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 «17» июня 2022 г. № 77

# Б1.О.42 Защита информации

## рабочая программа дисциплины

Специальность/направление подготовки – 38.05.01 Экономическая безопасность
Специализация/профиль – Экономико-правовое обеспечение экономической безопасности
Квалификация выпускника – Экономист
Форма и срок обучения – очная форма 5 лет; заочная форма 6 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108

Формы промежуточной аттестации
очная форма обучения:
экзамен 7 семестр
заочная форма обучения:
экзамен 5 курс

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

| Семестр | 7 | **Итого** |
|---|---|---|
| Вид занятий | Часов по УП | **Часов по УП** |
| **Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*** | 51 | **51** |
| – лекции | 17 | **17** |
| – практические (семинарские) | 34 | **34** |
| – лабораторные | | |
| **Самостоятельная работа** | 21 | **21** |
| **Экзамен** | 36 | **36** |
| **Итого** | 108 | **108** |

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

| Курс | 5 | **Итого** |
|---|---|---|
| Вид занятий | Часов по УП | **Часов по УП** |
| **Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*** | 12 | **12** |
| – лекции | 6 | **6** |
| – практические (семинарские) | 6 | **6** |
| – лабораторные | | |
| **Самостоятельная работа** | 78 | **78** |
| **Экзамен** | 18 | **18** |
| **Итого** | 108 | **108** |

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 38.05.01 Экономическая безопасность, утвержденным Приказом Минобрнауки России от 14.04.2021 г. № 293.

Программу составил(и):
к.э.н., доцент, С.П.Серёдкин
к.э.н., доцент, заведующий кафедрой, Т. К. Кириллова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «17» июня 2022 г. № 12

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

СОГЛАСОВАНО

Кафедра «Финансовый и стратегический менеджмент», протокол от «17» июня 2022 г. № 10

Зав. кафедрой, к.э.н., доцент С.А. Халетская

## 1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1 Цель дисциплины

| | |
|---|---|
| 1 | раскрытие сущности защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации в системе экономической безопасности организации |

### 1.2 Задачи дисциплины

| | |
|---|---|
| 1 | изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий и методологических принципов создания систем защиты информации в системе экономической безопасности организации; |
| 2 | изучение видов защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем |

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

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.23 Информационные системы в экономике |
| 2 | Б1.О.40 Основы информационной безопасности |

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

| | |
|---|---|
| 1 | Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы |
| 2 | Б3.02(Д) Защита 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-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. | ОПК-7.1 Знает основные типы информационных технологий, используемых для решения профессиональных задач | Знать: классификацию и характеристики составляющих защиты информации в создаваемых и функционирующих системах экономической безопасности |
| | | Уметь: разрабатывать модели угроз информационной безопасности в системах экономической безопасности хозяйствующих субъектов |
| | | Владеть: принципами и правилами построения организационных структур системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности хозяйствующих субъектов |
| | ОПК-7.2 Применяет современные IT-решения для выполнения задач в работе экономиста | Знать: виды защищаемой информации, угрозы информационной безопасности, методы и средства обеспечения информационной безопасности в создаваемых и функционирующих системах экономической безопасности |
| | | Уметь: определять комплекс мер (правила, процедуры, |

| | | |
|---|---|---|
| | | практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем хозяйствующих субъектов |
| | | Владеть: административно-управленческими методами реализации комплекса мер по информационной безопасности в системах экономической безопасности хозяйствующих субъектов |

## 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. Теория информационной безопасности.** | | | | | | | | | | | |
| 1.1 | Тема 1. Концептуальная модель информационной безопасности | 7 | 1 | 2 | | 2 | 5/уст. | 0.5 | 0.5 | | 8 | ОПК-7.1 |
| 1.2 | Тема 2. Угрозы информационной безопасности | 7 | 2 | 4 | | 2 | 5/уст. | 0.5 | 0.5 | | 8 | ОПК-7.1 |
| 1.3 | Тема 3. Реализация и гарантирование политики безопасности | 7 | 2 | 4 | | 4 | 5/уст. | 0.5 | 0.5 | | 8 | ОПК-7.2 |
| **2.0** | **Раздел 2. Методология защиты информации.** | | | | | | | | | | | |
| 2.1 | Тема 4. Понятие и виды защищаемой информации | 7 | 2 | 4 | | 2 | 5/уст. | 0.5 | 0.5 | | 10 | ОПК-7.1 ОПК-7.2 |
| 2.2 | Тема 5. Общая характеристика способов и средств защиты информации | 7 | 2 | 4 | | 2 | 5/уст. | 1 | 1 | | 8 | ОПК-7.1 ОПК-7.2 |
| 2.3 | Тема 6. Методы организации безопасного доступа | 7 | 2 | 4 | | 3 | 5/уст. | 1 | 1 | | 10 | ОПК-7.1 ОПК-7.2 |
| 2.4 | Тема 7. Электронная цифровая подпись и цифровые сертификаты | 7 | 2 | 4 | | 2 | 5/уст. | 0.5 | 0.5 | | 8 | ОПК-7.1 ОПК-7.2 |
| 2.5 | Тема 8. Каналы и методы несанкционированного доступа к конфиденциальной информации | 7 | 2 | 4 | | 2 | 5/уст. | 1 | 1 | | 2 | ОПК-7.1 ОПК-7.2 |
| 2.6 | Тема 9. Программно-аппаратные средства защиты информации | 7 | 2 | 4 | | 2 | 5/уст. | 0.5 | 0.5 | | 8 | ОПК-7.1 ОПК-7.2 |
| | Форма промежуточной аттестации – экзамен | 7 | 36 | | | | 5/зимняя | 18 | | | | ОПК-7.1 ОПК-7.2 |
| | Контрольная работа | 7 | | | | | 5/зимняя | | | | 8 | ОПК-7.1 ОПК-7.2 |
| | Итого часов (без учёта часов на промежуточную аттестацию) | | 17 | 34 | | 21 | | 6 | 6 | | 78 | |

## 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 | 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 |
| 6.1.1.2 | Ададуров, С. Е. Методология и система обеспечения информационной безопасности на железнодорожном транспорте : учеб. для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО : в 2 ч. / С. Е. Ададуров [и др.] ; ред. А. А. Корниенко. М. : УМЦ по образованию на ж.-д. трансп., 2014. - 439с. | 27 |
| 6.1.1.3 | Аршинский, Л. В. Техническая защита информации : практикум / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов [и др.]. Иркутск : ИрГУПС, 2022. - 76с. | 17 |
| 6.1.1.4 | Внуков, А. А. Защита информации : учебное пособие для вузов - 3-е изд. пер. и допА. А. Внуков.. Москва : Юрайт, 2021. - 161с. - Текст: электронный. - URL: https://urait.ru/bcode/470131 (дата обращения: 09.09.2022) | Онлайн |
| 6.1.1.5 | Демидов, Д. Г. Защита информации с использованием механизмов электронной цифровой подписи : учебно-методическое пособие / Д. Г. Демидов, О. Г. Швечкова, О. А. Москвитина, А. Н. Пылькин [и др.]. Рязань : РГРТУ, 2014. - 53с. - Текст: электронный. - URL: https://e.lanbook.com/book/168091 (дата обращения: 19.04.2023) | Онлайн |
| **6.1.2 Дополнительная литература** | | |
| | Библиографическое описание | Кол-во экз. в библиотеке/ онлайн |
| 6.1.2.1 | Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. Москва : ТУСУР, 2007. - 201с. - Текст: электронный. - URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=10927 (дата обращения: 19.04.2023) | Онлайн |
| 6.1.2.2 | Поляков, Е. А. Основы информационной безопасности : учебное пособие / Е. А. Поляков. Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2021. - 71с. - Текст: электронный. - URL: https://e.lanbook.com/book/282890 (дата обращения: 19.04.2023) | 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 | Серёдкин, С. П. Методические указания по изучению дисциплины Б1.О.42 Защита информации, 38.05.01 Экономическая безопасность, специализация – Экономико-правовое обеспечение экономической безопасности / С.П. Серёдкин, Т. К. Кириллова; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 12 с - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_4248_1562_2022_1_signed.pdf | Онлайн |
| **6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»** | | |
| 6.2.1 | Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/ | |
| 6.2.2 | Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/ | |
| 6.2.3 | Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/ | |
| 6.2.4 | Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/ | |
| 6.2.5 | Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/ | |
| 6.2.6 | Электронно-библиотечная система Polpred.com Обзор СМИ, https://polpred.com/ | |
| **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 | Не предусмотрено |
| **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-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной) |
| 3 | Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер |
| 4 | Учебная аудитория А-516 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, Мультимедиапроектор(переносной),экран(переносной),компьютер. |
| 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 |
| Самостоятельная работа | Обучение по дисциплине «Защита информации» 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 «Защита информации» участвует в формировании компетенций:

ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

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

| № | Наименование контрольно-оценочного мероприятия | Объект контроля | Код индикатора достижения компетенции | Наименование оценочного средства (форма проведения*) |
|---|---|---|---|---|
| **7 семестр** | | | | |
| **1.0** | **Раздел 1. Теория информационной безопасности** | | | |
| 1.1 | Текущий контроль | Тема 1. Концептуальная модель информационной безопасности | ОПК-7.1 | Собеседование (устно) |
| 1.2 | Текущий контроль | Тема 2. Угрозы информационной безопасности | ОПК-7.1 | Собеседование (устно) |
| 1.3 | Текущий контроль | Тема 3. Реализация и гарантирование политики безопасности | ОПК-7.2 | Доклад (устно) |
| **2.0** | **Раздел 2. Методология защиты информации** | | | |
| 2.1 | Текущий контроль | Тема 4. Понятие и виды защищаемой информации | ОПК-7.1 ОПК-7.2 | Доклад (устно) |
| 2.2 | Текущий контроль | Тема 5. Общая характеристика способов и средств защиты информации | ОПК-7.1 ОПК-7.2 | Ситуационная задача (письменно) |
| 2.3 | Текущий контроль | Тема 6. Методы организации безопасного доступа | ОПК-7.1 ОПК-7.2 | Ситуационная задача (письменно) |
| 2.4 | Текущий контроль | Тема 7. Электронная цифровая подпись и цифровые сертификаты | ОПК-7.1 ОПК-7.2 | Доклад (устно) |
| 2.5 | Текущий контроль | Тема 8. Каналы и методы несанкционированного доступа к конфиденциальной информации | ОПК-7.1 ОПК-7.2 | Собеседование (устно) |
| 2.6 | Текущий контроль | Тема 9. Программно-аппаратные средства защиты информации | ОПК-7.1 ОПК-7.2 | Ситуационная задача (письменно) |
| | Промежуточная аттестация | Раздел 1. Теория информационной безопасности. Раздел 2. Методология защиты информации. | ОПК-7.1 ОПК-7.2 | Экзамен (собеседование) Экзамен - 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*) |
|---|---|---|---|---|
| **5 курс, сессия установочная** | | | | |
| **1.0** | **Раздел 1. Теория информационной безопасности.** | | | |
| 1.1 | Текущий контроль | Тема 1. Концептуальная модель информационной безопасности | ОПК-7.1 | Собеседование (устно) |
| 1.2 | Текущий контроль | Тема 2. Угрозы информационной безопасности | ОПК-7.1 | Собеседование (устно) |
| 1.3 | Текущий контроль | Тема 3. Реализация и гарантирование политики безопасности | ОПК-7.2 | Доклад (устно) |
| **2.0** | **Раздел 2. Методология защиты информации.** | | | |
| 2.1 | Текущий контроль | Тема 4. Понятие и виды защищаемой информации | ОПК-7.1 ОПК-7.2 | Доклад (устно) |
| 2.2 | Текущий | Тема 5. Общая характеристика | ОПК-7.1 | Ситуационная задача |

| | | | | |
|---|---|---|---|---|
| | контроль | способов и средств защиты информации | ОПК-7.2 | (письменно) |
| 2.3 | Текущий контроль | Тема 6. Методы организации безопасного доступа | ОПК-7.1<br>ОПК-7.2 | Ситуационная задача (письменно) |
| 2.4 | Текущий контроль | Тема 7. Электронная цифровая подпись и цифровые сертификаты | ОПК-7.1<br>ОПК-7.2 | Доклад (устно) |
| 2.5 | Текущий контроль | Тема 8. Каналы и методы несанкционированного доступа к конфиденциальной информации | ОПК-7.1<br>ОПК-7.2 | Собеседование (устно) |
| 2.6 | Текущий контроль | Тема 9. Программно-аппаратные средства защиты информации | ОПК-7.1<br>ОПК-7.2 | Ситуационная задача (письменно) |
| **5 курс, сессия зимняя** | | | | |
| | Текущий контроль | Раздел 2. Методология защиты информации. | ОПК-7.1<br>ОПК-7.2 | Контрольная работа (КР) (письменно) |
| | Промежуточная аттестация | Раздел 1. Теория информационной безопасности.<br>Раздел 2. Методология защиты информации. | ОПК-7.1<br>ОПК-7.2 | Экзамен (собеседование)<br>Экзамен - 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 | Контрольная работа (КР) | Средство для проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по разделу дисциплины.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Типовое задание для выполнения контрольной работы по разделам/темам дисциплины |
| 2 | Собеседование | Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.<br>Может быть использовано для оценки знаний обучающихся | Вопросы для собеседования по темам/разделам дисциплины |
| 3 | Ситуационная задача | Проблемное задание, в котором обучающемуся | Типовое задание |

| | | | |
|---|---|---|---|
| | | предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности, а также отдельных компетенций (в рамках дисциплины) | для решения ситуационной задачи |
| 4 | Доклад | Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.<br>Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Темы докладов |

Промежуточная аттестация

| № | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в ФОС |
|---|---|---|---|
| 1 | 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 |
| 2 | 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 |

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

| Шкала оценивания | Критерии оценивания | Уровень освоения компетенции |
|---|---|---|
| «отлично» | 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» | 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 экзамена

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

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

Контрольная работа

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Обучающийся полностью и правильно выполнил задание контрольной работы. Показал отличные знания и умения в рамках усвоенного учебного материала. Контрольная работа оформлена аккуратно и в соответствии с предъявляемыми требованиями |
| «хорошо» | | Обучающийся выполнил задание контрольной работы с небольшими неточностями. Показал хорошие знания и умения в рамках усвоенного учебного материала. Есть недостатки в оформлении контрольной работы |
| «удовлетворительно» | | Обучающийся выполнил задание контрольной работы с существенными неточностями. Показал удовлетворительные знания и умения в рамках усвоенного учебного материала. Качество оформления контрольной работы имеет недостаточный уровень |
| «неудовлетворительно» | «не зачтено» | Обучающийся не полностью выполнил задания контрольной работы, при этом проявил недостаточный уровень знаний и умений |

Собеседование

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ |
| «хорошо» | | Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач |
| «удовлетворительно» | | Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий<br>Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ |
| «неудовлетворительно» | «не зачтено» | Не было попытки выполнить задание |

Ситуационная задача

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Обучающийся излагает материал логично, грамотно, без ошибок; свободное владеет профессиональной терминологией; умеет высказывать и обосновать свои суждения; дает четкий, полный, правильный ответ на теоретические вопросы; организует связь теории с практикой |
| «хорошо» | | Обучающийся грамотно излагает материал; ориентируется в материале; владеет профессиональной терминологией; осознанно применяет теоретические знания для решения кейса, но содержание и форма ответа имеют отдельные неточности.<br>Ответ обучающегося правильный, полный, с незначительными неточностями или недостаточно полный |
| «удовлетворительно» | | Обучающийся излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения кейса, не может доказательно обосновать свои суждения; обнаруживается недостаточно глубокое понимание изученного материала |
| «неудовлетворительно» | «не зачтено» | У обучающегося отсутствуют необходимые теоретические знания; допущены ошибки в определении понятий, искажен их смысл, не решен кейс.<br>В ответе обучающийся проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для решения кейса |

Доклад

| Шкалы оценивания | | Критерии оценивания |
|---|---|---|
| «отлично» | «зачтено» | Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые) |
| «хорошо» | | Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры) |
| «удовлетворительно» | | Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая |
| «неудовлетворительно» | «не зачтено» | Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль доклада не передана |

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

## 3.1 Типовые контрольные задания для выполнения контрольных работ

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

Ниже приведен образец типовых вариантов заданий для выполнения контрольных работ.

Образец типового варианта контрольной работы

### 3.2 Типовые контрольные задания для проведения собеседования

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

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

1. Что положено в основу принципа обеспечения защиты информации?
2. Дайте понятие информационной безопасности.
3. Какие требования предъявляются к организационной защите информации?
4. Какой ФЗ регламентирует порядок засекречивания и рассекречивания сведений,
5. относящихся к государственной тайне?
6. Назовите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации.
7. Назовите виды информации по категориям доступа

«Тема 1. Концептуальная модель информационной безопасности»

Образец типового варианта вопросов для проведения собеседования

«Тема 2. Угрозы информационной безопасности»

1. Перечислите виды угроз информационной безопасности РФ.

2 Что является источниками угроз информационной безопасности РФ?

3 Назовите основные задачи обеспечения информационной безопасности РФ. Какие из них требуют безотлагательного решения?

4 Перечислите основные методы обеспечения информационной безопасности РФ и кратко охарактеризуйте их.

5 Какова структура государственной системы обеспечения информационной безопасности РФ?

Образец типового варианта вопросов для проведения собеседования

«Тема 8. Каналы и методы несанкционированного доступа к конфиденциальной информации»

1. Какие у нас существуют законы по защите информации?
2. Какие цели ставит федеральный закон "Об информации, информатизации и
3. защите информации"?
4. Как, на ваш взгляд, можно защитить информацию?
5. Каковы особенности работы с документами, содержащими конфиденциальную
6. информацию?
7. Что такое СКУД?
8. Каковы основные функции СКУД при контроле рабочего времени?
9. В чем особенности пропускного режима?
10. Расскажите об особенностях защиты материальных ценностей и информации.

### 3.3 Типовые контрольные задания для решения ситуационной задачи

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

Ниже приведен образец типовых вариантов заданий для решения ситуационных задач.

Образец типового варианта ситуационной задачи

«Тема 5. Общая характеристика способов и средств защиты информации»

Дано пять информационных объектов:

- компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия (отдел кадров);
- компьютер бухгалтера (бухгалтерия);

- личная банковская карта;
- школьный компьютер (компьютерный класс);
- компьютер – рабочая станция оператора (ТЭЦ).

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами. Обозначить источник каждой из приведенных угроз.

Образец типового варианта ситуационной задачи
«Тема 6. Методы организации безопасного доступа»

Задача 1

Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу. Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему направлению: привлечение сторонних организаций к обработке информации.

Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации. Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.

Задача 2

Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу. Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2023 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора.

Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова? Ответ: согласно статьи №….

Задача 3

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией.

Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей.

Вопросы:

1. Какая статья УК РФ была нарушена?
2. Что послужило предметом преступления?
3. Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задача 4

Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации.

Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задача 5

Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Образец типового варианта ситуационной задачи

«Тема 9. Программно-аппаратные средства защиты информации»

Составить характеристику вируса на основе варианта задания. Номером варианта задания является порядковый номер студента в списке группы.

Таблица 1. Варианты задания

| Номер варианта | Среда обитания | Способ заражения среды обитания | Способ воздействия | Особенности алгоритма |
|---|---|---|---|---|
| 1. | 3 | 1 | 1 | 2 |
| 2. | 4 | 1 | 1 | 3 |
| 3. | 2 | 2 | 4 | 4 |
| 4. | 2 | 3 | 4 | 1 |
| 5. | 1 | 4 | 3 | 1 |
| 6. | 1 | 4 | 2 | 2 |
| 7. | 4 | 3 | 1 | 2 |
| 8. | 3 | 2 | 1 | 3 |
| 9. | 4 | 1 | 4 | 4 |
| 10. | 2 | 1 | 3 | 4 |
| 11. | 2 | 1 | 2 | 1 |
| 12. | 1 | 2 | 1 | 1 |
| 13. | 1 | 3 | 1 | 2 |
| 14. | 4 | 4 | 4 | 2 |
| 15. | 3 | 4 | 3 | 3 |
| 16. | 4 | 3 | 2 | 4 |
| 17. | 2 | 2 | 1 | 4 |
| 18. | 2 | 1 | 1 | 1 |
| 19. | 1 | 1 | 4 | 1 |
| 20. | 1 | 1 | 3 | 2 |
| 21. | 4 | 2 | 2 | 2 |
| 22. | 3 | 3 | 1 | 3 |
| 23. | 4 | 4 | 1 | 4 |
| 24. | 2 | 4 | 4 | 4 |
| 25. | 2 | 3 | 3 | 1 |
| 26. | 1 | 2 | 2 | 1 |
| 27. | 1 | 1 | 1 | 2 |
| 28. | 4 | 1 | 1 | 2 |
| 29. | 3 | 1 | 4 | 3 |

Классификация вирусов:

По среде обитания:

- сетевые;
- файловые;
- загрузочные;
- файлово-загрузочные.

По способу заражения среды обитания:

- резидентные;
- нерезидентные.

По способу воздействия:

- неопасные;
- опасные вирусы;
- очень опасные.

По особенностям алгоритма:

- макровирусы;

- стелс-вирусы;
- троянский конь;
- бэкдор.

### 3.4 Типовые контрольные темы для написания докладов

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

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов
«Тема 3. Реализация и гарантирование политики безопасности»

1. Законодательство о персональных данных.
2. Защита авторских прав.
3. Назначение, функции и типы систем видеозащиты
4. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
5. Информационная безопасность: экономические аспекты.
6. Безопасность применения пластиковых карт - законодательство и практика.

Образец тем докладов
«Тема 4. Понятие и виды защищаемой информации»

1. Методы борьбы с фишинговыми атаками.
2. Обзор угроз и технологий защиты Wi-Fi-сетей.
3. Проблемы внедрения дискового шифрования.
4. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
5. Особенности процессов аутентификации в корпоративной среде.
6. Квантовая криптография.
7. Утечки информации: как избежать. Безопасность смартфонов.

Образец тем докладов
«Тема 7. Электронная цифровая подпись и цифровые сертификаты»

Как подписывать с помощью ЭЦП электронные документы различных форматов.

1. Обеспечение безопасности Web-сервисов.
2. Защита от внутренних угроз.
3. Технологии RFID.
4. Уничтожение информации на магнитных носителях.
5. Ботнеты - плацдарм современных кибератак.
6. Цифровые водяные знаки в изображениях.
7. Электронный документооборот. Модели нарушителя.
8. Идентификация по голосу. Скрытые возможности.

### 3.5 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-7.1 | Тема 1. Концептуальная модель информационной | Знание | 2 – ОТЗ |

| | | | |
|---|---|---|---|
| | безопасности | | 2 – ЗТЗ |
| ОПК-7.1 | Тема 2. Угрозы информационной безопасности | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Умение | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.2 | Тема 3. Реализация и гарантирование политики безопасности | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 4. Понятие и виды защищаемой информации | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 5. Общая характеристика способов и средств защиты информации | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Умение | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 6. Методы организации безопасного доступа | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Умение | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 7. Электронная цифровая подпись и цифровые сертификаты | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 8. Каналы и методы несанкционированного доступа к конфиденциальной информации | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Умение | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Навык и (или) опыт деятельности/ действие | 1 – ЗТЗ |
| ОПК-7.1<br>ОПК-7.2 | Тема 9. Программно-аппаратные средства защиты информации | Знание | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Умение | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Навык и (или) опыт деятельности/ действие | 2 – ОТЗ<br>2 – ЗТЗ |
| | | Итого | 81 |

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. Массовая несанкционированная рассылка сообщений рекламного или несанкционированного характера это?
   - **A. спам**
   - B. атака
   - C. троян
   - D. дефрагментация.

2. Каналы распространения спама?
   - **A. письма по электронной почте**
   - **B. сообщения в формах, конференциях**
   - **C. сообщения в средствах мгновенного обмена сообщениями**
   - D. при установки ОС
   - E. при установки антивирусной программы

3. Специализированная программа для выявления и устранения вируса?
   - **A. антивирусное обеспечение**
   - B. утилита
   - C. архиватор
   - D. подозрительный упаковщик

E. Троян

4. Профилактические меры защиты от вредноносных программ

**A. Установить систему антивирусной защиты**
**B. Своевременно обновлять систему антивирусной защиты**
**C. Проверять все носители, которые находились за пределами вашей системы**
**D. не открывать вложений, полученных от неизвестных адресатов с неизвестными целями**
E. Своевременная смена пароля
**F. Регулярно проводить полную проверку системы**
G. Своевременное обновление программного обеспечения компьютера

5. Сочетание различных символов, которые сервис ассоциирует с пользователем, под которым его будут видеть другие пользователи

**A. логин**
B. пароль
C. аккаунт
D. аватар

6. Сочетание различных символов подтверждающих, что логином намеревается воспользоваться именно владелец логина это?

**A. пароль**
B. логин
C. аккаунт
D. аватар

7. К правовым методам, обеспечивающим информационную безопасность, относятся:

A. Разработка аппаратных средств обеспечения правовых данных

B. Разработка и установка во всех компьютерных правовых сетях журналов учета действий

**C. Разработка и конкретизация правовых нормативных актов обеспечения безопасности**

8. **Виды информационной безопасности:**

**A. Персональная, корпоративная, государственная**
B. Клиентская, серверная, сетевая
C. Локальная, глобальная, смешанная.

9. Цели информационной безопасности – своевременное обнаружение, предупреждение:

**A. несанкционированного доступа, воздействия в сети**
B. инсайдерства в организации
C. чрезвычайных ситуаций.

10. К основным типам средств воздействия на компьютерную сеть относится:

**Ответ: Логические закладки («мины»)**

11. Бесконтрольный выходконфиденциальной информации за пределы организации или круга лиц, которым она была доверена , –это…

**Ответ: утечка**

12. Ввизуально-оптических каналах связи используется излучение …волн

**Ответ:** ультрафиолетового, инфракрасногоивидимогодиапазонов

13. Возможности несанкционированногоиспользования конфиденциальных сведений в

значительной мере обусловливаются …

**Ответ:** злоумышленными действиями

14. Действия, направленные на устранение действующей угрозы иконкретных преступных действий, относятся к…угроз

**Ответ:** локализации

15. Информация осостоянии окружающей среды является …

**Ответ: общедоступной**

16. К недостаткам аппаратных средств инженерно-технической защиты относят …

**Ответ: недостаточную гибкость**

17. Потенциально или реально существующие воздействия на информационную систему, приводящие кматериальному или моральному ущербу

**Ответ: угроза**

18. Служебные сведения , доступ ккоторым ограничен органами государственной власти в соответствии сГражданским кодексом Российской Федерации и федеральными законами , относятся ккатегории …

**Ответ: служебная тайна.**

### 3.6 Перечень теоретических вопросов к экзамену

(для оценки знаний)

**Раздел 1. Теория информационной безопасности**

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Принципы защиты информации техническими средствами.
3. Основные направления инженерно-технической защиты информации.
4. Показатели эффективности инженерно-технической защиты информации.
5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
6. Семантическая информация, циркулирующая в человеческом обществе.
7. Признаковая информация. Информация о видовых признаках, о признаках сигналов, о признаках веществ.
8. Структурирование информации.
9. Классификация демаскирующих признаков.
10. Опознавательные признаки и признаки деятельности.
11. Видовые демаскирующие признаки.
12. Демаскирующие признаки сигналов.
13. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.

**Раздел 2. Методология защиты информации.**

14. Виды источников и носителей информации.
15. Прямые и косвенные источники семантической информации.
16. Принципы записи и съема информации с ее носителя.
17. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.
18. Побочные электромагнитные излучения и наводки Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
19. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
20. Источники угроз безопасности информации.
21. Опасные сигналы и их источники.
22. Способы и средства наблюдения в оптическом диапазоне.
23. Типовая структура и виды технических каналов утечки информации.
24. Каналы утечки речевой информации.

25. Каналы утечки видовой информации.

26. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.

27. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

28. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.

29. Средства звукоизоляции из звукопоглощения.

30. Средства обнаружения, локализации и подавления сигналов закладных устройств.

31. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.

### 3.7 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1. Какие требования предъявляются к организационной защите информации?
2. Опишите процедуру засекречивания и рассекречивания сведений, относящихся к гос. тайне.
3. Каковы особенности работы с документами, содержащими конфиденциальную информацию?
4. Расскажите об особенностях защиты материальных ценностей и информации.
5. Особенности защиты конфиденциальной информации при проведении переговоров.
6. Какова структура физической безопасности организации
7. Охарактеризуйте методы управления персоналом.
8. Назовите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации.
9. Назовите ФЗ, регламентирующий работу с государственной тайной, банковской, профессиональной, служебной, коммерческой тайной, персональными данными, защиты интеллектуальной собственности.
10. Что включает организация проведения государственной аттестации руководителей предприятий?
11. Каковы функции подразделения аналитического характера в области защиты информации?
12. Какие действия сопровождаются при подготовке служебных помещений, в которых планируется проведение совещания
13. За что предусмотрена уголовная ответственность
14. За какие действия предусмотрена ответственность
15. Чем характеризуется субъективная сторона преступления лица, совершившего неправомерный доступ к компьютерной информации?
16. Нормы составляющие правовую основу второго направления информационной безопасности?
17. Объекты профессиональной тайны

### 3.8 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите и объясните основные виды информации ограниченного доступа.
3. Перечислите направления защиты информации на объекте, согласно ГОСТ Р 50922 – 2006 «Защита информации. Основные термины и определения»
4. Напишите определения следующих терминов: информационная безопасность; доступность информации; целостность информации.
5. Начертите и объясните классификацию видов угроз информационной безопасности.
6. Начертите и объясните классификацию средств защиты информации.
7. Начертите и объясните базовую модель передачи данных.
8. Перечислите существующие методы взлома.
9. Перечислите существующие методы криптоанализа.
10. Начертите и объясните жизненный цикл системы информационной безопасности.
11. Начертите и объясните классификацию источников информационных угроз для РФ.
12. Начертите и объясните классификацию основных видов информационных угроз.
13. Перечислите и объясните любые пять фундаментальных законово информационной

безопасности.

14. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
15. Перечислите негативные факторы, влияющие на состояние ИБ с точки зрения ДИБ.
16. Что такое манифест свободного информационного пространства и в чем его суть?
17. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.
18. Перечислите существующие программные средства защиты информации.

## 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 |
|---|---|
| Контрольная работа | Преподаватель на установочном занятии доводит до обучающихся: темы, количество заданий в контрольной работе. Контрольная работа должна быть выполнена в установленный срок и в соответствии с правилами к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» в последней редакции. Выполненная контрольная работа передается для проверки преподавателю в установленные сроки. Если контрольная работа выполнена не в соответствии с указаниями или не в полном объеме, она возвращается на доработку |
| Собеседование | Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования |
| Ситуационная задача | Преподаватель не мене, чем за неделю до срока решения ситуационных задач должен довести до сведения обучающихся предлагаемые ситуационные задачи. Решенные ситуационные задачи в назначенный срок сдаются на проверку преподавателю |
| Доклад | Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите |

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 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**

| | | |
|---|---|---|
| ИРГУПС<br>20__-20__<br>учебный год | **Экзаменационный билет № 1**<br>**по дисциплине «Защита информации»** | Утверждаю:<br>Заведующий кафедрой «ИСиЗИ» ИрГУПС<br>_____ |
| 1. Прямые и косвенные источники семантической информации.<br>2. Принципы записи и съема информации с ее носителя<br>3. Какова структура физической безопасности организации<br>4. Начертите и объясните жизненный цикл системы информационной безопасности | | |