering material and a means of controlling it. It provides high-quality material delivery and uses various communication channels (text, audio, graphic, etc.). New technologies allow individualizing the learning process based on the pace and depth of the course. This differentiated approach gives a great positive result, because it creates conditions for the successful activity of each student, causing positive emotions in students and thus affects their educational motivation [3–4].

Information and communication technologies represent a wide range of digital technologies used to create, transmit and distribute information and provide services. The most frequently used elements of ICT in teaching a foreign language are: a multimedia projector, an interactive whiteboard, electronic encyclopedias and reference books, Internet educational resources, video and audio equipment, simulators and testing programs, electronic textbooks and manuals, interactive conferences and competitions, research works and projects and distance learning. If it is possible to use information technology tools in educational activities, the following classification can be derived: for searching for information; for working with texts; for translation of texts using translation programs and electronic dictionaries; for storing and accumulating information; for communication; for processing and reproducing graphics and sound, and for viewing images. These means of ICT training in English classes are an effective pedagogical means of forming communication skills, one of the most important aspects of optimizing the educational process and expanding the range of methodological tools and techniques.

The use of information and communication technologies opens up huge opportunities for effective learning. Computer training programs contribute to the development of various types of speech activity, awareness of language phenomena, creating communicative situations, and automating language and speech acts. Learning to listen involves working on two functional types of speech activity: listening in the process of direct communication and listening to connected texts in conditions of in-

direct communication. Multimedia capabilities allow you to listen to foreign speech, adapting it according to your level of perception, and adjusting the speed of sound allows you to split phrases into separate words, simultaneously comparing the pronunciation and spelling of words. Interactivity leads to more intensive participation in the learning process of the student himself, which helps to increase the efficiency of perception and memorization of educational material. Computer presentations allow teacher to adapt effectively the learning material to the characteristics of students. Interactive learning based on multimedia programs allows you to implement a set of methodological, didactic and psychological tasks, making the learning process more interesting and creative. The ability to take into account the level of language training of students is the basis for the implementation of the principles of individualization and differentiated approach in teaching. This takes into account the individual work opportunities of each student. Using ICT, you can organize individual, paired and group forms of work in the classroom, present the material more clearly, saving time for speech practice, make classes more visual, provide instant feedback, increase the intensity of the educational process, objectively evaluate the actions of students, teach them to work independently with the material, activate cognitive activity, make the course content non-standard and attractive, ensuring the repetition of previously passed material. Therefore, the use of modern information and communication technologies contributes to effective learning, and as a result, affects the overall development of students [5–8].

Numerous educational and language resources developed specially for foreign language learners are used in teaching foreign languages. Such resources are developed by publishing companies, government organizations whose goal is to promote this language and culture in the world, as well as by communities of interested professionals or amateurs. With all the opportunities of Internet technologies for learning and teaching a foreign language in high school, the greatest value of the Internet as ICT, have as a source of information for studying or teaching a foreign language, the culture of the country of studied language, literature, information, regional geographic and cultural character.

The possibilities of using Internet resources are huge. The global network creates conditions for obtaining any necessary information: country-specific material, news, newspapers and magazines, fiction and scientific literature, etc., in addition to working on reading and speaking skills, you can add vocabulary. To do this, students are invited to make dictionary entries based on the information they have read. Grammatical skills of the English language are acquired through working on examples found in articles. Students can take part in tests, quizzes, competitions, olympiads held on the Internet, etc.in English lessons, using the Internet, you can solve a number of didactic tasks: to form reading skills using the materials of the global network; to improve the writing skills of students; to expand the vocabulary of students; to form motivation to learn English.

Therefore, the use of ICT in the educational process allows you to get access to large amounts of information, organize independent educational work and increase interest in learning a foreign language. However, the introduction of ICT in the edu-

cational process does not exclude traditional ways and methods of training. They are combined with ICT at all stages of the educational process, which significantly increases the effectiveness of training, encourages students to improve themselves and helps them navigate freely in the information space. Thus, communicativecompetenceisformed.

References

1. Лебедева, О.Е. Информационно-коммуникативные технологии в процессе формирования коммуникативной компетенции у студентов неязыковых вузов / О.Е. Лебедева // Заметки ученого: научно-практический журнал. – 2018. – № 4(29). – С. 63–65.

2. Вардашкина, Е. В. Использование информационно-коммуникационных технологий в обучении английскому языку студентов неязыковых вузов // Инновации в науке. – 2011. – № 5-2.

3. Надеждина, Е. Ю., Использование современных информационно-коммуникационных технологий в процессе обучения студентов иностранным языкам в неязыковом вузе / Е.Ю. Надеждина, Е. Н. Шилина // Концепт. – 2018. – №11.

4. Khramtsova,T.G. The role of information technologies in modern educational institutions / T.G. Khramtsova, Yu.A.Olentsova // Образование: традиции и инновации: мат-лы XIVмеждународ. науч.-практ. конф. - Прага: WorldPress, 2017. - P. 289-291.

5. Храмцова, Т.Г. The main techniques in teaching foreign languages / Т.Г. Храмцова // Проблемы современной аграрной науки: мат-лы междунар. заоч. науч. конф. – Красноярск: Красноярский ГАУ, 2017. – С. 265–267.

6. Шмелева, Ж.Н. Из опыта внедрения платформы Moodle в преподавании иностранного языка в аграрном вузе / Ж.Н. Шмелева // Успехи современной науки. – 2017. – Т. 1, № 1. – С. 60–62.

7. ShmelevaZh. N., Kapsargina S. A., The use of modern software on LMS Moodle in teaching listening and speaking in a foreign language at the non-linguistic university // АНИ: педагогикаипсихология. – 2019. – № 1 (26). – С. 147–149.

8. Ambrosenko N. D., Skuratova O. N., Shmeleva Zh. N. Preliminary results of the University participation in the project «Modern digital educational environment» // АНИ: педагогика и психология. – 2019. – №1 (26).

УДК 378.1:004

TO THE ISSUE OF INFORMATION PEDAGOGICAL TECHNOLOGIES USE IN THE HIGHER EDUCATION SYSTEM

Kozulina Natalya Stanislavovna
candidate of agricultural sciences, docent
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The article discusses the experience and the results of applying informational pedagogical technologies in the system of higher education on the example of Krasnoyarsk state agrarian university.

Key words: *information pedagogical technologies, students, higher education, multi-media technologies, e-complex, Moodle platform.*

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ ПЕДАГОГИЧЕСКИХ ТЕХНОЛОГИЙ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Козулина Наталья Станиславовна
кандидат сельскохозяйственных наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В статье рассматривается опыт и результаты применения информационно-педагогических технологий в системе высшего образования на примере Красноярского государственного аграрного университета.

Ключевые слова: *информационно-педагогические технологии, студенты, высшее образование, мультимедийные технологии, электронный комплекс, платформа Moodle.*

Nowadays, there can be observed the transition from an industrial society to an information society. This type of society deploys unprecedented opportunities for human life-long development, more effective solutions of many professional, economic, social issues arising in the everyday life. Complete reform of higher education, caused by joining of Russia to Bologna agreement [2, p. 203–208], [15, p. 306–312] and various state, political and socio-economic transformations, continuous growth in the volume of information have led to transformation of the educational process. The contradiction between the rapid rate of increasing knowledge in the modern world and the limited opportunities for their assimilation by the individual makes modern pedagogy abandon the comprehensive development of the individual and move to the development of human abilities for self-regulation and self-education. Modernization of education will help to overcome the crisis and educate professionals competitive on the modern labor market [16, p. 209–213].

So, it is absolutely indispensable to help the future specialist in the training process in developing own individual education strategy taking into account the motivational sphere of the individual [1, p. 224–225] and the abilities. It is obvious that only those members of society who have the necessary knowledge and skills to navigate the new information space will be able to use all the opportunities in making a career and becoming competitive in the labor market. The issue of providing such educational services that would prepare the young generation for the information future in a timely manner is a matter of principle. With this approach, new information technologies allow to solve a number of fundamentally new didactic tasks, and their application will improve the quality of education. A characteristic feature of modern educational information technologies is the desire to use new technical achievements. In our opinion, it would be more correct to talk about new information technologies in the context of the concepts of new "pedagogical technologies".

This concept has recently become more widely used in the theory of education. It is in this sense that the term "technology" and its variations "learning technology", "educational technologies" have been used in pedagogical literature.

When computers became widely used in education, the term "new information technology for learning" appeared. Generally speaking, any pedagogical technology is an information technology, since the basis of the technological process of training is information and its movement (transformation). Another term for computer-based learning technologies is computer technology. Modernization of education is impossible without the introduction of information and communication pedagogical technologies in the educational process. Krasnoyarsk state agrarian university has been actively introducing these technologies into the educational process [3, p. 274–278], [4, p. 16–19]. The main means of informatization of education are hardware, software and content. The effectiveness of computers and information technologies depends on how they are used. In practice, information technology training refers to all technologies that use special technical information tools (computers, audio [8, p. 147–150], films, video lectures, Moodle platform [10, p. 69–73], etc.).

The goals of computer education are the development of higher mental functions, constructing individual learning path in the framework of student-centered approach [11, p. 365–369], [12, p. 111–126], [14, p. 297–300] and practice-based approach [5, p. 65–75], the formation of highly-educated personality with such qualities as: independence, critical thinking, responsibility, and reflexivity who is able to solve different tasks in his professional activity and every day communication. The computer in modern conditions is not just an electronic computer; it is a source of information, a tool for its transformation, and a universal communication system that provides interaction between all subjects of the didactic system, including those with whom communication is mediated through a computer program. The main task of using computer technologies is to expand the intellectual capabilities of a person. Currently, the very concept of learning is changing: the assimilation of knowledge gives way to the ability to use information, to get it using a computer.

Computer communication as an integrating tool that ensures the implementation of the educational process, creates conditions that allow to use new information

technologies in the learning process, learn how to use the latest technical tools and software products, and acquire skills in modern ways of processing information. Among the technologies that allow to master the educational material and to improve the motivational sphere of the student in the educational process, preference should be given to those that are the main components of the integrated technology of the pedagogical process:

1. Interactive technologies

The structure of an interactive lesson differs from the regular lesson [9, p. 209–211]. It includes the interactive learning technologies, that is, specific techniques and methods that make the lesson unusual and more intense and interesting. Faculty members can conduct lessons using an interactive whiteboard, as well as lessons with Internet access. Working with an interactive whiteboard creates a comfortable learning environment in which all students actively interact with the teacher and with each other. All buildings in Krasnoyarsk SAU are provided with computer classes with a free access to Internet.

2. Information and communication technologies

The use of information technologies in the educational process allows to make classes in different subjects more interesting, dynamic and convincing, and a huge flow of information studied is easily accessible. Modern information technologies provide the teacher with a large reserve of technical and technological support, which frees up a significant part of his time for live communication with students.

3. Project training methods

In the process of teaching, the main attention is paid to the methodology of organizing the educational process based on the project method of teaching using ICT. Educational projects are used as a form of work on generalization and systematization of knowledge and skills in computer science and to demonstrate their application in practice when solving a problem from a subject area. The faculty member uses the project form in lessons, in circles, on special courses, in educational research and home work. All this leads to the fact that many Bachelors, Masters and Post-graduate students annually take part in different kinds of conferences presenting the results of their research work and projects. Students develop the ability to work with information to create a project, master the software at a higher level, learn to explore, put forward their ideas, analyze information, make generalizations, conclusions, and learn various forms of a report on the work done.

4. Research methods in training

In the process of research, students do not receive knowledge in a ready-made form, but make a so-called “discovery” independently. The use of search and inventive activity technology is very popular nowadays [6, p. 57-61]. The faculty member only directs this activity and sums it up, giving an exact formulation of the established algorithms of action. The effectiveness of using this method is manifested in the dynamics of intellectual, creative and communicative abilities, increasing the number and quality of research works of students.

5. Multi-media technologies

Multi-media technology helps to use modern means of organizing educational activities and is focused on the formation of students' different competencies, search style of thinking, as well as visual and imaginative thinking skills. Using multimedia allows students to learn how to transfer research skills to the implementation of creative projects. Students apply their knowledge in practice; develop such necessary qualities in life as initiative, independence, and concentration. Moreover, multi-media technology allows students to develop the skills of self-presentation and public speaking. As we have already mentioned students are not afraid to participate in conferences presenting their material. So it is also the means of socialization and adaptation [13, p. 239–241], [17, p. 156–168]. Multimedia performances increase the effectiveness of the educational process because students' perception is activated through the use of sound and visual demonstrations; a large amount of information can be obtained from the Internet and from CDs and played on the screen in a format that is visible to all students; it is easier for students to respond when they rely on the speech plan displayed on the screen.

6. Computer testing and developing e-courses.

This type of works has been widely applied by faculty members of KSAU. It is not a secret that there are a lot of students that are studying by correspondence and the presence of e-courses developed on Moodle platform really makes their learning easier. As for full-time students, one can observe that the number of contact hours is constantly decreasing, so e-complexes help teachers to organize students' independent work effectively. Moodle complexes are being effectively introduced into the educational process [7], [8]. They have all necessary elements and resources that make teacher's work effective. The main elements of the Moodle course are:

- Assignment: the element allows to create a collection of files uploaded by students; the teacher writes a task to students that they perform on their computer, and receives from them a file (files) with the finished work (for text essays, there is another element);
- External Tool: communication with other learning systems based on the LTI data exchange format (Learning Tools Interoperability);
- Questionnaire: allows the teacher to conduct additional research that may be useful in evaluating and stimulating learning. The teacher can use the questionnaire to collect data about students, learn more about the study group as a whole, and use it to organize training in this discipline more effectively;
- Database: a complex information object that most computer programs work with and without which modern education is impossible. in fact, a database is a related (relational) data table, which is formed in several stages - from determining the installation parameters and setting the structure of stored information, developing forms for entering records and viewing data templates, to working with students to fill them in;
- Glossary: an electronic analogue of the dictionary of special terms (dictionary), can be created sequentially by students during the entire period of study;
- Lecture: an element for conducting a lesson with control points in the form of questions, correct answers to which are a prerequisite for continuing the lesson;

- Poll: vote for element (definition of participants), the teacher describes some of the circumstances and formulates the problem so that students can Express their opinions, the teacher offers several response options, the survey appears the percentage of students who chose a particular answer;
- Seminar: the element to generate social reflection, the teacher sets the topic of the seminar and the rules of participation; students make reports and can then assess the reports of all participants of the seminar on the basis of criteria specified by the teacher; the final grade is calculated as the weighted sum of the scores of all the participants: students and author of the report, the teachers;
- Test: the element allows the teacher to create tests consisting of different types of questions: Multiple choice, True/false, matching, Short answer, Numeric; the teacher is free to ask multiple attempts and random selection; the test is evaluated automatically with the exception of the Essay;
- Forum: teacher's tool for organizing asynchronous communication of students on certain topics;
- Chat: a tool for organizing synchronous communication in real time.

In addition to course elements, the concept of Resources is highlighted. The course resource is added by the teacher and used as a separate course element that is available to students throughout the course. Usually, these are educational materials: books, reference books, etc., that is, those materials that do not have interactive elements. You can use various types of information presented on the Internet as a resource:

- Hyperlink: a link to an Internet page used as a course resource;
- Book: multi-page resource with chapters and bookmarks;
- IMS content package: a resource in the form of an IMS package created in accordance with the IMS Content Packaging specification;
- Folder: a resource in the form of a folder with various files uploaded by the teacher;
- Explanation: a resource that differs from all the others in that its content appears directly on the course page, which means that it can be used to directly address students or to improve the design Of the main course page (when creating a course, the Main page is cluttered with links and is poorly perceived by students, but explanations placed in the right places can
- Text page: the most popular resource is a web page with information;
- File: a resource in the form of a file, if possible - is embedded in the course, if this is not possible-students are invited to download this file for themselves.

In conclusion it should be said that, the use of information technology helps the teacher to increase the motivation of students and leads to a number of positive consequences such as: psychologically facilitates the process of learning material by students; arouses a keen interest in the subject of knowledge; forms different types of competences starting from universal, general cultural and professional; expands the general outlook; improves the ability to extract information from a variety of sources and process it using computer technology; develops the ability to briefly and clearly

formulate your point of view is formed; increases the productivity of teachers and students in the classroom.

Information technologies, in combination with correctly selected (or designed) training technologies, create the necessary level of quality, variability, differentiation and individualization of training and education.

References

1. Kozulina N.S., Goreva N.V., Grishina I.I. Motivation on success as a factor of activation of internal potentials in students of the university // Проблемы современной аграрной науки: мат-лы междунар. заоч. науч. конф. – Красноярск: Красн. гос. агр. ун-т, 2017. – С. 224–228.

2. Shmelev R.V., Antonova N.V. Implementing the Bologna Declaration and European standards ideas in Krasnoyarsk state agrarian university // Проблемы современной аграрной науки: мат-лы междунар. науч. конф. – Красноярск: Красн. гос. агр. ун-т, 2018. – С. 203–208.

3. Амбросенко, Н.Д., Современные информационные образовательные технологии как важный компонент стратегии развития Института международного менеджмента и образования (Красноярский государственный аграрный университет) / Н.Д. Амбросенко, Н.В. Антонова, Ж.Н. Шмелева // Вестник КрасГАУ. – 2015. – № 4. – С. 274–278.

4. Амбросенко, Н.Д., Предварительные итоги участия университета в реализации проекта «современная цифровая образовательная среда» / Г.Д. Амбросенко, О.Н. Скуратова, Ж.Н. Шмелева // Азимут научных исследований: педагогика и психология. – 2019. – Т. 8, № 1 (26). – С. 16–19.

5. Антонова, Н.В. Опыт внедрения практико-ориентированного подхода к обучению в аграрном вузе / Н.В. Антонова, Ж.Н. Шмелева // Современные исследования социальных проблем. – Красноярск, 2017. – Т. 8, № 4. – С. 75–85.

6. Дмитриев, В.А. Технология поисково-изобретательской деятельности, как способ повышения эффективности образовательного процесса / В.А. Дмитриев, Д.В. Захаржевский, С.А. Вахрушев // Образовательные технологии: состояние и перспективы: тр. науч.-метод. конф., посвящ. 100-летию вступления в должность ректора ТТИ (ТПУ) проф. Е. Л. Зубашева, основоположника высшего технического образования в Сибири. – Томск: Томский политехнический университет,1999. – С. 57–61.

7. Капсаргина, С.А. The use of Moodle in the process of teaching a foreign language / С.А. Капсаргина // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. науч.-практ. конф. / Краснояр. гос. аграр. ун-т. – Красноярск, 2016. – С. 162–163.

8. Капсаргина, С.А. Использование современного программного обеспечения на платформе Moodle при обучении аудированию и говорению на иностранном языке в неязыковом университете / С.А. Капсаргина, Ж.Н. Шмелева // Азимут научных исследований: педагогика и психология. – 2019. – Т. 8, № 1 (26). – С. 147–150.

9. Козулина, Н.С. Методологические аспекты интерактивных технологий в профессиональном обучении Красноярского ГАУ / Н.С. Козулина, Ю.В. Кулешова // Проблемы современной аграрной науки: мат-лы международ. заоч. науч. конф. / Краснояр. гос. аграр. ун-т. – Красноярск, 2016. – С. 209–211.

10. Шмелева, Ж.Н. Requirements to the texts for the discipline “English for professional purposes” in the electronic educational complex on Moodle platform / Ж.Н. Шмелева // Современный педагогический взгляд. – Владивосток, 2019. – Вып. № 8 (33). – С. 69–73.

11. Шмелева, Ж.Н. The student-centred approach implementation in learning a foreign language using the LMS Moodle platform / Ж.Н. Шмелева // Психолого-педагогическое сопровождение образовательного процесса: проблемы, перспективы, технологии: мат-лы VI Междунар. науч.-практ. Конф. (4–5 апреля 2019 г., г. Орел) / под. ред. А.И. Ахулковой. – Орел: ОГУ им. И.С. Тургенева, 2019. – С. 365–369.

12. Шмелева, Ж.Н. Целесообразность имплементации стандарта ENQA по студентоцентрированному обучению при изучении иностранного языка. / Ж.Н. Шмелева, С.А. Капсаргина // Современные исследования социальных проблем. – 2018. – Т. 9, № 3. – С. 111–126.

13. Шмелева, Ж.Н. Социализация и адаптация студентов первого курса ИММО красноярского ГАУ посредством изучения иностранного языка / Ж.Н. Шмелева // Профессиональное самоопределение молодежи инновационного региона: проблемы и перспективы: сб. ст. по мат-лам всерос. науч.-практ. конф с междунар. участием. – Красноярск: Литера-принт, 2017. – С. 239–241.

14. Шмелева, Ж.Н. Студент-центрированное изучение иностранного языка в неязыковом университете / Ж.Н. Шмелева // Азимут научных исследований: педагогика и психология. – 2019. – Т. 8, № 1 (26). – С. 297–300.

15. Шмелева, Ж.Н., Проблемы внедрения и перспективы развития Болонского процесса в вузе (на примере Красноярского агроуниверситета) / Ж.Н. Шмелева, Н.В. Антонова // Вестн. КрасГАУ. – 2011. – № 12. – С. 306–312.

16. Шмелева, Ж.Н. Проблемы трудоустройства выпускников современного учреждения высшего профессионального образования. Ж.Н.Шмелева, Н.В. Антонова // Вестник КрасГАУ. – 2014. – № 3. – С. 209–213.

17. Шмелева, Ж.Н., Адаптация и социализация студентов аграрного вуза посредством изучения иностранного языка в институте международного менеджмента и образования. / Ж.Н. Шмелева, С.А. Капсаргина // Современные исследования социальных проблем. – 2016. – № 10 (66). – С. 156–168.

УДК 378.1:004

POSSIBILITIES FOR THE USE OF DIGITAL RESOURCES AT THE FOREIGN LANGUAGE LESSONS IN HIGHER EDUCATIONAL INSTITUTIONS

Khramtsova Tatyana Georgievna
Senior Lecturer
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

This article reports about the main possibilities of using modern digital resources at the lessons in foreign languages and their importance in modernization of higher school education.

Keywords: *development, modernization, possibilities, learner, foreign languages, communicative competence, motivation, digital educational resources, multimedia tools.*

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ РЕСУРСОВ НА УРОКАХ ИНОСТРАННОГО ЯЗЫКА В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

Храмцова Татьяна Георгиевна
старший преподаватель
Красноярский государственный аграрный университет, Красноярск, Россия

Данная статья рассказывает об основных возможностях использования современных цифровых ресурсов на уроках иностранного языка и их важности в модернизации высшего образования.

Ключевые слова: *развитие, модернизация, возможности, обучающийся, иностранные языки, информационные технологии, Интернет, коммуникативная компетенция, мотивация, цифровые образовательные ресурсы, мультимедийные инструменты.*

The rapid development of new information technologies influenced the great development the personality of a modern learner. Today computer learning is introduced into the school consciousness. One of the main parts in the progressive education is the use of information technology in educational disciplines.

Modernization of higher school education implies updating its content. Special attention is given to creating conditions for the development of students' personal potential and expanding the possibilities of advanced education, including international languages.

The Internet has become an integral part of modern high school reality. The Internet can help in learning languages, because it allows to use authentic texts, to listen and to communicate with native speakers. Such activities create a natural language environment. Access to the Internet makes it possible to take advantage of a huge

amount of additional materials to enrich the lessons with a variety of ideas and exercises.

The main goal in teaching foreign languages at high school is the development of communicative competence for participation in intercultural communication in a foreign language. But the quality of achieving this goal depends on motivation and needs of the individuals. It is motivation, that causes purposeful activity, determines the choice of tools and techniques, their ordering to achieve the goal. When students start studying in a foreign language, not a single teacher can complain about their lack of interest in the subject, but it decreases sometimes because of different problems in the learning process.

One of the most important motivators in this case, in my opinion, is the use of digital educational resources. A modern teacher should be able to create conditions for practical mastery of the language for each student, choose such teaching methods, which would allow them to show their activity, their creativity, and also to activate the student's cognitive activity in the process of teaching foreign languages. According to traditional methods of conducting the lesson, the teacher is the main source of information for students, and sometimes it does not work. Therefore, one conclusion can be made - it is necessary to conduct lessons using new information technologies. However, the introduction of multimedia programs into the educational process should not exclude traditional teaching methods, but should be harmoniously combined, what makes the learning process attractive and interesting. This is a powerful tool for increasing learner’s motivation to master a foreign language.

Besides, the use of digital educational resources by teacher’s preparation for the lessons became very important too, because it allows to include students into active cognitive activities by using multimedia tools. However, the use of digital educational resources has also some disadvantages, and the most remarkable of them are the growth in the volume of knowledge and the difficulty of assimilating it in a short time of training. The solution of this problem is to change the approach to educational activity. The educational process should correspond to the level of students’ perception, understanding and awareness.

УДК 343.1:351

CRIMINAL LAW COUNTERACTION OF CRIMES IN THE ECONOMIC SPHERE AS A BASIS FOR ENSURING NATIONAL SECURITY

Pakhritdinova Adema Shamilevna
scientific adviser ***Sambekova Bakytgul Raktaevna***
Eurasian National University named after L.N. Gumilyova, Nur-Sultan, Kazakhstan

The article considers a number of aspects of criminal legal counteraction to criminal activity in the economic sphere. The interaction between this counteraction and ensuring national security is shown. The features of criminal legal counteraction to crimes in the economic sphere are revealed on the example of the Republic of Kazakhstan.

Keywords*: criminal law, counteraction, crime, economic sphere, national security, Republic of Kazakhstan.*

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В ЭКОНОМИЧЕСКОЙ СФЕРЕ КАК ОСНОВА ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Пахритдинова Адема Шамилевна,
Научный руководитель ***Сембекова Бакытгуль Ракатаевна***
Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан

В статье рассмотрен ряд аспектов уголовно-правового противодействия преступной деятельности в экономической сфере. Показано взаимодействие между данным противодействием и обеспечением национальной безопасности. Выявлены особенности уголовно-правового противодействия преступлениям в экономической сфере на примере Республики Казахстан.

Ключевые слова*: уголовное право, противодействие, преступление, экономическая сфера, национальная безопасность, Республика Казахстан.*

Given the economic prosperity of Kazakhstan and the growth of the welfare of its citizens, the lack of legal regulation of these issues creates difficulties in general in ensuring the economic security of the state.

The term "economic crime" in the last decade are widely heard. Attention is drawn, in particular, to the fact that economic crime has become a problem on a national scale, because it has a powerful charge of destructive and dysfunctional properties and has a “negative impact on the processes taking place both in the economic and social spheres life of society [1].

The science of criminal law has not yet developed a consensus on the relative definition of the concept of economic crime. It is argued that “the boundaries of such

a concept are generally very difficult to clearly define in a strictly criminal legal sense in view of its (concept) well-known conventions [2]. A study of the literature gives reason to single out three views on economic crimes: wide, narrow, moderate (median).

So, it is noted that almost any crime can be reduced to economic categories, i.e. one from which his subject receives direct or indirect material benefit. If we consider material gain a mandatory sign of economic crime, then such a statement has a right to exist.

Many attacks on life are committed out of self-interest, and it is no coincidence that in paragraph 8 of part 2 of article 99 of the Criminal Code of the Republic of Kazakhstan as a qualifying circumstance provides for murder from selfish motives, as well as for hire or involving robbery, extortion or banditry. The theory of criminal law and judicial practice are considered mercenary to be the unlawful intentional infliction of death committed in order to obtain material benefits.

The intention to obtain material benefits most often lies at the basis of such assaults as murder committed with the aim of removing organs or tissues of a person for transplantation or other use (Section 12, Part 2, Article 99). The same motives are often guided by a person committing crimes against personal freedom - kidnapping, illegal imprisonment and placement in a psychiatric hospital (Articles 125-127). In particular, in paragraph 3 of part 2 of article 125 of the Criminal Code established increased responsibility for the abduction of a person from selfish motives. Many crimes against the constitutional rights and freedoms of man and citizen (chapter 3) also presuppose that the offender has mercenary intentions.

At the same time, it would be wrong to call these crimes economic, since unlawful property interest in them acts as a concomitant, and economic relations as an additional (mandatory or optional) object of criminal law protection. Actually, economic crimes have the above-mentioned relations as the main, leading object. Therefore, it is necessary to distinguish between offenses that have economic motivation (the so-called economic orientation) and economic crimes [4].

It is necessary to proceed from the fact that the legislation of many countries, including the Russian one, is now practically undecided in this matter. So, the Criminal Code of Russia included in section VIII “Crimes in the field of economics” acts committed not only in the field of economic activity (chapter 22), but also against property (chapter 21). This section also includes encroachments against the interests of service in commercial and other organizations (chapter 23), many of which, as B.V. Volzhenkin rightly notes, “are far from always connected with the economy” (for example, abuse of authority by private notaries and auditors, serving private detective and security services), in connection with which the presence of this chapter in section 8 is "very doubtful". Nevertheless, with some degree of conventionality, the crimes of this chapter should be called economic. Even more so, this name is applicable to property crimes. And it’s not at all because, as noted in the legal literature, almost all infringements in the sphere of economic activity also harm property relations, and crimes against property at the same time violate the normal way of economic relations, which “allows us to conclude about difficulties and practical the im-

possibility of a clear, unambiguous delineation of crimes against property and so-called economic crimes".

Of course, there are known difficulties in delimiting property acts from those committed in the field of economic activity both in Russian legislation and in the legislation of Kazakhstan. These gaps in both laws existed before – this is evidenced, in particular, by the fact that, despite the external isolation of the chapters on property and economic crimes in the previous codes, certain types of acts "migrated" from one chapter to another. Despite the well-known difficulties, acts directed against property, and committed in the field of economic activity, it is quite possible and necessary to distinguish, and especially on the object. In property relations, it is customary to distinguish between static and dynamic parties. If the static side is characterized by the state of ownership of material goods to the owner, then the dynamic side is characterized by the use of an object in the process of production, distribution, consumption and exchange, finding "things in circulation".

Everyone knows that economic crimes are tremendously damaging to both the state and citizens and organizations. The economic security of any country is primarily aimed at the positive development of the state economy. The list of articles of economic crime in the Criminal Code is defined in Chapter 8, which is illegal business, illegal credit, tax evasion, counterfeiting money, economic smuggling, the legalization of money obtained by illegal means etc. One of the relevant and common types of economic offenses is tax evasion and customs duties, the damage to the state from illegal activities of which amounts to billions of tenge.

The total amount of damage caused to the state, according to the statistics committee of the Republic of Kazakhstan, amounted to just over 1 billion tenge, of which 580 million tenge was compensated. Imposed seizure of property of the perpetrators in the amount of 183 million tenge. The main amount consists of tax evasion and customs payments – 532 million tenge, reimbursed - 205 million tenge.

At the same time, prior to decriminalization of Article 215 of the Criminal Code (pseudo-entrepreneurship), a lot of work was done to identify crimes and redress (the established amount of damage was 440 million tenge, compensated - 370 million tenge).

Already in mid-July 2017, the Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Improving the Law Enforcement System" dated July 3, 2017, article 215 (false business) was decriminalized (excluded) from the Criminal Code.

At the same time, before decriminalization, some unscrupulous entrepreneurs avoided paying taxes by concluding fictitious transactions with pseudo-enterprises, in other words, false invoices were written - invoices, invoices, etc., for allegedly performed work, thereby reflecting their mutual settlements.

At the same time, the criminal liability of business entities for taking actions to issue an invoice without actually performing work, providing services, or shipping goods occurs under article 216 of the Criminal Code.

In addition, for crimes of tax evasion and other obligatory payments, the budget, the guilty person, if for the first time such an act and voluntarily pays tax arrears and (or) other obligatory payments to the budget, is exempted from criminal liability.

Criminal offenses in the economic sphere inflict tremendous damage to the economic security of the Republic, as they undermine its sustainable development and internal economic independence. Criminal legislation often changes; the legislator does not yet have an effective legal basis for the disclosure of economic crimes; this gap is not only in Kazakhstan. Despite the more or less satisfactory development of the structure of economic crimes, statistics on them in the world cannot be collected. One of the main UN bodies, the Economic and Social Council, attempted to collect data on property appropriation, bribery and fraud, but they turned out to be very incomplete. The only conclusion that can be drawn from them is to say that such crimes are growing and becoming more and more unprovable.

List of references

1. Колесников, В.В. Преступность в сфере экономической деятельности и её криминологическая характеристика / В.В. Колесников // Вопросы квалификации и расследования преступлений в сфере экономики. – Саратов, 2011. – С. 75.

2. Яни, П.С. Экономические и служебные преступления. / П.С. Яни. – М., 2013. – С. 32.

3. Лопашенко, Н.А. Преступления в сфере экономической деятельности / Н.А. Лопашенко. – Ростов н/Д., 1999. – С. 9.

УДК 378.1:004

THE EXPERIENCE OF THE "FOREIGN LANGUAGE" DEPARTMENT AT KRASNOYARSK SAU ON THE IMPLEMENTATION OF THE MOODLE PLATFORM IN THE PROCESS OF LEARNING FOREIGN LANGUAGES

Shmeleva Zhanna Nikolaevna
candidate of science in philosophy, docent
Krasnoyarsk state agrarian university, Krasnoyarsk, Russia

The article discusses the experience and the results of introducing LMS MOODLE into the process of learning foreign languages at Krasnoyarsk SAU.

Key words: *foreign languages, students, higher education, non-linguistic institution, information-communication technologies, education, e-complex.*

ОПЫТ КАФЕДРЫ "ИНОСТРАННЫЙ ЯЗЫК" КРАСНОЯРСКОГО ГАУ ПО ВНЕДРЕНИЮ ПЛАТФОРМЫ MOODLE В ПРОЦЕСС ИЗУЧЕНИЯ ИНОСТРАННЫХ ЯЗЫКОВ

Шмелева Жанна Николаевна
кандидат философских наук, доцент
Красноярский государственный аграрный университет, Красноярск, Россия

В статье рассматривается опыт и результаты внедрения LMS MOODLE в процесс обучения иностранным языкам в Красноярском ГАУ.

Ключевые слова: *иностранные языки, студенты, высшее образование, неязыковое учебное заведение, информационно-коммуникационные технологии, образование, электронный комплекс.*

To substantiate the relevance of the issue it should be mentioned that information-communication technologies have become some kind of breakthrough in the system of modern higher education [3, p. 120-122], [10, p. 330-333], [11, p. 162-163]. It influenced to a great extent on the possibility of modern pedagogy trends implementation and allowed to develop both humanistic and technological directions of education [12, p. 209-211]. The experience of introducing information technologies gives grounds to assert that when they are successfully used in teaching of various subjects (including foreign language) [13, p. 247-249], [4, p. 428-433], they help to reveal the reserves of the educational process, to provide the interaction of the teacher and students, and to develop the strategies of independent and autonomous learning that increase motivation for the subject [2, p. 420-423], [5, p. 224-228], [7, p. 218-223]. An important condition for the successful implementation of these advantages is the choice of the right model of training based on the integration of traditional and innovative approaches.

The introduction of electronic information resources in learning a foreign language at the universities will expand the range of opportunities to practice language skills [14, p. 287-290], [15, p. 267-269], thanks to the multimedia system by embedding into a single system a variety of text materials, functions, options, methods of processing the hypertext information.

Computer linguistic didactics is one of the fastest growing areas of language teaching methods and one of the most popular interactive technologies [12, p. 209-211]. For a relatively short period of its existence, it has come a long way, closely associated with the development of computer technology, on the one hand, and the concepts of language learning – on the other. The opportunities offered by modern information technologies are so important for language acquisition that learning with the use of computers and computer-based learning materials becomes an integral part of the educational process. Moreover, the foreign language teachers at the non-linguistic universities are working in the conditions of the constant reduction of contact hours for learning English, so they simply have to develop different educational information-communicative resources in order to fill the gap and establish also inter-subject links [8, p. 45-49].

The "Foreign language" Department of Krasnoyarsk SAU has actively started the implementation of the Moodle platform into the educational process [1, p. 414-419], [17, p. 508-513], and it helps to manage the educational process at the university [18, p. 130-133], [19, p. 211-212] as well as to identify talented students [9, p. 146-148], [6, p. 175-177]. These talented students may further use their English language knowledge for their academic mobility [2, p. 420-423]. First, the complexes were rather simple and even primitive, but then, when the skills of teachers became better, they started using different types of tasks like "Crosswords" and even use the elements of gamification to make the process of learning more interesting and competitive.

If we compare computer training materials and printed manuals, audio and video courses, we can note the technological and methodological advantages provided by the computer. The main ones are the following: handling large amounts of information; individualization of learning; choosing own tempo of learning; integrated multi-touch effect on a variety of channels perception through the use of text, sound, animation, video; unlimited number of requests to tasks; immediate feedback.

Moreover, computer training materials have a certain number of characteristics inherent only in this type of learning tools such as: interactivity; adaptability; non-linearity of information provision; individuality of design; the opportunity to use special software to produce audio-tracks for texts and vocabulary; the need for special training of the user to work with the program.

Speaking about the effectiveness, we should say that the effective use of information technologies in language teaching depends on such factors as: provision of computer equipment and Internet access; availability of computer training materials and the necessary set of programs of different types; educational quality of the used computer training tools; sufficient level of general computer literacy of students and teachers; special training of teachers in the field of computer linguistic didactics; availability of qualified engineering support staff; effective organization of the educa-

tional process. Krasnoyarsk SAU being among the best agrarian universities in Russia managed to fulfill all these requirements. First, university has well-developed information-computer resources with the access to the Internet and support staff to provide large-scale work with the information resources. The requirements for a language teacher in the use of computer technology are much higher than the requirements for teachers of other subject disciplines, because the language teaching software includes a very wide range of software and educational materials focused on different levels, stages, aspects and profiles of training. As a result, all the teachers of the "Foreign language" department (100%) have been trained in the programme "Work in the information educational environment to support the educational process using Distant Learning Technologies" in the amount of 72 hours and have been developing educational complexes on Moodle platform. Actually one can distinguish some levels of the computer literacy. The first level, which can be called basic, is an indicator of the general professional culture of each teacher of a foreign language. At this level, the teacher should be able to use a limited number of computer applications: text editor, computer dictionaries, e-mail, web browser, search engines. The second level, which can be considered the main one, assumes the presence of theoretical training in the field of computer linguistic didactics and the ability to work with a set of tools used in language learning. It includes all kinds of training programs, extended block of applications and tools. The teacher of a foreign language must also possess the necessary terminological apparatus for the use of a set of software in the target language. The third level, advanced training is aimed at teachers-methodologists in the field of computer didactics. Such a teacher should not only have the most complete understanding of computer language teaching tools and resources for teachers, but also act as an organizer and coordinator of the process of using information technology in language learning. In order to achieve the third level, the re-training of faculty members is conducted every three years.

Moreover, all the teachers have been trained in the programme "Methods of teaching English and innovative approaches to the organization of the educational process in the implementation of the Federal General Educational Standard", so the content of the courses complies with all the standards.

References

1. Kapsargina S.A. Professionally-oriented foreign language teaching in non-linguistic university// Проблемы современной аграрной науки: мате-лы междунар. науч. конф. / отв. за вып. В.Л. Бопп, Ж.Н. Шмелева. – Красноярск, 2019. – С. 414–419.

2. Kapsargina S.A. Programmes of academic mobility as a factor of increasing motivation to learn a foreign language // Проблемы современной аграрной науки. Материалы международной научной конференции / отв. за вып. В.Л. Бопп, Ж.Н. Шмелева. – Красноярск, 2019. – С. 420–423.

3. Kapsargina S.A. The use of LMS Moodle to intensify the independent work of students in teaching a foreign language in a non-linguistic university // Азимут

научных исследований: педагогика и психология. – 2018. – Т. 7, № 4 (25). – С. 120–122.

4. Kozulina N.S. Specificity of the Bachelor's training in the direction 44.03.04 (professional training (in branches)) at the Krasnoyarsk SAU // Проблемы современной аграрной науки: мат-лы междунар. науч. конф. – Красноярск: Красн. гос. агр. ун-т, 2019. – С. 428–433.

5. Kozulina N.S., Goreva N.V., Grishina I.I. Motivation on success as a factor of activation of internal potentials in students of the university // Проблемы современной аграрной науки: мат-лы междунар. заоч. науч. конф. – Красноярск: Красн. гос. агр. ун-т, 2017. – С. 224–228.

6. Kuleshova Yu.V., Kozulina N.S., Grishina I.I. The method of problematic presentation as a way of organizing the productive activity of students and disclosing their creativity // Наука и образование: опыт, проблемы, перспективы развития: мат-лы междунар. науч-практ. конф. – Красноярск: Красн. гос. агр. ун-т, 2018. С. 175–177.

7. Вахрушев С.А., Вахрушева Л.П., Бабик Я.С. К вопросу о создании познавательных мотивов у детей младшего школьного возраста // Культура. Искусство. Образование: сб. науч. и метод. тр. / Краснояр. гос. ин-т искусств. – Красноярск, 2016. – С. 218–223.

8. Вахрушев, С.А. К вопросу о влиянии межпредметных связей на развитие метапредметных умений обучающихся / С.А. Вахрушев, А.А. Логинова // Культурно-образовательное пространство: новые задачи – новые решения: мат-лы II Всерос. (с междунар. участием) заоч. науч. конф. / Краснояр. гос. акад. музыки и театра. – Красноярск, 2015. – С. 45–49.

9. Вахрушев, С.А. Об особенностях воспитания одаренных детей / С.А. Вахрушев, М. Сазонова, Л.П. Вахрушева // Культура. Искусство. Образование: сб. науч. и метод. тр. / отв. ред. Н. А. Еловская. Красноярск, 2013. – С. 146–148.

10. Капсаргина, С.А. The use of LMS Moodle for creating e-courses in a discipline of foreign language for students of non-linguistic university / С.А. Капсаргина // Наука и образование: опыт, проблемы, перспективы развития: мат-лы междунар. науч.-практ. конф. – Красноярск: Красн. гос. агр. ун-т, 2019. – С. 330–333.

11. Капсаргина, С.А. The use of Moodle in the process of teaching a foreign language / С.А. Капсаргина // Наука и образование: опыт, проблемы, перспективы развития: мат-лы XIV междунар. науч.-практ. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2016. – С. 162–163.

12. Козулина, Н.С. Методологические аспекты интерактивных технологий в профессиональном обучении Красноярского ГАУ / Н.С. Козулина, Ю.В. Кулешова // Проблемы современной аграрной науки: мат-лы междунар. заоч. науч. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2016. – С. 209–211.

13. Храмцова, Т.Г. Использование современных коммуникативно-ориентированных методов преподавания немецкого языка как иностранного в неязыковых вузах / Т.Г. Храмцова // Проблемы современной аграрной науки:

мат-лы междунар. заоч. науч. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2016. – С. 247–249.

14. Храмцова, Т.Г. Обучение грамматике: практические советы и рекомендации / Т.Г. Храмцова // Наука и образование: опыт, проблемы, перспективы развития: мат-лы междунар. науч.-практ. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2019. – С. 287–290.

15. Храмцова Т.Г. Основные методы и подходы при обучении иностранному языку// Проблемы современной аграрной науки: мат-лы междунар. науч. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2017. – С. 267–269.

16. Храмцова, Т.Г. Роль технологий в традиционном понимании с точки зрения образования / Т.Г. Храмцова // Проблемы современной аграрной науки: мат-лы междунар. науч. конф. – Красноярск: Краснояр. гос. аграр. ун-т, 2018. – С. 298–301.

17. Храмцова, Т.Г. Современные формы организации самостоятельной работы обучающихся в университете / Т.Г. Храмцова // Проблемы современной аграрной науки: мат-лы междунар. науч. конф. / отв. за вып. В.Л. Бопп, Ж.Н. Шмелева. – Красноярск: Краснояр. гос. аграр. ун-т, 2019. – С. 508–513.

18. Храмцова, Т.Г. Управление учебно-воспитательным процессом в вузе / Т.Г. Храмцова // Ресурсосберегающие технологии сельского хозяйства: сб. науч. ст. – Красноярск: Краснояр. гос. аграр. ун-т, 2019. – С. 130–133.

19. Lukhtina M.A. About conditions of training of future bachelor in agriculture for performance of organizational and management activity // Инновационные тенденции развития российской науки: мат-лы IX Междунар. науч.-практ. конф. молодых ученых. – Красноярск: Краснояр. гос. аграр. ун-т, 2016. – С. 211–212.

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ: ГЕНЕЗИС И ПЕРСПЕКТИВЫ

Материалы I Международной межвузовской научно-практической конференции 28 февраля 2020 года

Электронное издание

Подписано в свет 20.04.2020. Регистрационный номер 63
Редакционно-издательский центр Красноярского государственного аграрного университета
660017, Красноярск, ул. Ленина, 117 e-mail: rio@kgau.ru