П О Л О Ж Е Н И Е

о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных ФГБОУ ВПО КрасГАУ

2014

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор безопасности ИСПДн – лицо, ответственное за защиту ИСПДн от несанкционированного доступа к информации.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Документ – материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения.

Информационная система персональных данных (ИСПДн) – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Объект информатизации (ОИ) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы персональных данных (ТС ИСПДн) – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных ФГБОУ ВПО КрасГАУ (далее – Положение) относится к основополагающим документам, определяющим общие принципы организации работ по информационной безопасности персональных данных, обрабатываемых с использованием средств автоматизации.

Данное Положение разработано в соответствии с:

- Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ,
- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
-

Организация и проведение работ по обеспечению безопасности информации, содержащей ПДн, на объектах информатизации организации проводится на основании законодательных и нормативных актов Российской Федерации в области защиты информации и настоящего Положения.

Требования настоящего Положения являются обязательными для исполнения в организации, а также организациями, учреждениями и предприятиями, выполняющими работы по защите информации в организации.

Положение определяет порядок организации и проведения работ по защите информации, содержащей ПДн, на объектах информатизации организации как в период их создания, так и в процессе повседневной эксплуатации.

Принимаемые меры по защите информации на объектах информатизации организации должны обеспечивать выполнение действующих требований и норм по защите информации. Разработка мер и обеспечение защиты информации на объектах информатизации осуществляются управлением информатизации и компьютерной безопасности организации или ответственным за обеспечение безопасности ИСПДн работником. Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России и ФСБ России на право проведения соответствующих работ.

Согласование планируемых мер, контроль выполнения работ на местах, соответствия принятых мер и проводимых мероприятий по защите информации действующим требованиям и нормам производит управление информатизации и компьютерной безопасности или ответственный работник (Приложение 1, 2).

Объекты информатизации организации должны соответствовать требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

Ответственность за общее состояние и организацию работ по созданию и эксплуатации объектов информатизации возлагается на руководителя организации. Ответственность за обеспечение требований по защите информации, циркулирующей на объектах информатизации, возлагается на начальников структурных подразделений организации, эксплуатирующих эти объекты.

Контроль выполнения требований настоящего Положения возлагается на руководителя организации.

Финансирование мероприятий по защите персональных данных предусматривается сметами организации на планируемый год. При этом:

- расходы по защите информации при эксплуатации существующих помещений, технических систем и средств включаются в стоимость их содержания;
- затраты, связанные с защитой информации в создаваемых информационно-вычислительных и других технических системах, предусматриваются в стоимости создания и развития этих систем;
- расходы по защите информации при ремонте и реконструкции помещений предусматриваются в стоимости этих работ.

2. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ПОРЯДКУ ОСУЩЕСТВЛЕНИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ (ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ) ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ, В ФГБОУ ВПО КРАСГАУ

2.1. Требования по защите (обеспечению безопасности) персональных данных от утечки по техническим каналам и от НСД

Организацию безопасности персональных данных при их обработке в ИСПДн, в состав которых входят СВТ, предназначенные для обработки персональных данных, осуществляет начальник подразделения по защите информации, ответственный за эксплуатацию объекта информатизации.

Состав программного обеспечения, технических средств и систем ИСПДн, предназначенных для обработки персональных данных, должен соответствовать номенклатуре, объему и сложности задач, решаемых с использованием средств автоматизации, а также степени конфиденциальности и характеристикам (особенностям) информационного ресурса, подлежащего обработке с использованием средств автоматизации.

В состав программного обеспечения ОИ, предназначенного для обработки персональных данных, помимо общего (операционные системы, текстовые и графические редакторы, средства архивации данных, средства доступа к файловой системе, средства мультимедиа и пр.) и специального (прикладного) программного обеспечения рекомендуется включать сертифицированные по требованиям безопасности информации средства антивирусной защиты.

Из состава технических средств и систем СВТ, предназначенных для обработки персональных данных, должны быть исключены (заблокированы) избыточные элементы и, в первую очередь, устройства ввода/вывода персональных данных на внешние носители, не входящие в состав ОТСС.

Средства обработки и передачи персональных данных в составе сети передачи данных, включая модемы, терминалы, рабочие станции и серверы, должны отвечать требованиям и нормам нормативных документов федерального органа-уполномоченного в области противодействия техническим разведкам и технической защите информации, предъявляемым к ТС ИСПДн по защите информации от утечки по техническим каналам.

Линии передачи данных и условия их прокладки должны отвечать требованиям и нормам нормативных документов федерального органа, уполномоченного в области противодействия техническим разведкам и технической защите информации.

Размещение и монтаж ТС ИСПДн, предназначенных для отображения и создания копий документов на бумажных носителях (видеотерминалов, печатающих устройств, графопостроителей и т.п.) необходимо проводить с учетом максимального затруднения визуального просмотра информации посторонними лицами (шторы и/или жалюзи на окнах, непрозрачные экраны и т.п.).

Условия размещения СВТ, предназначенных для обработки персональных данных, должны удовлетворять требованиям:

- по удалению СВТ от ближайших строений, зданий и сооружений сторонних организаций;
- по удалению СВТ от помещений, сдаваемых в аренду сторонним организациям;
- по удалению СВТ от границ КЗ (с учетом этажности здания и функционального назначения соседних помещений, а также помещений, расположенных этажами выше и ниже).

Системы электропитания и заземления СВТ должны соответствовать нормам, установленным нормативными документами федерального органа, уполномоченного в области противодействия техническим разведкам и технической защите информации.

Запрещается обработка персональных данных с использованием СВТ, имеющих выход в открытые телекоммуникационные сети без использования сертифицированных по требованиям безопасности межсетевых экранов.

Защита персональных данных, обрабатываемой с использованием средств автоматизации, должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также по предупреждению преднамеренных программно-технических воздействий на информацию с целью нарушения ее конфиденциальности, целостности и доступности в процессе ее обработки, передачи и хранения.

Все средства защиты информации (СЗИ), применяемые для защиты персональных данных, обрабатываемой с использованием СВТ, должны иметь сертификаты соответствия по требованиям безопасности информации, а эффективность применяемых технических и/или организационных решений, направленных на обеспечение конфиденциальности, целостности и доступности информации, должна быть подтверждена результатами аттестационных испытаний ОИ.

Технические и организационные решения для конкретной информационной технологии разрабатываются специалистами по защите информации ФГБОУ ВПО КрасГАУ либо организацией, имеющей соответствующие лицензии органа, уполномоченного на ведение лицензионной деятельности.

Испытания ОИ на соответствие требованиям по безопасности информации, контроль защищенности информации, обрабатываемой с использованием ОИ, техническое обслуживание и

ремонт СВТ, предназначенных для обработки персональных данных, могут проводиться специалистами ООО «ЦБС» или специалистами других организаций, имеющих соответствующие лицензии.

При проведении технического обслуживания и ремонта СВТ непосредственно на объекте информатизации допуск сотрудников сервисных (ремонтных) организаций осуществляется в установленном порядке при наличии у них соответствующего допуска к персональным данным.

При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения персональных данных. Вышедшие из строя элементы и блоки СВТ заменяются на новые элементы и блоки, при этом осуществляется контроль эффективности защиты информации.

Обработка персональных данных определенного уровня защищенности должна проводиться с использованием сертифицированных СВТ по классу защищенности и с использованием программного обеспечения СЗИ, прошедших контроль отсутствия недекларированных возможностей по уровню, определяемым «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Ответственность за обеспечение защиты персональных данных в процессе эксплуатации СВТ, предназначенных для обработки персональных данных, возлагается на руководителя подразделения, ответственного за эксплуатацию объекта информатизации.

Допуск пользователей к работе в ИСПДн, соответствующей требованиям безопасности информации, осуществляется приказом по организации и назначением лиц, ответственных за эксплуатацию ИСПДн.

Основанием для допуска пользователя (пользователей) к обработке персональных данных с использованием ИСПДн является утвержденное ректором ФГБОУ ВПО КрасГАУ и подписанное руководителем подразделения по защите информации "Разрешение на автоматизированную обработку информации" или приказ о допуске к работе в ИСПДн.

Контроль допуска к автоматизированной обработке информации осуществляет начальник управления информатизации и компьютерной безопасности, руководитель структурного подразделения, ответственного за эксплуатацию объекта информатизации, а также в пределах своих полномочий администратор безопасности ИСПДн.

2.2 Комплекс мероприятий, проводимых в организации по защите (обеспечению безопасности) персональных данных, обрабатываемой с использованием СВТ, реализующий требования по защите (обеспечению безопасности) персональных данных от утечки по техническим каналам и от несанкционированного доступа.

- Проведение подготовки прогнозных оценок в области защиты информации;
- Разработка модели угроз безопасности персональных данных;
- Разработка организационных и технических документов на объекты информатизации, подготавливаемые к аттестации;
- Определение уровня защищенности ПДн;
- Разработка должностных инструкций администратору безопасности, ответственному за обеспечение безопасности, пользователям ИСПДн;
- Сопровождение СЗИ от НСД на стадии эксплуатации;

- Разработка системы разграничения доступа к средствам вычислительной техники и в помещения, в которых они установлены, а также к персональных данных в средствах вычислительной техники;
- Закупка сертифицированных средств защиты персональных данных, определение обязательных требований к ним, а также порядка и условий их эксплуатации;
- Выделение и оборудование помещений, где проводится обработка персональных данных на ПЭВМ;
- Ведение учета машинных носителей информации;
- Установка и настройка программного обеспечения СЗИ;
- Осуществление периодических проверок файлов на жестких дисках рабочих станций антивирусными пакетами;
- Периодическое обновление антивирусных пакетов;
- Регулярное сканирование жестких дисков в поисках компьютерных вирусов;
- Осуществление резервного копирования важных документов (не менее двух резервных копий);
- Периодический контроль целостности корпусов коробов, в которых проложены кабели;
- Организация заземления всех розеток, к которым подключены компьютеры во всех помещениях;
- Ведение технической документации на объект информатизации (периодическое заполнение техпаспорта и др).

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации установлен в «Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных».

Для обеспечения защиты информационных ресурсов ИСПДн от программно-математических воздействий должна осуществляться антивирусная защита. При организации антивирусной защиты администратор безопасности руководствуется требованиями «Инструкции по проведению антивирусного контроля в ИСПДн».

Парольная защита объекта ВТ является составной частью подсистемы управления доступом системы защиты ИСПДн от НСД. При организации парольной защиты администратор безопасности руководствуется требованиями «Инструкции по организации парольной защиты при работе в ИСПДн».

3. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАЩЕНИИ С МАШИННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

При обработке персональных данных с использованием СВТ периодически, но не реже одного раза в год, проводится детальный анализ технологического процесса обработки информации, в первую очередь, организации выдачи персональных данных на печать и исключения возможности записи информации на неучтенные носители. Контроль проводится администратором безопасности ФГБОУ ВПО КрасГАУ.

Учет машинных носителей информации ведется в каждом подразделении, обрабатывающем персональные данные, с проставлением регистрационного номера, даты регистрации, номера экземпляра.

Уничтожение съемных машинных носителей информации типа ГМД, Flash, CD и DVD-дисков производится путем сожжения. Перед уничтожением машинных носителей персональных данных информация, содержащаяся на них, стирается. Стирание информации, а также уничтожение самих съемных машинных носителей производится по акту соответствующей формы. При этом НЖМД разбираются на отдельные элементы, а затем электронная и электромеханическая части деформируются до состояния, которое исключает их повторное использование, а магнитные диски уничтожаются путем сожжения.

Уничтожение машинных носителей информации может осуществляться с применением устройств уничтожения, сертифицированных по требованиям безопасности информации.

При необходимости вывода СВТ из режима обработки персональных данных запрещается передавать входящие в состав СВТ накопители персональных данных для обработки неконфиденциальной информации.

Машинные носители информации и печатные документы с информацией об обращениях к СВТ, попытках или фактах несанкционированного доступа к персональных данных, а также иная технологическая документация подлежат регистрации по определенным формам учета.

Отметка об уничтожении информации производится в «Журнале учета материальных носителей конфиденциальной информации (персональных данных)».

Порядок обращения с машинными носителями информации, обрабатываемой с использованием средств автоматизации, включает следующие основные этапы:

- получение допуска на автоматизированную обработку информации в ИСПДн (разрешительная система доступа);
- оформление и получение в подразделении по защите информации ФГБОУ ВПО КрасГАУ машинных носителей информации и необходимого количества зарегистрированных рабочих листов;
- регистрация пользователя в «Журнале учета лиц, допущенных к работе с персональными данными в ИСПДн»;
- обработка информации в ИСПДн;
- копирование информации на съемный машинный носитель информации;
- распечатка документа на зарегистрированные рабочие листы или с использованием СЗИ, обеспечивающих маркировку и учет выходных печатных документов;
- очистка оперативной памяти СВТ в соответствии с руководством по эксплуатации СЗИ или СВТ.

Оставшиеся отпечатанные (бракованные) после формирования документа учтенные листы сдаются пользователем ИСПДн (исполнителем документа) уничтожаются определенным порядком.

При эксплуатации информационных систем, предназначенных для обработки персональных данных, запрещается:

- проводить обработку персональных данных без выполнения обязательных мероприятий по ее защите;
- вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств аттестованной по требованиям безопасности информации ИСПДн:

- вносить изменения в состав программного обеспечения, структуру файловой системы ИСПДн без письменного разрешения руководителя подразделения, ответственного за эксплуатацию объекта информатизации, согласованного с администратором безопасности ИСПДн и руководителем подразделения по защите информации;
- осуществлять попытки несанкционированного доступа к резервам информационной системы и других пользователей;
- подключать ИСПДн к информационным сетям общего пользования и другим ИСПДн;
- отключать (блокировать) средства защиты информации ИСПДн;
- использовать неисправные машинные носители информации для ее хранения и обработки;
- использовать неучтенные машинные носители информации;
- производить запуск ПЭВМ, входящих в состав ИСПДн, с системных дискет или загрузочных CD дисков без письменного разрешения руководителя подразделения по защите информации, согласованного с администратором безопасности ИСПДн;
- обрабатывать информацию категории выше установленной для данной ИСПДн;
- производить модификацию, уничтожение и блокирование в отношении общего и специального (прикладного) программного обеспечения, применяемого для обработки персональных данных;
- разглашать сведения о реализованном на ОИ комплексе средств защиты информации;
- накапливать на машинных носителях информации сведения, содержащие персональные данные, надобность в которых миновала;
- хранить машинные носители информации вблизи сильных источников электромагнитных излучений;
- оставлять ПЭВМ, из состава ИСПДн, при выходе пользователя из помещения, в котором она установлена, не убедившись, что она заблокирована средствами защиты или отключена.

4. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ ФГБОУ ВПО КРАСГАУ, ОТВЕТСТВЕННЫХ ЗА ОСУЩЕСТВЛЕНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ (ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ) ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМОЙ С ИСПОЛЬЗОВАНИЕМ СВТ

4.1. Должностные лица подразделений организации, ответственные за разработку, обеспечение и реализацию мероприятий по защите персональных данных, их функциональные обязанности и права.

В ФГБОУ ВПО КрасГАУ установлен и обеспечивается режим безопасности персональных данных, предусматривающий в том числе распределение обязанностей работников по защите персональных данных.

Согласно должностным инструкциям:

- ответственность за обеспечение безопасности персональных данных в ФГБОУ ВПО КрасГАУ возлагается на начальника административно-правового управления ФГБОУ ВПО КрасГАУ.
- ответственность за организацию работ по защите (обеспечению безопасности) обрабатываемой с использованием СВТ информации и осуществление контроля выполнения требований по безопасности информации на ИСПДн возлагается на ответственного за

обеспечение безопасности ИСПДн и на Администратора безопасности, назначенных из состава сотрудников отдела экономической безопасности или отдела защиты информации предприятия.

Руководитель подразделения по защите информации отвечает за организацию работ по защите (обеспечению безопасности) обрабатываемой с использованием СВТ информации и осуществление контроля выполнения требований по безопасности информации на ОИ - ИСПДн.

Он обязан:

- планировать мероприятия по обеспечению защиты (обеспечению безопасности) персональных данных, обрабатываемых с использованием СВТ;
- определять порядок приобретения и приемки СВТ и СЗИ;
- организовывать работы по приведению в соответствие (либо аттестации) ИСПДн требованиям безопасности информации,
- организовывать разработку организационных и технических документов на объекты информатизации, подготавливаемые к приведению в соответствие требованиям безопасности информации;
- знать перечень задач, решаемых с использованием соответствующих требованиям безопасности информации ИСПДн, сроки их выполнения, категорию обрабатываемых персональных данных и лиц, допущенных к решению этих задач;
- вести учет аттестованных по требованиям безопасности информации объектов информатизации, СВТ и оргтехники;
- организовывать разработку (уточнение) Положения и обеспечивать ее строгое выполнение;
- организовывать проведение с пользователями ИСПДн занятий по изучению нормативных правовых и руководящих документов по вопросам защиты (обеспечения безопасности) информации на объектах информатизации и режиму конфиденциальности;
- контролировать выполнение комплекса организационно-технических мероприятий по защите (обеспечению безопасности) информации на объектах информатизации;
- организовывать работы по контролю эффективности технических (программно-технических, программных) мероприятий по защите (обеспечению безопасности) информации на объектах информатизации;
- контролировать порядок учета, хранения и обращения с программным и информационным обеспечением, съемными машинными носителями персональных данных;
- контролировать правильность ведения технических паспортов на объекты информатизации;
- организовывать работы по устранению выявленных в результате контроля нарушений требований безопасности информации, обрабатываемой в ИСПДн;
- обеспечивать проведение служебных расследований по фактам и попыткам НСД к персональных данных, обрабатываемых в ИСПДн;
- проводить анализ причин выявленных нарушений и недостатков в организации защиты (обеспечении безопасности) персональных данных, обрабатываемых с использованием СВТ.

Руководитель подразделения, ответственного за эксплуатацию объекта информатизации, предназначенного для обработки персональных данных, отвечает за организацию работ по обеспечению безопасности информации, обрабатываемой с использованием СВТ, в подразделении.

Он обязан:

- организовывать разработку номенклатуры задач, решаемых с использованием средств автоматизации, определять характеристику, объем и категорию информационного ресурса, подлежащего обработке с использованием средств автоматизации;
- организовывать развертывание комплекса ТС ИСПДн, общего и специального (прикладного) программного обеспечения для решения задач обработки персональных данных с использованием средств автоматизации;
- организовывать разработку предложений по размещению (расположению) технических средств и систем ИСПДн, подлежащей приведению в соответствие требованиям безопасности информации;
- разрабатывать и представлять на утверждение руководителю предложения о назначении ответственных за защиту (обеспечение безопасности) персональных данных, обрабатываемой с использованием СВТ;
- определять порядок эксплуатации СВТ и СЗИ;
- организовывать разработку разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн, подлежащей приведению в соответствие по требованиям безопасности информации;
- организовывать работу по категорированию персональных данных и классификации ИСПДн;
- организовывать разработку технического паспорта объекта информатизации;
- организовывать разработку организационно-методических документов (инструкций, памяток и т.п.) по защите персональных данных, обрабатываемой с использованием СВТ;
- участвовать в проведении аттестационных испытаний ИСПДн (при необходимости таких);
- организовывать периодический контроль работоспособности СЗИ, применяемых на объекте информатизации;
- контролировать выполнение правил разграничения доступа к техническим средствам и персональным данным на объекте информатизации;
- контролировать установленный порядок обращения с учтенными съемными машинными носителями персональных данных и бумажными носителями информации;
- контролировать выполнение комплекса мероприятий по защите ИСПДн от компьютерных "вирусов";
- осуществлять организацию специальной подготовки должностных лиц (в том числе в системе дополнительного профессионального образования), ответственных за эксплуатацию объекта информатизации, по вопросам обеспечения безопасности информации.

Администратор безопасности ИСПДн отвечает за соблюдение на объекте информатизации требований по обеспечению безопасности информации, порядка обращения с машинными носителями информации и правильность применения средств защиты персональных данных от НСД.

Администратор безопасности ИСПДн назначается из состава сотрудников подразделения по защите информации или сотрудников подразделения, ответственного за эксплуатацию ИСПДн, прошедших специальную подготовку.

Он обязан:

- разрабатывать предложения по составу общесистемных программных средств, обеспечивающих функционирование ИСПДн;
- разрабатывать предложения по разграничению доступа к информационным ресурсам, программным и техническим средствам ИСПДн;
- определять класс ИСПДн;
- участвовать и контролировать проведение аттестационных испытаний ИСПДн (при необходимости аттестации);
- знать способы, методы и средства защиты информации, обрабатываемой в ИСПДн, от НСД;
- знать перечень задач, решаемых с использованием средств автоматизации, и пользователей, допущенных к их решению;
- вести технический паспорт объекта информатизации;
- осуществлять допуск пользователей к техническим средствам ИСПДн и информации в соответствии с разрешительной системой доступа;
- вести учет разрешений на автоматизированную обработку информации;
- ежеквартально проводить занятия с пользователями ИСПДн, доводить основные положения нормативных, правовых и руководящих документов по вопросам защиты (обеспечению безопасности) персональных данных;
- контролировать ведение «Журнала учета лиц, допущенных к работе с персональными данными в ИСПДн»;
- еженедельно проверять системный журнал регистрации событий на предмет попыток НСД к информации;
- контролировать своевременность представления списков пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними паролей, а также прав пользования ресурсами СВТ;
- обеспечивать (осуществлять) смену и ввод пароля для разграничения доступа к информационным ресурсам пользователей с периодичностью не реже одного раза в квартал;
- периодически, но не реже двух раз в год, тестировать все функции системы разграничения доступа к информации, обрабатываемой в ИСПДн;
- осуществлять визуальный контроль целостности компонентов СВТ, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;
- осуществлять проверку ИСПДн на наличие компьютерных "вирусов";
- своевременно обновлять базы антивирусных программ;
- контролировать правильность применения и работоспособность средств защиты информации от НСД на объекте информатизации;
- вести учет, хранение, закрепление и выдачу паролей доступа к техническим средствам и информационным ресурсам ИСПДн;

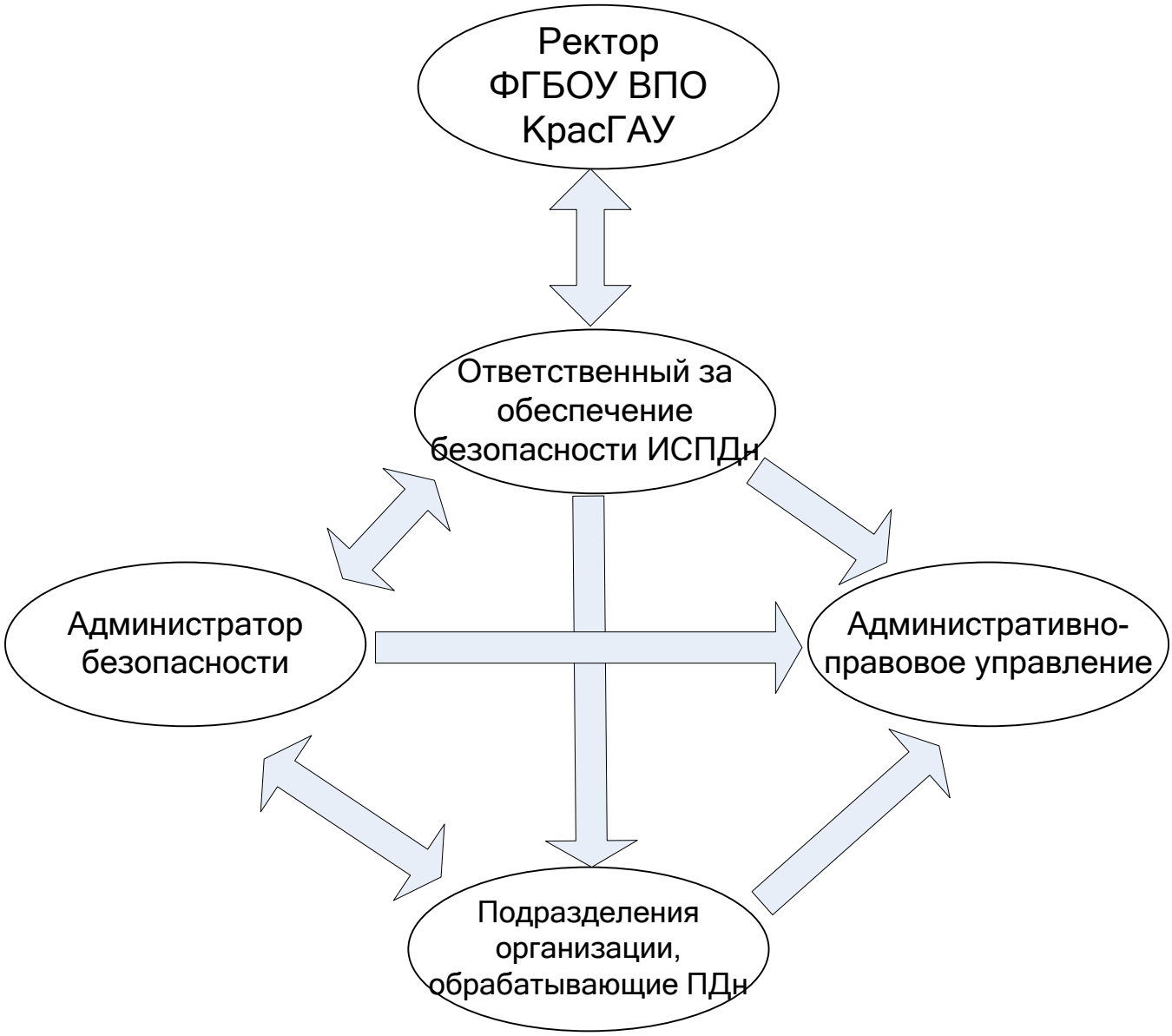
- докладывать руководителю подразделения, ответственного за эксплуатацию объекта информатизации, о нарушениях или невыполнении пользователями ИСПДн требований по защите (обеспечению безопасности) персональных данных и правил обращения со съемными машинными носителями информации;
- регулярно создавать резервные копии системных файлов и обрабатываемых данных, подлежащих хранению, на специально учтенных съемных машинных носителях информации;
- в своей работе руководствоваться требованиями «Инструкции администратора безопасности ИСПДн».

Ответственный за эксплуатацию ИСПДн (пользователь ИСПДн) отвечает за техническое состояние ИСПДн, установленный порядок использования программного обеспечения, а также применение технических и программных СЗИ.

Он обязан:

- знать требования руководящих документов по защите (обеспечению безопасности) информации и Положения;
- осуществлять работы в ИСПДн только после получения разрешения на автоматизированную обработку информации. Допуск пользователей для работы в ИСПДн осуществляется на основании утвержденного ректором ФГБОУ ВПО КрасГАУ «Перечня подразделений и работников, допущенных к работе с персональными данными в ИСПДн»;
- использовать для работы только учтенные съемные машинные носители персональных данных;
- соблюдать утвержденную разрешительную систему доступа к техническим средствам и информации, обрабатываемой в ИСПДн;
- передавать СВТ по журналу приема-передачи сотрудникам, допущенным к работе в ИСПДн, и по окончании работ принимать СВТ обратно, проверяя наличие и целостность печатей и защитных знаков на технических средствах ИСПДн;
- осуществлять визуальный контроль целостности компонентов СВТ, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;
- по окончании обработки персональных данных произвести стирание остаточной информации на несъемных машинных носителях информации и в оперативной памяти;
- докладывать администратору безопасности ИСПДн и информировать руководителя подразделения, ответственного за эксплуатацию объекта информатизации, о выявленных изменениях в конфигурации технических средств и программного обеспечения ИСПДн;
- немедленно докладывать администратору безопасности ИСПДн и информировать руководителя подразделения, ответственного за эксплуатацию объекта информатизации, о фактах и попытках НСД к обрабатываемой (хранящейся) в ИСПДн информации.
- при обработке персональных данных в ИСПДн выполнять требования «Инструкции пользователя, обрабатывающего персональные данные в ИСПДн».

4.2. Структурная схема взаимодействия подразделений, решающих задачи по защите (обеспечению безопасности) информации в ФГБОУ ВПО КрасГАУ



5. КОНТРОЛЬ ВЫПОЛНЕНИЯ КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ (ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ) ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМОЙ С ИСПОЛЬЗОВАНИЕМ СВТ В ФГБОУ ВПО КРАСГАУ

5.1. Установленный порядок организации и проведения контроля обеспечения безопасности персональных данных при их обработке с использованием СВТ в ФГБОУ ВПО КрасГАУ уполномоченными федеральными органами

Контроль за обеспечением режима безопасности при обработке персональных данных в ФГБОУ ВПО КрасГАУ осуществляется в целях изучения и оценки фактического состояния обеспечения защиты персональных данных, выявления недостатков и нарушений и выработки предложений, направленных на их устранение и предотвращение.

Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации (требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных), осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

5.2. Порядок проведения объектового контроля организации защиты (обеспечения безопасности) персональных данных, обрабатываемых с использованием СВТ

Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в структурных подразделениях ФГБОУ ВПО КрасГАУ;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн организации;
- разработка предложений по устранению демаскирующих признаков и технических каналов утечки информации.

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических средств воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации, на предприятии ФГБОУ ВПО КрасГАУ организован контроль состояния и эффективности защиты информации, который включает в себя:

- проверку по действующим методикам выполнения требований нормативных документов организационно-технического характера по защите информации (в том числе и настоящей инструкции), а также в оценке обоснованности и эффективности принятых мер;
- проверку выполнения принятых мер защиты информации;
- проверку выполнения норм эффективности защиты информации по действующим методикам с применением контрольно-измерительной аппаратуры и сертифицированных программных средств контроля;
- тестирование всех функций СЗИ от НСД согласно Приказу ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- проверку работоспособности и правильности эксплуатации СЗИ;
- проверку выполнения требований предписания на эксплуатацию (в случае необходимости);
- проверку срока действия сертификатов на средства защиты информации;
- оценку эффективности принятых мер защиты информации от утечки за счет ПЭМИН (при актуальной угрозе утечки информации за счет ПЭМИН);
- проверку соответствия состава и структуры программно-аппаратных средств ИСПДн представленной документации;
- проверку работоспособности и правильности настроек СЗИ;
- проверку целостности пломбирования объекта информатизации;
- проверку соответствия описанного в документации технологического процесса реальному.

Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах организации.

Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию ректора ФГБОУ ВПО КрасГАУ проводится расследование.

Для проведения расследования назначается комиссия, которая должна установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению.

Начальник административно-правового управления Р.В. Демин

ЛИСТ ОЗНАКОМЛЕНИЯ

ФИО	Должность	Роспись	Дата
1	2	3	4

ПРИМЕЧАНИЕ: Лист ознакомления не может заменяться на новый, а может только продолжаться путем вклейки его продолжений.

Лист регистрации изменений и дополнений

Изм.	Номера листов				Указание об изменении (N вх. докум.)	Подпись исполнителя	Дата
	изменя-емых	заменя-емых	новых	аннули-рованных			
1	2	3	4	5	6	7	8

ПРИМЕЧАНИЕ: Лист регистрации изменений и дополнений не может заменяться на новый, а может только продолжаться путем вклейки его продолжений.

Приложение 1
Ф О Р М А

УТВЕРЖДАЮ
Руководитель предприятия: ____
_____

_____ И.О. Фамилия
«___»_____ 20__г.

План мероприятий по защите персональных данных при их обработке в ИСПДн

_____

(наименование ИСПДн)

№ п/п	Мероприятие	Исполнители	Сроки	Отметка о выполнении
1	Ревизия информационных ресурсов предприятия на предмет содержания в них ПДн	Ответственный за ОБПДн		
2	Разработка перечня персональных данных, обрабатываемых в ИСПДн	Ответственный за ОБПДн		
3	Разработка и утверждение списка лиц, подлежащих допуску к обработке ПДн	Ответственный за ОБПДн		
4	Проведение классификации ИСПДн. Разработка и утверждение акта классификации ИСПДн предприятия	Комиссия		
5	Расчет исходной защищенности ИСПДн предприятия	Ответственный за ОБПДн		
6	Разработка частной модели угроз безопасности ПДн обрабатываемых в ИСПДн	Ответственный за ОБПДн		
7	Разработка на основе модели угроз подсистем защиты персональных данных для каждой ИСПДн: а) Постановка требований к защите ПДн. б) Принятие решений о целесообразности применения существующих в __ средств защиты информации от несанкционированного доступа. в) Принятие решений о целесообразности закупки недостающих средств защиты информации от несанкционированного доступа. г) Принятие решений о целесообразности привлечения сторонних организаций для создания подсистем защиты персональных данных для ИСПДн. д) Принятие решений о целесообразности дополнительных организационных мер по защите информации от несанкционированного доступа.	Ответственный за ОБПДн		
8	Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации	Ответственный за ОБПДн		
9	Изучение и эксплуатация средств защиты информации от НСД сотрудниками, обрабатывающими персональные данные	Ответственный за ОБПДн, Ответственный за эксплуатацию ИСПДн		
10	Создание журнала учета лиц, допущенных к работе с персональными данными в ИСПДн, содержащего в т.ч. копии приказов о допуске лиц к работе в ИСПДн	Ответственный за ОБПДн		
11	Установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией, контроль принятия организационных мер.	Администратор безопасности		

12	Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними. а) Проведение занятий с сотрудниками подразделений по работе с подсистемами защиты информации в ИСПДн. б) Подготовка инструкций по работе с подсистемами защиты информации ИСПДн (в т.ч. включающих организационные меры).	Администратор безопасности		
13	Создание журнала учета средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных для последующего учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.	Администратор безопасности		
14	Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией: а). Создание журнала проверок. б) Утверждение плана проверок АРМ сотрудников на предмет соблюдения конфиденциальности ПДн. в) Контроль электронного журнала обращений к ПДн и проведение проверок сотрудников в соответствии с планом проверок.	Администратор безопасности		
15	Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.	Ответственный за ОБПДн, Администратор безопасности		
16	Описание подсистем защиты персональных данных для каждой ИСПДн	Администратор безопасности		
17	Оценка соответствия ИСПДн по требованиям безопасности	Организация, имеющая лицензии на деятельность по технической защите конфиденциальной информации	По мере необходимости	

Приложение 2
Ф О Р М А

УТВЕРЖДАЮ
Руководитель предприятия: ____
_____

_____ И.О. Фамилия
«___»_____ 20__г.

План внутренних проверок состояния защиты персональных данных в ИСПДн

_____

(наименование ИСПДн)

№ п/п	Мероприятие	Исполнители	Сроки	Отметка о выполнении
1	Проверка выполнения принятых мер защиты информации			
2	Тестирование всех функций СЗИ от НСД согласно Приказу ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».			
3	Проверка правильности настройки СЗИ			
4	Проверка работоспособности и правильности эксплуатации СЗИ			
5	Проверка выполнения требований предписания на эксплуатацию (в случае необходимости)			
6	Проверка сертификатов на средства защиты информации			
7	Оценка эффективности принятых мер защиты информации от утечки за счет ПЭМИН			
8	Проверка соответствия состава и структуры программно-аппаратных средств ИСПДн информации в техническом паспорте на ИСПДн;			
9	Проверка целостности пломбирования объекта информатизации			
10	Проверка правильности ведения журналов на ОИ			
11	Проведение занятий с пользователями ИСПДн, доведение до них основных положений нормативных, правовых и руководящих документов по вопросам защиты (обеспечению безопасности) персональных данных			
12	Проверка соответствия описанного в документации технологического процесса реальному.			
13	Проверка системного журнала регистрации событий на предмет попыток НСД к информации			
14	Проверка смены паролей для разграничения доступа к информационным ресурсам пользователей			
15	Проверка обновлений баз антивирусных программ			
16	Проверка осуществления резервирования системных файлов и обрабатываемых данных			

Уч. ПД/31к, 25.03.2014
Отп. 1 экз.
ПЭВМ-6, б/ч
Экз. № 1 – г. Красноярск, ФГБОУ ВПО КрасГАУ.
Исп. отп., Соловей Н.С., 25.03.2014.
Тел. (391) 223-20-50, доб. 103