

Министерство сельского хозяйства Российской Федерации  
Департамент научно-технологической политики и образования  
*Федеральное государственное бюджетное образовательное учреждение  
высшего образования*  
**«Красноярский государственный аграрный университет»**

УТВЕРЖДАЮ:

Директор института

\_\_\_\_\_ Шапорова З.Е.

«21» \_\_\_\_\_ марта \_\_\_\_\_ 2023 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**  
(текущего оценивания, промежуточной аттестации)

Институт экономики и управления АПК

Кафедра Информационные технологии и математическое обеспечение ин-  
формационных систем

Наименование и код ОПОП: **09.02.07** «Информационные системы и про-  
граммирование»

Дисциплина:

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Красноярск 2023



**ДОКУМЕНТ ПОДПИСАН  
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ  
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

ВЫДАННОЙ: ФГБОУ ВО КРАСНОЯРСКИЙ ГАУ  
ВЛАДЕЛЕЦ: РЕКТОР ПЫЖИКОВА Н.И.  
ДЕЙСТВИТЕЛЕН: 16.03.2023 - 08.06.2024

Составитель: Титовская Н.В., канд. техн. наук, доцент  
(ФИО, ученая степень, ученое звание)

\_\_\_\_\_ «20» марта 2023г.

ФОС разработан в соответствии с рабочей программой дисциплины: Информационная безопасность

ФОС обсужден на заседании кафедры «Информационные технологии и математическое обеспечение информационных систем»

\_\_\_\_\_ протокол № 7 «20» марта 2023г.

Зав. кафедрой ИТ и МОИС Бронов С.А., д.т.н., доцент

\_\_\_\_\_ «20» марта 2023г.

ФОС принят методической комиссией института  
Экономики и управления АПК \_\_\_\_\_ протокол № 7 «21» марта 2023г.

Председатель методической комиссии

Рожкова А.В., ст. преподаватель \_\_\_\_\_ «21» марта 2023г

## Содержание

1	Цель и задачи фонда оценочных средств.....	4
2	Нормативные документы.....	4
3	Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины. Формы контроля формирования компетенций. ....	4
4	Показатели и критерии оценивания компетенций.....	5
5	Фонд оценочных средств.....	7
5.1	Фонд оценочных средств для текущего контроля.....	7
5.1.1	Оценочное средство (опрос). Критерии оценивания. ....	7
5.2	Фонд оценочных средств для промежуточного контроля.....	9
5.2.1	Оценочное средство зачет с оценкой (итоговое тестирование). Критерии оценивания.....	9
6	Учебно-методическое и информационное обеспечение дисциплины.....	13
6.1	Основная литература.....	13
6.2	Дополнительная литература.....	13
6.3	Методические указания, рекомендации и другие материалы к занятиям.....	13
6.4	Программное обеспечение.....	13
6.5	Интернет-ресурсы, электронные библиотечные системы.....	13

## 1 Цель и задачи фонда оценочных средств

**Целью** создания ФОС дисциплины «Информационная безопасность» является установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательных программ и рабочих программ модулей.

ФОС по дисциплине решает задачи:

- контроль и управление процессом приобретения студентами необходимых знаний, умений, навыков и уровня сформированности компетенций, определённых в ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование»;
- контроль и управление достижением целей реализации ОПОП, определенных в виде набора общих и профессиональных компетенций выпускников;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс университета.

**Назначение** фонда оценочных средств:

Используется для оперативного и регулярного управления учебной деятельностью студентов. А также предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины «Информационная безопасность» в установленной учебным планом форме в 6 семестре – зачетом с оценкой.

## 2 Нормативные документы

ФОС разработан на основе ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование», рабочей программы дисциплины «Информационная безопасность».

## 3 Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины. Формы контроля формирования компетенций.

Компетенция	Этап формирования компетенции	Образовательные технологии	Тип контроля	Форма контроля
ОК 01. - Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	теоретический (информационный)	лекции	текущий	Опрос
	практико-ориентированный	практические занятия	текущий	Опрос
	оценочный	аттестация	промежуточный	Зачет с оценкой
ОК 02. - Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	теоретический (информационный)	лекции	текущий	Опрос
	практико-ориентированный	практические занятия	текущий	Опрос
	оценочный	аттестация	промежуточный	Зачет с оценкой
ОК 09. - Пользоваться профессиональной документацией на государственном и иностранном языках.	теоретический (информационный)	лекции	текущий	Опрос
	практико-ориентированный	практические занятия	текущий	Опрос
	оценочный	аттестация	промежуточный	Зачет с оценкой
ПК 5.3. - Разрабатывать подсистемы безопасности информационной системы	теоретический (информационный)	лекции	текущий	Опрос
	практико-	практические	текущий	Опрос

в соответствии с техническим заданием	ориентированный	занятия		
	оценочный	аттестация	промежуточный	Зачет с оценкой
ПК 6.4. - Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания	теоретический (информационный)	лекции	текущий	Опрос
	практико-ориентированный	практические занятия	текущий	Опрос
	оценочный	аттестация	промежуточный	Зачет с оценкой
ПК 7.5. - Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации	теоретический (информационный)	лекции	текущий	Опрос
	практико-ориентированный	практические занятия	текущий	Опрос
	оценочный	аттестация	промежуточный	Зачет с оценкой

#### 4 Показатели и критерии оценивания компетенций

Таблица 4.1 – Показатели и критерии оценки результатов обучения

Показатель оценки результатов обучения	Критерий оценки результатов обучения
ОК 01. - Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	
Высокий уровень	<b>Практический опыт:</b> Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
Продвинутый уровень	<b>Умения:</b> распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
Пороговый уровень	<b>Знания:</b> актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02. - Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	
Высокий уровень	<b>Практический опыт:</b> Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Продвинутый уровень	<b>Умения:</b> определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска;

	структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска. Применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; Использовать информационные технологии в профессиональной деятельности.
Пороговый уровень	<b>Знания:</b> номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации. Современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности основные виды информационных технологий, используемых в профессиональной деятельности
ОК 09. - Пользоваться профессиональной документацией на государственном и иностранном языках	
Высокий уровень	<b>Практический опыт:</b> Использовать информационные технологии для оформления профессиональной документации
Продвинутый уровень	<b>Умения:</b> Пользоваться профессиональной документацией на государственном и иностранном языках: заполнять и оформлять профессиональную документацию на государственном и иностранном языках. понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
Пороговый уровень	<b>Знания:</b> правила построения простых и сложных предложений на профессиональные темы; основные общепотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; знать приемы и способы заполнения и оформления профессиональной документации на государственном и иностранном языках. правила чтения текстов профессиональной направленности на государственном и иностранном языках
ПК 5.3. - Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	
Высокий уровень	<b>Практический опыт:</b> Управлять процессом разработки приложений с использованием инструментальных средств. Модифицировать отдельные модули информационной системы.

Продвинутый уровень	<b>Умения:</b> Создавать и управлять проектом по раз работке приложения и формулировать его задачи.
Пороговый уровень	<b>Знания:</b> Национальной и международной системы стандартизации и сертификации и систему обеспечения качества продукции. Методы контроля качества объектно - ориентированного программирования. Объектно-ориентированное программирование. Спецификации языка программирования, принципы создания графического пользовательского интерфейса (GUI), файлового ввода-вывода, создания сетевого сервера и сетевого клиента
ПК 6.4. - Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания	
Высокий уровень	<b>Практический опыт:</b> Выполнять оценку качества и надежности функционирования информационной системы на соответствие техническим требованиям.
Продвинутый уровень	<b>Умения:</b> Применять документацию систем качества. Применять основные правила и документы системы сертификации РФ.
Пороговый уровень	<b>Знания:</b> Характеристики и атрибуты качества ИС. Методы обеспечения и контроля качества ИС в соответствии со стандартами. Политику безопасности в современных информационных системах.
ПК 7.5. - Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации	
Высокий уровень	<b>Практический опыт:</b> Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.
Продвинутый уровень	<b>Умения:</b> Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных. Владеть технологиями проведения сертификации программного средства.
Пороговый уровень	<b>Знания:</b> Технология установки и настройки сервера баз данных. Требования к безопасности сервера базы данных. Государственные стандарты и требования к обслуживанию баз данных.

Таблица 4.2 – Шкала оценивания

Показатель оценки результатов обучения	Шкала оценивания
Пороговый уровень	60-72 баллов (удовлетворительно)
Продвинутый уровень	73-86 баллов (хорошо)
Высокий уровень	87-100 баллов (отлично)

## 5 Фонд оценочных средств.

### 5.1 Фонд оценочных средств для текущего контроля

Текущий контроль используется для оперативного и регулярного управления учебной деятельностью студентов. В условиях рейтинговой системы контроля результаты текущего оценивания студента используются как показатель его текущего рейтинга. Текущий контроль успеваемости студентов включает в себя опрос по всем темам курса.

#### 5.1.1 Оценочное средство (опрос). Критерии оценивания.

##### Перечень вопросов :

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
2. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.
3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
4. Законодательный уровень информационной безопасности. Обзор зарубежного зако-

- нодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.
5. Международные стандарты информационного обмена. Стандарт ISO/IEC15408.
  6. Российские стандарты защищенности автоматизированных систем.
  7. Основные положения теории информационной безопасности. Модели безопасности и их применение.
  8. Информационная безопасность в условиях функционирования в России глобальных сетей.
  9. Виды противников или "нарушителей". Понятия о видах вирусов Виды возможных нарушений информационной системы. Виды защиты.
  10. Файловые вирусы.
  11. Загрузочные вирусы.
  12. Вирусы и операционные системы.
  13. Методы и средства борьбы с вирусами.
  14. Профилактика заражения вирусами компьютерных систем.
  15. Защита информации от случайных угроз.
  16. Дублирование информации. RAID - массивы
  17. Повышение надежности компьютерных систем.
  18. Обеспечение отказоустойчивости компьютерных систем.
  19. Блокировка ошибочных операций.
  20. Защита информации от традиционного шпионажа и диверсий.
  21. Система охраны объектов компьютерных систем.
  22. Организация работы с конфиденциальными информационными ресурсами.
  23. Противодействие подслушиванию и наблюдению в оптическом диапазоне.
  24. Средства борьбы с закладными подслушивающими устройствами.
  25. Защита от злоумышленных действий обслуживающего персонала и пользователей.
  26. Средства защиты компьютеров. Программно аппаратные методы и средства ограничения доступа к компонентам компьютера. Типы несанкционированного доступа и условия работы средств защиты.
  27. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.
  28. Защита от несанкционированного копирования программного обеспечения.
  29. Методы криптографии
  30. Основные понятия шифрования.
  31. Методы шифрования с симметричным ключом.
  32. Системы шифрования с открытым ключом.
  33. Стандарты шифрования.
  34. Промышленные программные средства Kerberos, PGP.
  35. Методы и средства хранения ключевой информации. Анализ программных реализаций.
  36. Защита от разрушающих программных воздействий.
  37. Основные технологии построения защищенных ЭИС.
  38. Системные вопросы защиты программ и данных.
  39. Основные категории требований к средствам обеспечения информационной безопасности
  40. Место информационной безопасности экономических систем в национальной безопасности страны
  41. Безопасность платежных систем в среде Интернет.
  42. Аналитические методы шифрования.
  43. Программные закладки
  44. Организационные методы защиты информации
  45. Электронно-цифровая подпись.
  46. Этапы враждебного воздействия
  47. Кодирование информации
  48. Методы враждебного воздействия

### Критерии оценивания:

По итогам опроса студент получает баллы, количество которых рассчитывается по формуле

$$N = \frac{P}{S} \times M$$



где N – количество баллов, получаемых студентом, P – количество вопросов, на которые студент дал правильные ответы, S – общее количество вопросов, заданных студенту в ходе опроса. M – количество баллов за опрос для конкретного модуля.

Всего в ходе текущего контроля (опрос) студент может набрать максимум 60 баллов.

## 5.2 Фонд оценочных средств для промежуточного контроля

Промежуточная аттестация – зачет с оценкой проводится в форме итогового тестирования.

### 5.2.1 Оценочное средство зачет с оценкой (итоговое тестирование). Критерии оценивания

#### Примеры тестовых вопросов/заданий

№	Вопрос	Ответ
1	Что такое идентификация	Присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информации
2	Что такое конфиденциальность	Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные
3	Что такое аутентификация	Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы
4	Что такое угроза	Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы
5	Что такое информационная безопасность	Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам или пользователям информации
6	Программная закладка - это	Специально скрытно внедренная в защитную систему программа, позволяющая злоумышленнику путем модификации свойств системы защиты осуществлять несанкционированный доступ к тем или иным ресурсам систем
7	Установите соответствие : 1. Доступность 2. Атака 3. Защита информации 4. Угроза 5. Аутентификация А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы Б) Комплекс мероприятий, направленных на обеспечение ИБ Д) Реализованная угроза	1-г, 2-д, 3-б, 4-а, 5-в

	<p>Г) Гарантия того, что авторизованные пользователи всегда получают доступ к данным</p> <p>В) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы</p>	
8	<p>Установите соответствие.</p> <ol style="list-style-type: none"> <li>1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов</li> <li>2. метод несанкционированного доступа к электронной почте</li> <li>3. метод несанкционированного доступа к ресурсам системы рассылки новостей USENET</li> <li>4. метод несанкционированного доступа к клиентскому программному обеспечению www <ol style="list-style-type: none"> <li>а) переполнение буфера с разрушением области кодов</li> <li>б) выведение из строя серверов сети internet</li> <li>в) перехват электронной почты</li> <li>г) использование постоянно поступающей информации</li> </ol> </li> </ol>	1-б, 2-в, 3-г, 4-а
9	<p>Комплексная защита информации - это</p>	<p>Целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации</p>
10	<p>Установите соответствие между типами взаимосвязей и их характеристиками:</p> <ol style="list-style-type: none"> <li>1. Целостность</li> <li>2. Идентификация</li> <li>3. Угроза</li> <li>4. Конфиденциальность</li> <li>5. Аутентификация</li> </ol> <p>А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы</p> <p>Б) Гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными)</p> <p>В) Присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информации</p> <p>Г) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы</p> <p>Д) Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо об-</p>	1-б, 2-в, 3-а, 4-д, 5-г

	разом изменять, модифицировать, разрушать или создавать данные	
11	Использование управляющих сообщений - метод ... эффективности работы сети на уровне транспортных и коммуникационных протоколов	снижения
12	Укажите все правильные ответы К методам выведения из строя серверов сети internet относится: 1) перехват электронной почты 2) получение списка пользователей сервера 3) пересылка файлов, которые приводят к краху программ-браузеров 4) перехват номеров кредитных карточек	2, 3
13	Создание паразитного трафика - метод ... доступа к электронной почте	несанкционированного
14	Что такое информационная безопасность?	Информационная безопасность - это защита информации от угроз и рисков, связанных с ее хранением, передачей и обработкой.
15	Что такое угрозы информационной безопасности?	Угрозы информационной безопасности - это действия или события, которые могут привести к нарушению целостности, конфиденциальности или доступности информации.
16	Что такое многопользовательские системы?	Многопользовательские системы - это системы, которые позволяют нескольким пользователям работать с одним и тем же компьютером или сетью.
17	Что такое пароль?	Пароль - это секретная строка символов, используемая для аутентификации пользователя.
18	Что такое аутентификация?	Аутентификация - это процесс проверки подлинности пользователя или устройства.
19	Что такое авторизация?	Авторизация - это процесс проверки прав доступа пользователя к ресурсам системы.
20	Что такое двухфакторная аутентификация?	Двухфакторная аутентификация - это метод аутентификации, при котором используются два различных фактора подтверждения личности пользователя.
21	Что такое шифрование данных?	Шифрование данных - это процесс преобразования информации в зашифрованный вид, который может быть прочитан только с помощью ключа.
22	Что такое открытый ключ?	Открытый ключ - это ключ, который может быть свободно распространен, и используется для шифрования сообщений.
23	Что такое закрытый ключ?	Закрытый ключ - это ключ, который является секретным и используется для расшифровки сообщений.
24	Что такое атака методом перебора?	Атака методом перебора - это метод

		криптоанализа, при котором все возможные комбинации ключей перебираются до тех пор, пока не будет найден правильный ключ.
25	Что такое фишинг?	Фишинг - это мошенническая попытка получить конфиденциальную информацию, такую как пароли и номера кредитных карт, путем подделки электронного сообщения или веб-сайта.
26	Что такое вирус?	Вирус - это программное обеспечение, которое может внедряться в компьютер и копировать себя.
27	Что такое бэкдор?	Бэкдор - это специальная программа, которая позволяет злоумышленнику получить несанкционированный доступ к компьютерной системе.
28	Что такое защита периметра?	Защита периметра - это защита сети от угроз путем настройки брандмауэра и других устройств на границе сети.
29	Что такое защита конечных точек?	Защита конечных точек - это защита компьютеров и других устройств от угроз, связанных с их использованием в сети.
30	Что такое DDoS-атака?	DDoS-атака - это атака на компьютерную систему, при которой злоумышленник пытается перегрузить систему, отправляя ей большое количество запросов.

Банк тестовых заданий в полном объеме размещен в ЭИОС Красноярского ГАУ на платформе LMS Moodle по адресу <https://e.kgau.ru>

### Критерии оценивания:

По итогам тестирования студент получает дополнительно баллы, количество которых рассчитывается по формуле

$$N = \frac{P}{S} \times 40$$

где N – количество баллов, получаемых студентом, P – количество вопросов, на которые студент дал правильные ответы, S – общее количество вопросов, заданных студенту в ходе тестирования.

Баллы, полученные на итоговом тестировании, суммируются с баллами, полученными в течение семестра на текущей аттестации, и выводится итоговая оценка по следующим критериям:

60 – 73 – минимальное количество баллов – оценка «удовлетворительно».

74 – 86 – среднее количество баллов – оценка «хорошо».

87 – 100 – максимальное количество баллов – оценка «отлично».

Студент, не набравший минимальное количество баллов, отрабатывает текущие задолженности, готовя ответы на вопросы по темам задолженности в письменном виде

Обучающийся, не сдавший зачет с оценкой, приходит на пересдачу в сроки в соответствии с графиком ликвидации академических задолженностей: [http://www.kgau.ru/new/news/news/2017/grafik\\_lz.pdf](http://www.kgau.ru/new/news/news/2017/grafik_lz.pdf).

## **6 Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература**

1. *Казарин, О. В.* Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/475889>
2. *Внуков, А. А.* Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/475890>

### **6.2 Дополнительная литература**

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2021. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/470351>

### **6.3 Методические указания, рекомендации и другие материалы к занятиям**

Титовский С.Н., Титовская Н.В. Информационная безопасность. Электронный обучающий ресурс. <http://e.kgau.ru/course/view.php?id=1051>

### **6.4 Программное обеспечение**

1. Операционная система Windows (академическая лицензия № 44937729 от 15.12.2008).
2. Офисный пакет приложений Microsoft Office (академическая лицензия № 44937729 от 15.12.2008).
3. Программа для создания и просмотра электронных публикаций в формате PDF; Acrobat Professional (образовательная лицензия № CE0806966 от 27.06.2008).
4. Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 1000-1499 Node 2 year Educational License (1B08-230201-012433-600-1212 с 01.02.2023 до 09.02.2024).
5. Moodle 3.5.6a (система дистанционного образования) - Открытые технологии договор 969.2 от 17.04.2020.
6. Библиотечная система «Ирбис 64», контракт 37–5–20 от 27.10.2020
7. Python - среда программирования, свободно распространяемое ПО
8. Visual Studio Community – бесплатная среда разработки программного обеспечения на C++
9. PGP Freeware, бесплатно распространяемое ПО
10. Ad Muncher, бесплатно распространяемое ПО
11. Malwarebytes AdwCleaner, бесплатно распространяемое ПО
12. Ad-Aware, бесплатно распространяемое ПО
13. SUPERAntiSpyware, бесплатно распространяемое ПО
14. Ghostery, бесплатно распространяемое ПО
15. Spyware Terminator, бесплатно распространяемое ПО
16. Spyware Process Detector, бесплатно распространяемое ПО

### **6.5 Интернет-ресурсы, электронные библиотечные системы.**

*Интернет-ресурсы*

1. Национальный Открытый Университет «ИНТУИТ» <https://intuit.ru/>
2. Портал CIT Forum <http://citforum.ru/>
3. Информационно-аналитическая система «Статистика» <http://www.ias-stat.ru/>

#### *Электронные библиотечные системы*

4. Каталог библиотеки Красноярского ГАУ -- [www.kgau.ru/new/biblioteka/](http://www.kgau.ru/new/biblioteka/) ;
5. Центральная научная сельскохозяйственная библиотека - [www.cnshb.ru/](http://www.cnshb.ru/) ;
6. Научная электронная библиотека "eLibrary.ru" – [www.elibrary.ru](http://www.elibrary.ru) ;
7. Электронная библиотечная система «Лань» - <https://e.lanbook.com/>
8. Электронно-библиотечная система «Юрайт» - <https://urait.ru/>
9. Электронно-библиотечная система «AgriLib» - <http://ebs.rgazu.ru/>
10. Электронная библиотека Сибирского Федерального университета - <https://bik.sfu-kras.ru/>
11. Национальная электронная библиотека - <https://rusneb.ru/>
12. Электронная библиотечная система «ИРБИС64+» - [http://5.159.97.194:8080/cgi-bin/irbis64r\\_plus/cgiirbis\\_64\\_ft.exe?C21COM=F&I21DBN=IBIS\\_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5](http://5.159.97.194:8080/cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5)
13. Электронный каталог Государственной универсальной научной библиотеки Красноярского края - <https://www.kraslib.ru/>

#### *Информационно-справочные системы*

14. справочно-правовая система КонсультантПлюс  
<http://www.consultant.ru/cons/cgi/online.cgi?req=home;rnd=0.8636296761039928>
15. Информационно-правовой портал «Гарант». <http://www.garant.ru/>

#### *Профессиональные базы данных*

16. Коллективный блог по информационным технологиям, бизнесу и интернету. <https://habr.com/ru/>
17. Форум программистов и сисадминов Киберфорум <https://www.cyberforum.ru/>

#### *Сторонние электронно-образовательные ресурсы*

18. Министерство науки и высшего образования РФ
19. Российское образование
20. Единое окно доступа к образовательным ресурсам
21. Единая коллекция цифровых образовательных ресурсов
22. Федеральный центр информационно-образовательных ресурсов
23. Современная цифровая образовательная среда в РФ <http://window.edu.ru/>
24. [http://window.edu.ru/catalog/resources?p\\_rubr=2.2.75.6](http://window.edu.ru/catalog/resources?p_rubr=2.2.75.6)

## ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

на фонды оценочных средств по дисциплине «Информационная безопасность»  
для подготовки специалистов среднего звена по программе ФГОС СПО,  
специальность 09.02.07 «Информационные системы и программирование»  
ФГБОУ ВО Красноярский государственный аграрный университет

Представленные на рецензию фонды оценочных средств оформлены с соблюдением всех требований, предъявляемых к оформлению ФОС по стандартам ФГОС СПО.

Дисциплина «Информационная безопасность» является частью учебного плана по подготовке специалистов среднего звена по программе ФГОС СПО, специальность 09.02.07 «Информационные системы и программирование»

Оценочные средства для контроля успеваемости студентов представлены в полном объеме. При помощи фонда оценочных средств осуществляется контроль и управление процессом приобретения студентами необходимых знаний, умений, практического опыта и компетенций, определенных ФГОС СПО.

Представленные оценочные средства по дисциплине стимулируют познавательную деятельность за счет заданий разного уровня сложности, компетентного подхода, формируют навыки само- и взаимопонимания.

Фонды оценочных средств соответствуют обязательному минимуму содержания ФГОС СПО, обеспечивают проведение аттестации студентов учреждений СПО, дают возможность определить соответствие студентов конкретной характеристике.

Представленные ФОС для специальности 09.02.07 «Информационные системы и программирование» могут быть использованы в учебном процессе и соответствуют требованиям ФГОС СПО.

Эксперт:

доцент кафедры Вычислительной техники  
ФГАОУ ВО Сибирский федеральный университет,  
Институт космических и информационных  
технологий, канд. техн. наук



Постников  
Александр  
Иванович