ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом и.о. ректора
от «07» июня 2021 г. № 79

# Б1.О.23 Безопасность информационных технологий и систем

## рабочая программа дисциплины

Специальность/направление подготовки – 09.03.02 Информационные системы и технологии
Специализация/профиль – Информационные системы и технологии
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года; заочная форма 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 8
Часов по учебному плану (УП) – 288

Формы промежуточной аттестации
очная форма обучения:
зачет 6 семестр, экзамен 5 семестр, курсовая работа 6 семестр
заочная форма обучения:
зачет 4 курс, экзамен 4 курс, курсовая работа 4 курс

**Очная форма обучения** **Распределение часов дисциплины по семестрам**

| Семестр | 5 | 6 | **Итого** |
|---|---|---|---|
| Вид занятий | Часов по УП | Часов по УП | **Часов по УП** |
| **Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*** | 68 | 68 | **136** |
| – лекции | 34 | 34 | **68** |
| – практические (семинарские) | | | |
| – лабораторные | 34 | 34 | **68** |
| **Самостоятельная работа** | 40 | 76 | **116** |
| **Экзамен** | 36 | | **36** |
| **Итого** | 144 | 144 | **288** |

**Заочная форма обучения** **Распределение часов дисциплины по семестрам**

| Курс | 4 | **Итого** |
|---|---|---|
| Вид занятий | Часов по УП | **Часов по УП** |
| **Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*** | 34 | **34** |
| – лекции | 16 | **16** |
| – практические (семинарские) | | |
| – лабораторные | 18 | **18** |
| **Самостоятельная работа** | 232 | **232** |
| **Зачет** | 4 | **22** |
| **Экзамен** | 18 | **0** |
| **Итого** | 288 | **288** |

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 19.09.2017 № 926.

Программу составил(и):
к.ф.-м.н., доцент, А.А. Бутин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11/2

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

## 1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

**1.1 Цель дисциплины**

| | |
|---|---|
| 1 | ознакомление с правовыми, организационными, техническими, программно-аппаратными, криптографическими технологиями обеспечения безопасности информации при проектировании, построении и эксплуатации автоматизированных информационных систем (АИС) |

**1.2 Задачи дисциплины**

| | |
|---|---|
| 1 | определение места и роли технологий построения защищенных АИС в деятельности современной организации; |
| 2 | ознакомление с основными видами угроз информационной безопасности (ИБ) в АИС, причинами и каналами утечки информации; |
| 3 | изучение правовых и методических основ защиты информации (ЗИ); |
| 4 | освоение организационных, технических, программно-аппаратных и криптографических методов и средств обеспечения ИБ в АИС; |
| 5 | анализ рынка современных средств обеспечения ИБ в АИС |

**1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины**

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.
Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

## 2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

| | |
|---|---|
| Блок/часть ОПОП | Блок 1. Дисциплины / Обязательная часть |

**2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины**

| | |
|---|---|
| 1 | Б1.О.04 Философия |
| 2 | Б1.О.08 Информатика |
| 3 | Б1.О.11 Экономика |
| 4 | Б1.О.19 Теория информации |
| 5 | Б2.О.01(У) Учебная - ознакомительная практика |
| 6 | ФТД.01 Основы научных исследований |

**2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее**

| | |
|---|---|
| 1 | Б1.О.06 Правоведение |
| 2 | Б1.О.29 Технологии обработки информации |
| 3 | Б1.О.30 Методы и средства проектирования информационных систем и технологий |
| 4 | Б1.О.31 Анализ больших данных |
| 5 | Б1.О.33 Управление ИТ-проектами |
| 6 | Б2.О.04(Пд) Производственная - преддипломная практика |
| 7 | Б3.01(Д) Выполнение выпускной квалификационной работы |

## 3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения |
|---|---|---|
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знать: основные принципы и требования обеспечения ИБ; методики обнаружения уязвимостей АИС |
| | | Уметь: применять приемы тестирования уязвимостей корпоративных программно-технических сервисов современным аппаратом для количественной и качественной оценки результатов аудита |
| | | Владеть: навыками обнаружения уязвимостей АИС, участия в предпроектных и проектных работах при создании систем защиты информации |
| | ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знать: характеристики и возможности штатных (встроенных) и добавочных средств обеспечения ИБ |
| | | Уметь: произвести выбор необходимых средств ЗИ в зависимости от типа (природы) информационного риска в программном, программно-аппаратном или техническом исполнении |
| | | Владеть: навыками администрирования штатных подсистем и добавочных средств защиты информации |
| | ОПК-3.3 Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности | Знать: функциональные возможности представителей основных классов средств ЗИ |
| | | Уметь: оценивать состояние рынка современных программно-аппаратных средств обеспечения ИБ АС, готовить соответствующие обзоры |
| | | Владеть: навыками экономически обоснованного выбора и рационального использования средств обеспечения ИБ, составления соответствующего обоснования |
| УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1 Знает принципы сбора, отбора и обобщения информации | Знать: базовые методы поиска информации; основные понятия, определения, специальную терминологию в области ИБ |
| | | Уметь: выделять информацию в АИС, подлежащую защите от угроз ИБ |
| | | Владеть: навыками определения состава, важности и ценности конфиденциальной информации применительно к видам тайны |
| | УК-1.2 Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности | Знать: методические основы разработки общих положений политики ИБ |
| | | Уметь: разрабатывать общие положения политики ИБ |
| | | Владеть: навыками проведения анализа защищенности информации в АИС |
| | УК-1.3 Имеет практический опыт работы с информационными источниками, опыт | Знать: информационные источники и аналитические методы конкурентной разведки |
| | | Уметь: производить поиск необходимой информации по выбранной тематике |
| | | Владеть: опытом анализа и обобщения информации |

| | | |
|---|---|---|
| | научного поиска, создания научных текстов | |
| УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы | Знать: основную правовую и нормативно-методическую базу в области информационной безопасности |
| | | Уметь: производить поиск необходимых нормативно-правовых документов в области обеспечения ИБ |
| | | Владеть: навыками проведения мониторинга и выявления условий, способствующих совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональные данные, других сведений ограниченного распространения |
| | УК-2.2 Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности | Знать: типовые модели угроз и нарушителей информации; методики построения частных моделей угроз |
| | | Уметь: оценивать информационные риски, выделять значимые (опасные) угрозы ИБ |
| | | Владеть: навыками проведения аудита информационной безопасности АИС и планирования необходимых мероприятий при проектировании ком-плексной системы ЗИ |
| | УК-2.3 Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности | Знать: базовый набор рекомендованных методик для решения задач обеспечения безопасности информационных технологий и систем |
| | | Уметь: применять на практике руководящие документы Гостехкомиссии РФ, приказы ФСТЭК и ФСБ РФ в области защиты информации |
| | | Владеть: навыками использования нормативно-методической базы при разработке и эксплуатации комплексных систем информационной безопасности |

## 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

| Код | Наименование разделов, тем и видов работ | Очная форма | | | | | Заочная форма | | | | | *Код индикатора достижения компетенции |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Семестр | Часы | | | | Курс | Часы | | | | |
| | | | Лек | Пр | Лаб | СР | | Лек | Пр | Лаб | СР | |
| **1.0** | **Раздел 1. Основные понятия и положения ЗИ в АИС. Модели угроз информации в АИС.** | | | | | | | | | | | |
| 1.1 | Тема 1. Основные понятия, термины и определения; предмет и объект защиты | 5 | 2 | | | 6 | 4/уст. | 2 | | | 36 | ОПК-3.1 ОПК-3.2 ОПК-3.3 УК-1.1 УК-1.2 УК-1.3 УК-2.1 УК-2.2 УК-2.3 |
| 1.2 | Тема 2. Уязвимости и угрозы безопасности информации в АИС; риски ИБ и методы их оценки; обзор основных технологий защиты | 5 | 8 | | | 10 | 4/уст. | 4 | | | 40 | ОПК-3.1 ОПК-3.2 ОПК-3.3 УК-1.1 УК-1.2 УК-1.3 УК-2.1 УК-2.2 УК-2.3 |

| 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Код** | **Наименование разделов, тем и видов работ** | **Очная форма** | | | | | **Заочная форма** | | | | | ***Код индикатора достижения компетенции** |
| | | **Семестр** | **Часы** | | | | **Курс** | **Часы** | | | | |
| | | | **Лек** | **Пр** | **Лаб** | **СР** | | **Лек** | **Пр** | **Лаб** | **СР** | |
| 1.3 | Тема 3. Базовые принципы организации ЗИ | 5 | 2 | | | 6 | 4/уст. | 2 | | | 34 | ОПК-3.1<br>ОПК-3.2<br>УК-2.1<br>УК-2.3 |
| 1.4 | Лабораторная работа № 1. Сканирование уязвимостей данной конфигурации ОС Windows с помощью сканера безопасности | 5 | | | 2 | 2 | 4/уст. | | | 2 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 1.5 | Лабораторная работа № 2. Проверка стойкости паролей данной конфигурации ОС Windows | 5 | | | 2 | 2 | 4/уст. | | | 3 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 1.6 | Лабораторная работа № 3. Средство резервного копирования Acronis | 5 | | | 4 | 2 | 4/уст. | | | 3 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| | Форма промежуточной аттестации – экзамен | | | | | | 4/зимняя | 18 | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3 |
| **2.0** | **Раздел 2. Технологии идентификации и аутентификации субъектов доступа. Механизмы разграничения доступа к ресурсам АИС.** | | | | | | | | | | | |
| 2.1 | Тема 4. Методы и средства идентификации/ аутентификации | 5 | 2 | | | 4 | 4/зимняя | | | | 10 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 2.2 | Тема 5. Механизм разграничения доступа субъектов к объектам: основные понятия и определения. Модели разграничения доступа: избирательное управление; мандатное управление; замкнутая программная среда; реализация моделей на примере системы защиты информации (СЗИ) от НСД SecretNet | 5 | 10 | | | 4 | 4/зимняя | 2 | | | 10 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 2.3 | Тема 6. Защита в Windows NT | 5 | 10 | | | 4 | 4/зимняя | | | | 10 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 2.4 | Лабораторная работа № 4. Защита в ОС Windows (создание учётных записей; назначение прав пользователей; шаблоны безопасности; регистрация и аудит) | 5 | | | 10 | 4 | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |

| 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Код** | **Наименование разделов, тем и видов работ** | **Очная форма** | | | | | **Заочная форма** | | | | | ***Код индикатора достижения компетенции** |
| | | **Семестр** | **Часы** | | | | **Курс** | **Часы** | | | | |
| | | | **Лек** | **Пр** | **Лаб** | **СР** | | **Лек** | **Пр** | **Лаб** | **СР** | |
| 2.5 | Лабораторная работа № 5. СЗИ от НСД SecretNet (дискреционное и полномочное разграничение доступа; контроль целостности; замкнутая программная среда; аудит; работа с электронным идентификатором; затирание данных) | 5 | | | 16 | 4 | 4/зимняя | | | 4 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| | Форма промежуточной аттестации – экзамен | 5 | 36 | | | | | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 |
| **3.0** | **Раздел 3. Криптографические методы защиты информации, контроля целостности и электронной подписи.** | | | | | | | | | | | |
| 3.1 | Тема 7. Классификация методов криптографического преобразования информации | 6 | 2 | | | 4 | 4/зимняя | 1 | | | 10 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.2 | Тема 8. Требования к симметричным и асимметричным криптосистемам | 6 | 2 | | | 4 | 4/зимняя | 1 | | | 20 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.3 | Тема 9. Стандарты и алгоритмы шифрования | 6 | 12 | | | 4 | 4/зимняя | 1 | | | 10 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.4 | Тема10. Функции хэширования | 6 | 6 | | | 2 | 4/зимняя | | | | 20 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.5 | Тема 11. Электронная подпись; инфраструктура открытых ключей | 6 | 4 | | | 6 | 4/зимняя | 1 | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.6 | Лабораторная работа № 6 .Криптоанализ шифра простой замены | 6 | | | 2 | 2 | 4/зимняя | | | 2 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.7 | Лабораторная работа № 7. Программная реализация метода XOR - кодирования (схема Вернама) | 6 | | | 4 | 2 | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.8 | Лабораторная работа № 8. Программная реализация шифра многоалфавитной подстановки Виженера | 6 | | | 4 | 2 | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 3.9 | Лабораторная работа № 9. Программная | 6 | | | 4 | 2 | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2 |

| 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Код** | **Наименование разделов, тем и видов работ** | **Очная форма** | | | | | **Заочная форма** | | | | | ***Код индикатора достижения компетенции** |
| | | **Семестр** | **Часы** | | | | **Курс** | **Часы** | | | | |
| | | | **Лек** | **Пр** | **Лаб** | **СР** | | **Лек** | **Пр** | **Лаб** | **СР** | |
| | реализация варианта алгоритма RSA | | | | | | | | | | | ОПК-3.3 |
| 3.10 | Лабораторная работа № 10. Пакеты Криптоофис, КриптоАРМ, Криптосейф | 6 | | | 4 | 2 | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| **4.0** | **Раздел 4. Многофункциональные средства защиты от несанкционированного доступа к информации и иные технологии ЗИ в АИС.** | | | | | | | | | | | |
| 4.1 | Тема 12. СЗИ от НСД Dallas Lock: основные функциональные возможности | 6 | 4 | | | 7 | 4/зимняя | 2 | | | 12 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 4.2 | Тема 13. Технологии сетевой безопасности (межсетевые экраны, сканеры безопасности, средства построения виртуальных частных сетей, системы обнаружения вторжений) | 6 | 4 | | | 7 | 4/зимняя | | | | 20 | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 4.3 | Лабораторная работа № 11. СЗИ от НСД Dallas Lock: основные функциональные возможности | 6 | | | 10 | | 4/зимняя | | | 4 | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 4.4 | Лабораторная работа № 12. Сканеры безопасности | 6 | | | 4 | | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| 4.5 | Лабораторная работа № 13. Антивирусно программное обепечение | 6 | | | 2 | | 4/зимняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 |
| | Форма промежуточной аттестации – зачет | 6 | | | | | 4/летняя | 4 | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2 |
| | Курсовая работа | 6 | | | | 24 | 4/летняя | | | | | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2 |
| | Итого часов (без учёта часов на промежуточную аттестацию) | | 68 | | 68 | 116 | | 16 | | 18 | 232 | |

## 5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

## 6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1 Учебная литература

#### 6.1.1 Основная литература

| | Библиографическое описание | Кол-во экз. в библиотеке/ онлайн |
|---|---|---|
| 6.1.1.1 | Буранова, М. А. Комплексная система защиты информации : учебное пособие / М. А. Буранова, Н. В. Киреева. Самара : ПГУТИ, 2019. - 145с. - Текст: электронный. - URL: https://e.lanbook.com/book/223181 | Онлайн |
| 6.1.1.2 | Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. Москва : РТУ МИРЭА, 2020. - 136с. - Текст: электронный. - URL: https://e.lanbook.com/book/167606 | Онлайн |
| 6.1.1.3 | Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций : курс лекций / Н. Г. Милославская, А. И. Толстой. Москва : НИЯУ МИФИ, 2020. - 536с. - Текст: электронный. - URL: https://e.lanbook.com/book/284378 | Онлайн |
| 6.1.1.4 | А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте : в 2 частях : учебник / А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик. Москва : УМЦ ЖДТ, - 448с. - Текст: электронный. - URL: https://umczdt.ru/books/42/30051/ | Онлайн |

#### 6.1.2 Дополнительная литература

| | Библиографическое описание | Кол-во экз. в библиотеке/ онлайн |
|---|---|---|
| 6.1.2.1 | Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин,И. Б. Шубинский.. Москва : Юрайт, 2019. - 342с. - Текст: электронный. - URL: https://urait.ru/bcode/441287 | Онлайн |

#### 6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

| | Библиографическое описание | Кол-во экз. в библиотеке/ онлайн |
|---|---|---|
| 6.1.3.1 | Бутин А.А. Методические указания по изучению дисциплины Б1.О.23 Безопасность информационных технологий и систем по направлению подготовки 09.03.02 Информационные системы и технологии, профиль Информационные системы и технологии / А.А. Бутин ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 17 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_4616_1396_2021_1_signed.pdf | Онлайн |

### 6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

| | |
|---|---|
| 6.2.1 | Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/ |
| 6.2.2 | Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/ |
| 6.2.3 | Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/ |
| 6.2.4 | Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/ |
| 6.2.5 | Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/ |
| 6.2.6 | Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/ |

### 6.3 Программное обеспечение и информационные справочные системы

#### 6.3.1 Базовое программное обеспечение

| | |
|---|---|
| 6.3.1.1 | Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01 |

| | |
|---|---|
| 6.3.1.2 | Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01 |
| 6.3.1.3 | FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/ |
| 6.3.1.4 | Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/ |
| 6.3.1.5 | Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License |
| **6.3.2 Специализированное программное обеспечение** | |
| 6.3.2.1 | Сканер MBSA (свободное ПО) Сканер-ВС (свободное ПО для вузов) СЗИ от НСД SecretNet (лицензия) Персональные идентификаторы ruToken СЗИ от НСД Dallas Lock 8.0 (С, К) (свободное ПО для вузов) Пакет PrZamena (свободное ПО) Утилита LC 4+ (свободное ПО) Dr.Web Cureit! (свободное ПО) 360 Total Security (свободное ПО) Средство резервного копирования Acronis (лицензия) Сканер «XSpider.exe 7.x» (demo-версия) |
| 6.3.2.2 | Сканер Nessus-3.x (свободное ПО) |
| 6.3.2.3 | Сканер SSS v5.27 (demo-версия). |
| **6.3.3 Информационные справочные системы** | |
| 6.3.3.1 | Не предусмотрены |
| **6.4 Правовые и нормативные документы** | |
| 6.4.1 | Не предусмотрены |

## 7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

| | |
|---|---|
| 1 | Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80 |
| 2 | Учебная аудитория Д-605 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, компьютер. Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты). |
| 3 | Учебная аудитория Д-313 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, компьютер. Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты). |
| 4 | Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации». «Безопасность программно-аппаратных средств защиты информации» для проведения лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ИрГУПС, учебно-наглядные пособия (презентации, плакаты). Электронный замок Соболь-PCI |
| 5 | Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся:<br>– читальные залы;<br>– учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507;<br>– помещения для хранения и профилактического обслуживания учебного оборудования – А-521 |

## 8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

| Вид учебной деятельности | Организация учебной деятельности обучающегося |
|---|---|
| Лекция | Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся.<br>Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, |

| | |
|---|---|
| | образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии |
| Практическое занятие | Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности.<br>На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины |
| Лабораторная работа | Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1.<br>Исходя из цели, содержанием лабораторных работ могут быть:<br>- экспериментальная проверка формул, методик расчета;<br>- проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов;<br>- ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.;<br>- наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения;<br>- имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах;<br>- наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест);<br>- установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.;<br>- ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.;<br>- установление свойств веществ, их качественных и количественных характеристик;<br>- анализ различных характеристик процессов, в том числе производственных и иных процессов;<br>- расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.);<br>- наблюдение развития явлений, процессов и др.<br>Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций.<br>По характеру выполняемых лабораторных работ возможны:<br>- ознакомительные работы, используемые для закрепления изученного теоретического материалы; |

| | |
|---|---|
| | - аналитические работы, используемые для получения новой информации на основе формализованных методов;<br>- творческие работы, ориентированные на самостоятельный выбор подходов решения задач.<br>Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину |
| Самостоятельная работа | Обучение по дисциплине «Безопасность информационных технологий и систем» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.<br>Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» |
| Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет | |

**Приложение № 1 к рабочей программе**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## для проведения текущего контроля успеваемости и промежуточной аттестации

# 1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

## 2. Перечень компетенций, в формировании которых участвует дисциплина.
## Программа контрольно-оценочных мероприятий.
## Показатели оценивания компетенций, критерии оценки

Дисциплина «Безопасность информационных технологий и систем» участвует в формировании компетенций:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

**Программа контрольно-оценочных мероприятий очная форма обучения**

| № | Наименование контрольно-оценочного мероприятия | Объект контроля | Код индикатора достижения компетенции | Наименование оценочного средства (форма проведения*) |
|---|---|---|---|---|
| **5 семестр** | | | | |
| **1.0** | **Раздел 1. Основные понятия и положения ЗИ в АИС. Модели угроз информации в АИС** | | | |
| 1.1 | Текущий контроль | Тема 1. Основные понятия, термины и определения; предмет и объект защиты | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | Тестирование (компьютерные технологии) |
| 1.2 | Текущий контроль | Тема 2. Уязвимости и угрозы безопасности информации в АИС; риски ИБ и методы их оценки; обзор основных технологий защиты | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | Тестирование (компьютерные технологии) |
| 1.3 | Текущий контроль | Тема 3. Базовые принципы организации ЗИ | ОПК-3.1<br>ОПК-3.2<br>УК-2.1<br>УК-2.3 | Тестирование (компьютерные технологии) |
| 1.4 | Текущий контроль | Лабораторная работа № 1. Сканирование уязвимостей данной конфигурации ОС Windows с помощью сканера безопасности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 1.5 | Текущий контроль | Лабораторная работа № 2. Проверка стойкости паролей данной конфигурации ОС Windows | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 1.6 | Текущий контроль | Лабораторная работа № 3. Средство резервного копирования Acronis | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| **2.0** | **Раздел 2. Технологии идентификации и аутентификации субъектов доступа. Механизмы разграничения доступа к ресурсам АИС** | | | |

| | | | | |
|---|---|---|---|---|
| 2.1 | Текущий контроль | Тема 4. Методы и средства идентификации/ аутентификации | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.2 | Текущий контроль | Тема 5. Механизм разграничения доступа субъектов к объектам: основные понятия и определения. Модели разграничения доступа: избирательное управление; мандатное управление; замкнутая программная среда; реализация моделей на примере системы защиты информации (СЗИ) от НСД SecretNet | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.3 | Текущий контроль | Тема 6. Защита в Windows NT | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.4 | Текущий контроль | Лабораторная работа № 4. Защита в ОС Windows (создание учётных записей; назначение прав пользователей; шаблоны безопасности; регистрация и аудит) | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 2.5 | Текущий контроль | Лабораторная работа № 5. СЗИ от НСД SecretNet (дискреционное и полномочное разграничение доступа; контроль целостности; замкнутая программная среда; аудит; работа с электронным идентификатором; затирание данных) | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| | Промежуточная аттестация | Все разделы | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | Экзамен (собеседование)<br>Экзамен - тестирование (компьютерные технологии) |
| **6 семестр** | | | | |
| **3.0** | **Раздел 3. Криптографические методы защиты информации, контроля целостности и электронной подписи** | | | |
| 3.1 | Текущий контроль | Тема 7. Классификация методов криптографического преобразования информации | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.2 | Текущий контроль | Тема 8. Требования к симметричным и асимметричным криптосистемам | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.3 | Текущий контроль | Тема 9. Стандарты и алгоритмы шифрования | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.4 | Текущий контроль | Тема10. Функции хэширования | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.5 | Текущий контроль | Тема 11. Электронная подпись; инфраструктура открытых ключей | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.6 | Текущий контроль | Лабораторная работа № 6 .Криптоанализ шифра простой замены | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |

| | | | | |
|---|---|---|---|---|
| 3.7 | Текущий контроль | Лабораторная работа № 7. Программная реализация метода XOR - кодирования (схема Вернама) | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 3.8 | Текущий контроль | Лабораторная работа № 8. Программная реализация шифра многоалфавитной подстановки Виженера | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 3.9 | Текущий контроль | Лабораторная работа № 9. Программная реализация варианта алгоритма RSA | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 3.10 | Текущий контроль | Лабораторная работа № 10. Пакеты Криптоофис, КриптоАРМ, Криптосейф | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| **4.0** | **Раздел 4. Многофункциональные средства защиты от несанкционированного доступа к информации и иные технологии ЗИ в АИС** | | | |
| 4.1 | Текущий контроль | Тема 12. СЗИ от НСД Dallas Lock: основные функциональные возможности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 4.2 | Текущий контроль | Тема 13. Технологии сетевой безопасности (межсетевые экраны, сканеры безопасности, средства построения виртуальных частных сетей, системы обнаружения вторжений) | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 4.3 | Текущий контроль | Лабораторная работа № 11. СЗИ от НСД Dallas Lock: основные функциональные возможности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 4.4 | Текущий контроль | Лабораторная работа № 12. Сканеры безопасности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 4.5 | Текущий контроль | Лабораторная работа № 13. Антивирусно программное обепечение | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| | Промежуточная аттестация | Все разделы | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2 | Курсовая работа (письменно)<br>Курсовая работа (устно) |
| | Промежуточная аттестация | Все разделы | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2 | Зачет (собеседование)<br>Зачет - тестирование (компьютерные технологии) |

## Программа контрольно-оценочных мероприятий заочная форма обучения

| № | Наименование контрольно-оценочного мероприятия | Объект контроля | Код индикатора достижения компетенции | Наименование оценочного средства (форма проведения*) |
|---|---|---|---|---|
| **4 курс, сессия установочная** | | | | |
| **1.0** | **Раздел 1. Основные понятия и положения ЗИ в АИС. Модели угроз информации в АИС.** | | | |
| 1.1 | Текущий контроль | Тема 1. Основные понятия, термины и определения; предмет и объект защиты | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1 | Тестирование (компьютерные технологии) |

| | | | | |
|---|---|---|---|---|
| | | | УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | |
| 1.2 | Текущий контроль | Тема 2. Уязвимости и угрозы безопасности информации в АИС; риски ИБ и методы их оценки; обзор основных технологий защиты | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | Тестирование (компьютерные технологии) |
| 1.3 | Текущий контроль | Тема 3. Базовые принципы организации ЗИ | ОПК-3.1<br>ОПК-3.2<br>УК-2.1<br>УК-2.3 | Тестирование (компьютерные технологии) |
| 1.4 | Текущий контроль | Лабораторная работа № 1. Сканирование уязвимостей данной конфигурации ОС Windows с помощью сканера безопасности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 1.5 | Текущий контроль | Лабораторная работа № 2. Проверка стойкости паролей данной конфигурации ОС Windows | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| 1.6 | Текущий контроль | Лабораторная работа № 3. Средство резервного копирования Acronis | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| **4 курс, сессия зимняя** | | | | |
| | Промежуточная аттестация | Все разделы | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3 | Экзамен (собеседование)<br>Экзамен - тестирование (компьютерные технологии) |
| **4 курс, сессия зимняя** | | | | |
| **2.0** | **Раздел 2. Технологии идентификации и аутентификации субъектов доступа. Механизмы разграничения доступа к ресурсам АИС.** | | | |
| 2.1 | Текущий контроль | Тема 4. Методы и средства идентификации/ аутентификации | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.2 | Текущий контроль | Тема 5. Механизм разграничения доступа субъектов к объектам: основные понятия и определения. Модели разграничения доступа: избирательное управление; мандатное управление; замкнутая программная среда; реализация моделей на примере системы защиты информации (СЗИ) от НСД SecretNet | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.3 | Текущий контроль | Тема 6. Защита в Windows NT | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 2.4 | Текущий контроль | Лабораторная работа № 5. СЗИ от НСД SecretNet (дискреционное и полномочное разграничение доступа; контроль целостности; замкнутая программная среда; аудит; работа с электронным | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |

| | | | | |
|---|---|---|---|---|
| | | идентификатором; затирание данных) | | |
| **3.0** | **Раздел 3. Криптографические методы защиты информации, контроля целостности и электронной подписи.** | | | |
| 3.1 | Текущий контроль | Тема 7. Классификация методов криптографического преобразования информации | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.2 | Текущий контроль | Тема 8. Требования к симметричным и асимметричным криптосистемам | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.3 | Текущий контроль | Тема 9. Стандарты и алгоритмы шифрования | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.4 | Текущий контроль | Тема10. Функции хэширования | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.5 | Текущий контроль | Тема 11. Электронная подпись; инфраструктура открытых ключей | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 3.6 | Текущий контроль | Лабораторная работа № 6 .Криптоанализ шифра простой замены | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| **4.0** | **Раздел 4. Многофункциональные средства защиты от несанкционированного доступа к информации и иные технологии ЗИ в АИС.** | | | |
| 4.1 | Текущий контроль | Тема 12. СЗИ от НСД Dallas Lock: основные функциональные возможности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 4.2 | Текущий контроль | Тема 13. Технологии сетевой безопасности (межсетевые экраны, сканеры безопасности, средства построения виртуальных частных сетей, системы обнаружения вторжений) | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тестирование (компьютерные технологии) |
| 4.3 | Текущий контроль | Лабораторная работа № 11. СЗИ от НСД Dallas Lock: основные функциональные возможности | ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Лабораторная работа (письменно/устно) |
| **4 курс, сессия летняя** | | | | |
| | Промежуточная аттестация | Все разделы | | Зачет (собеседование)<br>Зачет - тестирование (компьютерные технологии) |

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

## Описание показателей и критериев оценивания компетенций. Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

| № | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в ФОС |
|---|---|---|---|
| 1 | Тестирование (компьютерные технологии) | Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Фонд тестовых заданий |
| 2 | Лабораторная работа | Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы.<br>Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся | Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты |

Промежуточная аттестация

| № | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в ФОС |
|---|---|---|---|
| 1 | Зачет | Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Перечень теоретических вопросов и практических заданий к зачету |
| 2 | Тест – промежуточная аттестация в форме зачета | Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Фонд тестовых заданий |
| 3 | Экзамен | Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену |
| 4 | Тест – промежуточная аттестация в форме экзамена | Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Фонд тестовых заданий |
| 5 | Курсовая работа | Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления.<br>Может выполняться в индивидуальном порядке или группой обучающихся. | Образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты |

| | | | |
|---|---|---|---|
| | | Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях | |

**Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена. Шкала оценивания уровня освоения компетенций**

| Шкалы оценивания | | Критерии оценивания | Уровень освоения компетенции |
|---|---|---|---|
| «отлично» | «зачтено» | Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы | Высокий |
| «хорошо» | | Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов | Базовый |
| «удовлетворительно» | | Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы | Минимальный |
| «неудовлетворительно» | «не зачтено» | Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов | Компетенция не сформирована |

Тест – промежуточная аттестация в форме зачета и экзамена

| Шкала оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования |
| «хорошо» | | Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования |
| «удовлетворительно» | | Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования |
| «неудовлетворительно» | «не зачтено» | Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования |

Курсовая работа

| Шкала оценивания | Критерии оценивания |
|---|---|
| «отлично» | Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы |
| «хорошо» | Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе |
| «удовлетворительно» | Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы |
| «неудовлетворительно» | Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала.<br>Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы |

## Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Тестирование

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования |
| «хорошо» | | Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования |
| «удовлетворительно» | | Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования |
| «неудовлетворительно» | «не зачтено» | Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования |

Лабораторная работа

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний.<br>Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для |

| | | |
|---|---|---|
| | | проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме |
| «хорошо» | | Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.<br>Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета) |
| «удовлетворительно» | | Лабораторная работа выполнена с задержкой, письменный отчет с недочетами.<br>Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами |
| «неудовлетворительно» | «не зачтено» | Лабораторная работа не выполнена, письменный отчет не представлен.<br>Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений.<br>Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки |

# 3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

## 3.1 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

| Индикатор достижения компетенции | Тема в соответствии с РПД | Характеристика ТЗ | Количество тестовых заданий, типы ТЗ |
|---|---|---|---|
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2<br>УК-2.3 | Тема 1. Основные понятия, термины и определения; предмет и объект защиты | Знание терминологи-ческой базы предмет-ной области | 6 – ОТЗ<br>6 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3<br>УК-1.1<br>УК-1.2<br>УК-1.3<br>УК-2.1<br>УК-2.2 | Тема 2. Уязвимости и угрозы безопасности информации в АИС; риски ИБ и методы их оценки; обзор основных технологий защиты | Знание состава и содержания угроз ИБ, основных технологий защиты | 6 – ОТЗ<br>6 – ЗТЗ |

| | | | |
|---|---|---|---|
| ОПК-3.1<br>ОПК-3.2<br>УК-2.1<br>УК-2.3 | Тема 3. Базовые принципы организации ЗИ | Знание базовых принципы организации ЗИ | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 4. Методы и средства идентификации/ аутентификации | Знание технологий идентификации/ аутентификации субъектов | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 5. Механизм разграничения доступа субъектов к объектам: основные понятия и определения. Модели разграничения доступа: избирательное управление; мандатное управление; замкнутая программная среда; реализация моделей на примере системы защиты информации (СЗИ) от НСД SecretNet | Знание технологий разграничения доступа к обектам | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 6. Защита в Windows NT | Знание подсистем защита в Windows NT | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 7. Классификация методов криптографического преобразования информации | Знание классификации методов криптографической защиты информации | 4 – ОТЗ<br>4 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 8. Требования к симметричным и асимметричным криптосистемам | Знание требований к симметричным и асимметричным криптосистемам | 3 – ОТЗ<br>3 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 9. Стандарты и алгоритмы шифрования | Знание свойств стандартов и алгоритмов шифрования | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема10. Функции хэширования | Знание технологий хэширования | 4 – ОТЗ<br>4 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 11. Электронная подпись; инфраструктура открытых ключей | Знание технологий электронной подписи | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 12. СЗИ от НСД Dallas Lock: основные функциональные возможности | Знание основных защитных механизмов СЗИ от НСД Dallas Lock | 5 – ОТЗ<br>5 – ЗТЗ |
| ОПК-3.1<br>ОПК-3.2<br>ОПК-3.3 | Тема 13. Технологии сетевой безопасности (межсетевые экраны, сканеры безопасности, средства построения виртуальных частных сетей, системы обнаружения вторжений) | Знание технологий сетевой безопасности | 5 – ОТЗ<br>5 – ЗТЗ |
| | | Итого | 63 – ОТЗ<br>63 – ЗТЗ |

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. Выберите правильное определение термина «обладатель информации»:

а) лицо, самостоятельно создавшее информацию;

б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;

**в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;**

г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

2. Выберите правильное определение термина «защищаемые помещения»:

а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;

б) помещения, специально предназначенные для размещения технических средств информационной системы;

в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;

**г) помещения, специально предназначенные для проведения конфиденциальных мероприятий;**

3. Выберите правильное определение термина «контролируемая зона»:

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

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;

в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;

г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

4. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

**а) методы и способы защиты информации от несанкционированного доступа;**

**б) методы и способы сокрытия информации от внутренних нарушителей;**

в) методы и способы устранения конкурентов;

**г) методы и способы защиты информации от утечки по техническим каналам;**

5. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;

**б) пассивные;**

в) разноплановые;

г) удостоверяющие;

**д) активные.**

6. “Технический канал утечки информации” - это:

**а) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;**

б) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств;

в) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

г) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.

7. «Несанкционированный доступ к информации» - это:

а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

**б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;**

в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;

г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

8. «Персональный идентификатор» — это

а) устройство для хранения зашифрованной информации пользователя;
**б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;**
в) устройство для хранения журнала аудита

9. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для
**а) ограничения использования программного обеспечения на компьютере;**
б) установки ограниченного количества программ;
в) сбора сведений об используемых приложениях.
10. Механизм контроля_____ СЗИ Secret Net предназначен для слежения за неизменностью содержимого ресурсов компьютера
**Ответ: целостности**
11. В СЗИ Secret Net с помощью _____ конфиденциальности реализован механизм полномочного разграничения доступа в ресурсам
**Ответ: меток**
12. Длина ключа шифрования алгоритма ГОСТ 28147-89 равна _____ бит.
**Ответ: 256**
13. Алгоритм AES относится к _____ типу криптосистем
О**твет: симметричному**
14. Вставьте слово: Межсетевой экран служит для _____ трафика при передачи данных
**Ответ: фильтрации**
15. Вставьте слово: В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____
Ответ: NTFS
16. Вставьте слово: Практическая стойкость алгоритма RSA основана на сложности решения задачи_____:
**Ответ: факторизации**
17. Вставьте слово: Хэш-функции предназначены, главным образом, для контроля ____ данных
**Ответ: целостности**
18. Вставьте слова: Технология электронной подписи разработана с целью подтверждения _____ и _____ сообщений.
**Ответ: авторства: подлинности**

### 3.2 Типовые задания для выполнения лабораторной работы

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 1. Сканирование уязвимостей данной конфигурации ОС Windows с помощью сканера безопасности»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 2. Проверка стойкости паролей данной конфигурации ОС Windows»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 3. Средство резервного копирования Acronis»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 4. Защита в ОС Windows (создание учётных записей; назначение прав пользователей; шаблоны безопасности; регистрация и аудит)»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 5. СЗИ от НСД SecretNet (дискреционное и полномочное разграничение доступа; контроль целостности; замкнутая программная среда; аудит; работа с электронным идентификатором; затирание данных)»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 6 .Криптоанализ шифра простой замены»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 7. Программная реализация метода XOR - кодирования (схема Вернама)»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 8. Программная реализация шифра многоалфавитной подстановки Виженера»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 9. Программная реализация варианта алгоритма RSA»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 10. Пакеты Криптоофис, КриптоАРМ, Криптосейф»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 11. СЗИ от НСД Dallas Lock: основные функциональные возможности»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 12. Сканеры безопасности»

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Лабораторная работа № 13. Антивирусное программное обеспечение»

**3.3 Типовое задание для выполнения курсовой работы**

Типовые задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты.

Образец типового задания для выполнения курсовой работы

Организация и настройка параметров защищенного по требованиям информационной безопасности рабочего места сотрудника в составе АИС виртуального предприятия

Студент выступает роли администратора информационной безопасности (в дальнейшем АИБ), ответственного за реализацию технологий защищенных обработки и хранения информации ограниченного доступа (ИОД) на отдельном компьютере в подразделении виртуального предприятия. Число подразделений соответствует количеству студентов в группе (см. Приложение 1 к методическим указаниям по выполнению КР).

АИБу необходимо с помощью штатных подсистем ЗИ ОС Windows в среде виртуальной машины VirtualBox и добавочных механизмов/сервисов защиты от несанкционированного доступа (НСД) (Dallas Lock/Secret Net) сделать следующее:

**1. Определить:**

1.1. Граф взаимодействия данного подразделения с другими отделами на минимально необходимом функциональном уровне.

**2. Обеспечить:**

2.1. Общий уровень безопасности работы в ОС Windows в соответствии с рекомендациями (см. Приложение № 2 к методическим указаниям к КР).

2.2. Организацию защищенной от НСД работу сотрудников данного подразделения в плане доступа к ИОД в зависимости от занимаемой должности, при этом:

2.2.1. Создать:

- учетные записи (в том числе задать сильные пароли),
- рабочие папки;
- рабочие файлы;

2.2.2. Предоставить необходимые привилегии пользователям (см. Приложение № 2 к методическим указаниям к КР) .

2.2.3. Организовать дискреционный доступ (разрешения на папки-файлы) к данным ресурсам сотрудникам только тех подразделений предприятия, которым считается это нужным в силу производственной необходимости (минимизируя распространение прав доступа).

2.2.4. Настроить мандатное разграничение доступа пользователей к ресурсам (Dallas Lock/Secret Net).

2.2.5. Настроить механизм контроля целостности (Dallas Lock/Secret Net).

2.2.6. Настроить механизм очистки остаточной информации (Dallas Lock/Secret Net).

### 3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
2. Требования к симметричным и асимметричным криптосистемам;
3. Стандарты и алгоритмы шифрования (с детализацией);
4. Электронный замок «Соболь»;
5. СЗИ от НСД Dallas Lock: основные функциональные возможности;
6. Функции хэширования; криптографические стандарты;
7. Электронная подпись; инфраструктура открытых ключей;
8. Назначение, механизмы и функциональные возможности DLP-систем;
9. Компьютерные вирусы; троянские программы; сетевые черви; сертифицированные средства антивирусной защиты;

10. Технологии сетевой безопасности: межсетевые экраны;
11. Технологии сетевой безопасности: сканеры безопасности;
12. Технологии сетевой безопасности: средства построения виртуальных частных сетей;
13. Технологии сетевой безопасности: системы обнаружения вторжений

### 3.5 Перечень теоретических вопросов к экзамену
(для оценки знаний)

1. Основные понятия, термины и определения; предмет и объект защиты;
2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
3. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
4. Базовые принципы организации ЗИ;
5. Резервирование и восстановление информации; повышение надежности АИС;
6. Блокировка ошибочных операций пользователей; минимизация ущерба от аварий и стихийных бедствий;
7. Противодействие наблюдению в оптическом диапазоне; противодействие утечкам по группе акустических каналов;
8. Методы и средства защиты от побочных электромагнитных излучений и наводок;
9. Способы аутентификации. Парольные системы;
10. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
11. Реализация моделей: система защиты информации (СЗИ) от НСД SecretNet;
12. Назначение и функции механизма аудита;
13. Механизм разграничения доступа в ОС Windows NT;
14. Механизм идентификации/аутентификации в ОС Windows NT;
15. Аудит в ОС Windows NT

## 4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

| Наименование оценочного средства | Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения |
|---|---|
| Тестирование (компьютерные технологии) | Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста |
| Лабораторная работа | Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено.<br>Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы.<br>Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия |
| Курсовая работа | Ход выполнения разделов курсовой работы в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания. Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия. |

| | |
|---|---|
| | В ходе защиты курсовой работы обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовую работу после завершения защиты, учитывая уровень ее защиты |

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

**Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения**

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

**Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)**

| Средняя оценка уровня сформированности компетенций по результатам текущего контроля | Шкала оценивания |
|---|---|
| Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю | «зачтено» |
| Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю | «не зачтено» |

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

**Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения**

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к

экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

**Образец экзаменационного билета**

<table>
<tr><td>ИРГУПС<br>20__-20__<br>учебный год</td><td>Экзаменационный билет № 1<br>по дисциплине «<u>Безопасность информационных технологий и систем</u>»</td><td>Утверждаю:<br>Заведующий кафедрой<br>ИСиЗИ ИрГУПС<br>_____</td></tr>
<tr><td colspan="3">1. …….<br>2. …….<br>3. …….<br>4. …….</td></tr>
</table>