ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «08» мая 2020 г. № 266-1

# Б1.В.ДВ.08.02 Инструментарий анализа информационных рисков

## рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль подготовки – Безопасность автоматизированных систем
Программа подготовки – академический бакалавриат
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 2
Часов по учебному плану – 72

Формы промежуточной аттестации в семестрах:
зачет 6

**Распределение часов дисциплины по семестрам**

| Семестр | 6 | **Итого** |
|---|---|---|
| Число недель в семестре | 18 | |
| Вид занятий | Часов по учебному плану | **Часов по учебному плану** |
| **Аудиторная контактная работа по видам учебных занятий** | **36** | **36** |
| – лекции | 18 | 18 |
| – практические (семинарские) | 18 | 18 |
| **Самостоятельная работа** | **36** | **36** |
| **Итого** | **72** | **72** |

ИРКУТСК

| 1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ | |
|---|---|
| **1.1 Цели освоения дисциплины** | |
| 1 | изучение видов, практических методов и средств проведения аудита информационной безопасности (ИБ) информационных технологий (ИТ) и систем обеспечения ИБ (СОИБ). |
| **1.2 Задачи освоения дисциплины** | |
| 1 | определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия; |
| 2 | оценить существующие методические подходы и инструментарий в оценке информационных рисков для выявления возможностей совершенствования данной деятельности; |
| 3 | изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта; |
| 4 | освоить методические положения и инструментарий в совершенствовании деятельности в сфере оценки информационных рисков хозяйствующих субъектов; освоить методические подходы и инструментарий в оценке эффективности деятельности по защите информационных активов предприятия. |
| **1.3 Задачи освоения дисциплины** | |
| Научно-образовательное воспитание обучающихся | |
| Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.<br><br>Цель достигается по мере решения в единстве следующих задач:<br>– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;<br>– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;<br>– популяризация научных знаний среди обучающихся;<br>– содействие повышению привлекательности науки, поддержка научно-технического творчества;<br>– 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;<br>– 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.<br><br>Цель достигается по мере решения в единстве следующих задач:<br>– формирование сознательного отношения к выбранной профессии;<br>– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;<br>– формирование психологи профессионала;<br>– формирование профессиональной культуры, этики профессионального общения;<br>– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли | |

| 2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП | |
|---|---|
| **2.1 Требования к предварительной подготовке обучающегося** | |
| 1 | Б1.Б.15 Организационное и правовое обеспечение информационной безопасности |
| 2 | Б1.Б.25 Информационные технологии |
| 3 | Б1.Б.11 Основы информационной безопасности |
| 4 | Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков |
| **2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее** | |
| 1 | Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем |
| 2 | Б2.В.03(П) Производственная практика - эксплуатационная |
| 3 | Б2.В.04(Пд) Производственная практика - преддипломная |

| | |
|---|---|
| 4 | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты |

## 3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

**ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений**

| | |
|---|---|
| **Минимальный уровень освоения компетенции** | |
| Знать | состав минимального набора необходимых мер по обеспечению ИБ в зависимости от специфики функционирования автоматизированной системы; |
| Уметь | формировать проект минимального набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования автоматизированной системы; |
| Владеть | навыками проектирования минимального набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования автоматизированной системы; |
| **Базовый уровень освоения компетенции** | |
| Знать | методики проведения аудита автоматизированной системы объекта информатизации; |
| Уметь | провести аудит АС ОИ по необходимым требованиям ИБ; |
| Владеть | навыками проектирования базового набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС; |
| **Высокий уровень освоения компетенции** | |
| Знать | методики разработки политики информационной безопасности организации; |
| Уметь | провести аудит АС ОИ по требованиям ИБ с формированием соответствующих проектных решений; |
| Владеть | навыками проектирования полного набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС. |

**ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности**

| | |
|---|---|
| **Минимальный уровень освоения компетенции** | |
| Знать | законодательную базу, нормативно-методические документы в области ИБ; |
| Уметь | анализировать направления развития информационной безопасности в РФ; |
| Владеть | навыками анализа нормативно-методических документов и российских стандартов в области ИБ; |
| **Базовый уровень освоения компетенции** | |
| Знать | средства и системы обеспечения ИБ объектов информатизации в соответствии с российскими стандартами; |
| Уметь | анализировать эффективность функционирования ИТ в области ИБ; |
| Владеть | навыками применения расчетов эффективности функционирования ИТ в области ИБ. |
| **Высокий уровень освоения компетенции** | |
| Знать | методы анализа информационной безопасности объектов и систем обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; |
| Уметь | анализировать и оценивать риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ; |
| Владеть | навыками анализа и оценки риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ. |

**В результате освоения дисциплины обучающийся должен**

| | |
|---|---|
| **Знать** | |
| 1 | процессы проверки и оценки ИБ ИТ и СОИБ |
| 2 | принципы организации процесса аудита ИБ и подготовки отчетных документов по результатам; |
| 3 | свидетельства аудита ИБ; |
| 4 | критерии и стандарты в области аудита ИБ. |
| **Уметь** | |
| 1 | осуществлять аудит ИБ и организовывать работы по его проведению; |
| 2 | составлять программу аудита ИБ, определять его область действия и критерии; |
| 3 | собирать свидетельства аудита ИБ и грамотно анализировать их; |
| 4 | формулировать выводы и заключение по результатам аудита ИБ; |

| | |
|---|---|
| 5 | вырабатывать практические рекомендации по результатам аудита ИБ для совершенствования СОИБ; |
| 6 | документировать результаты аудита ИБ. |
| **Владеть** | |
| 1 | терминологией в области аудита ИБ; |
| 2 | практическими приемами проведения аудита ИБ, методами сбора данных, оценки рисков, анализа защищенности; |
| 3 | навыками использования инструментальных средств, автоматизированных процессов ИБ. |

## 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр | Часы | Код компетенции | Учебная литература, ресурсы сети «Интернет» |
|---|---|---|---|---|---|
| | **Раздел 1. Теоретические подходы к анализу информационных рисков** | | | | |
| 1.1 | Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Структура курса. Разделы и темы, их распределение по видам аудиторных занятий. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса. /Лек/ | 6 | 2 | ПК-7 | Л1.1, Л3.1, Э1 Э2 |
| 1.2 | Понятие и сущность информационных активов предприятия./Лек/ | 6 | 2 | ПК-10 | Л1.1 Л3.1, Э1 Э2 |
| 1.3 | Подготовка к практической работе по теме «Понятие и сущность информационных активов предприятия. Деловая репутация организации (гудвилл)» /Ср/ | 6 | 2 | ПК-10 | Л1.2, Л1.3, , Э1 |
| 1.4 | Понятие и сущность информационных активов предприятия. Деловая репутация организации (гудвилл). /Пр/ | 6 | 2 | ПК-10 | Л1.1, Л.2.2, Э1 Э2 |
| 1.5 | Понятие информационных рисков. Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия. /Лек/ | 6 | 2 | ПК-7 | Л1.2, Л1.3, Л2.1, Л2.3, Э1 |
| 1.6 | Подготовка к практической работе по теме «Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия» /Ср/ | 6 | 2 | ПК-7 | Л1.2, Л1.3, Л2.1, Л2.3, Э1 |
| 1.7 | Понятие информационных рисков. Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия. /Пр/ | 6 | 2 | ПК-7 | Л1.2, Л1.3, Э1 |
| 1.8 | Методические подходы и инструментарий в оценке информационных рисков. /Лек/ | 6 | 2 | ПК-10 | Л1.2, Л1.3, Л2.1, Л2.3, Э1 |
| 1.9 | Подготовка к практической работе по теме «Методические подходы к оценке информационных рисков на современном этапе» /Ср/ | 6 | 4 | ПК-10 | Л1.1, Л1.2, Л3.1, Э2 |
| 1.10 | Методические подходы к оценке информационных рисков на современном этапе. /Пр/ | 6 | 4 | ПК-10 | Л1.1, Л1.2, Л3.1, Э2 |
| 1.11 | Особенности и проблемы организационного направления в деятельности по защите информационных активов предприятия. /Лек/ | 6 | 2 | ПК-7 ПК-10 | Л1.1, Л1.2, Л3.1, Э2 |
| 1.12 | Подготовка к практической работе по теме | 6 | 4 | ПК-7 ПК-10 | Л1.1, Л1.2, |

| | | | | | |
|---|---|---|---|---|---|
| | «Подбор квалифицированного персонала как одна из особенностей и проблем в деятельности по защите информационных активов предприятия» /Ср/ | | | | Л3.1, Э2 |
| 1.13 | Подбор квалифицированного персонала как одна из особенностей и проблем в деятельности по защите информационных активов предприятия. /Пр/ | 6 | 2 | ПК-7 ПК-10 | Л1.3, Л2.1, Л3.1, Э1 Э2 |
| | **Раздел 2. Практика и технология анализа информационных рисков на предприятии.** | | | | |
| 2.1 | Методический подход и инструментарий в оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков. /Лек/ | 6 | 2 | ПК-7 ПК-10 | Л1.3, Л2.1, Л3.1, Э1 Э2 |
| 2.2 | Подготовка к практической работе по теме «Методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков» /Ср/ | 6 | 4 | ПК-7 ПК-10 | Л1.3, Л2.1, Л3.1, Э1 Э2 |
| 2.3 | Методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков. /Пр/ | 6 | 2 | ПК-7 ПК-10 | Л1.3, Л2.1, Л3.1, Э1 Э2 |
| 2.4 | Методика определения степени надежности персонала, как составная часть методики оценки информационных рисков хозяйствующего субъекта. /Лек/ | 6 | 2 | ПК-7 ПК-10 | Л1.1, Л.2.2, Л3.1 |
| 2.5 | Подготовка к практической работе по теме «Методика определения степени надежности персонала, как составная часть методики оценки информационных рисков хозяйствующего субъекта» /Ср/ | 6 | 4 | ПК-7 ПК-10 | Л1.1, Л.2.2, |
| 2.6 | Методика определения степени надежности персонала, как составная часть методики оценки информационных рисков хозяйствующего субъекта. /Пр/ | 6 | 2 | ПК-7 ПК-10 | |
| 2.7 | Основные направления по применению защитных мероприятий по увеличению рискозащищенности информационных активов предприятия. /Лек/ | 6 | 2 | ПК-7 ПК-10 | Л1.1, Л1.2, Л2.1, Л2.3, Л3.1, Э1 Э2 |
| 2.8 | Подготовка к практической работе по теме «Основные направления по применению защитных мероприятий по увеличению рискозащищенности информационных активов предприятия» /Ср/ | 6 | 4 | ПК-7 ПК-10 | Л1.1, Л1.3, Л2.1, Л.2.2, Л2.3, Л3.1, Э1 Э2 |
| 2.9 | Основные направления по применению защитных мероприятий по увеличению рискозащищенности информационных активов предприятия. /Пр/ | 6 | 2 | ПК-7 ПК-10 | Л1.2, Л1.3, Л2.1, Л.2.2, Л2.3, Л3.1, Э1 Э2 |
| 2.10 | Определение ценности информационных активов. Оценка уязвимостей информационных активов. /Лек/ | 6 | 2 | ПК-7 ПК-10 | Л1.1, Л1.2, Л1.3, Л.2.2, Л2.3, Л3.1, Э1 Э2 |
| 2.11 | Подготовка к практической работе по теме «Управление информационными рисками ценных информационных активов» /Ср/ | 6 | 4 | ПК-7 ПК-10 | Л1.1, Л1.3, Л2.1, Л.2.2, Л3.1, Э1 |
| 2.12 | Управление информационными рисками ценных информационных активов. /Пр/ | 6 | 2 | ПК-7 ПК-10 | Л1.1, Л1.2, , Л2.1, Л.2.2, Л3.1, Э2 |
| | **Раздел 3. Контроль знаний.** | | | | |
| 3.1 | Зачет | 6 | 8 | ПК-7 ПК-10 | Л1.1, Л1.3, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Л.2.2, Л2.3, Л3.1, Э1 |

## 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 разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются 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

| | Авторы, составители | Заглавие | Издательство, год издания | Кол-во экз. в библиотеке/ 100% онлайн |
|---|---|---|---|---|
| Л1.1 | И.А. Никитин, М.Т. Цулая | Процессы анализа и управления рисками в области ИТ: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=429089 | М:Национальный Открытый Университет «ИНТУИТ», 2016 | 100% онлайн |
| Л1.2 | С.А. Нестеров | Основы информационной безопасности: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040 | СПб.: Издательство Политехнического университета, 2014 | 100% онлайн |
| Л1.3 | В.И. Подольский, Н.С. Щербакова, В.Л. Комиссаров | Компьютерные информационные системы в аудите: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=115315 | М. : Юнити-Дана, 2015 | 100% онлайн |

#### 6.1.2 Дополнительная литература

| | Авторы, составители | Заглавие | Издательство, год издания | Кол-во экз. в библиотеке/ 100% онлайн |
|---|---|---|---|---|
| Л2.1 | В.А. Сердюк | Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие //biblioclub.ru/index.php?page=book&id=440285 | М. : Издательский дом Высшей школы экономики, 2015 | 100% онлайн |
| Л2.2 | М.А. Лапина, А.Г. Ревин, В.И. Лапин | Информационное право : учебное пособие[Электронный ресурс] biblioclub.ru/index.php?page=book&id=118624 | М. : Юнити-Дана, 2015 | 100% онлайн |
| Л2.3 | О.В. Порядина | Управление информационными ресурсами: учебно-методическое пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=439328 | Йошкар-Ола: ПГТУ, 2015 | 100% онлайн |

#### 6.1.3 Методические разработки

| | Авторы, составители | Заглавие | Издательство, год издания/ Личный кабинет обучающегося | Кол-во экз. в библиотеке/ 100% онлайн |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Л3.1 | Глухов Н.И. | Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с | - Иркутск: ИрГУПС, 2013 | 55 |
| **6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине** | | | | |
| | Авторы, составители | Заглавие | Издательство, год издания/ Личный кабинет обучающегося | Кол-во экз. в библиотеке/ 100% онлайн |
| Л4.1 | Середкин С.П. | Материалы для самостоятельной работы студентов | Личный кабинет обучающегося | 100% онлайн |
| **6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»** | | | | |
| Э.1 | Линия защиты «Сюртель» www.suritel.ru | | | |
| Э.2 | Федеральная служба по техническому и экспортному контролю, www.fstec.ru | | | |
| **6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем** | | | | |
| **6.3.1 Перечень базового программного обеспечения** | | | | |
| 6.3.1.1 | ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844 | | | |
| 6.3.1.2 | Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org | | | |
| **6.3.2 Перечень специализированного программного обеспечения** | | | | |
| 6.3.2.1 | Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено. | | | |
| **6.3.3 Перечень информационных справочных систем** | | | | |
| 6.3.3.1 | «Консультант +» http://www.consultant.ru/ | | | |
| 6.3.3.2 | «Техэксперт» http://www.cntd.ru/ | | | |
| **6.4 Перечень правовых и нормативных документов** | | | | |
| 6.4.1 | Не предусмотрено | | | |

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

| | |
|---|---|
| 1 | Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80. |
| 2 | Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации). |
| 3 | Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации». |
| 4 | Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС.<br>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. |
| 5 | Помещение А-521 (для хранения и профилактического обслуживания учебного оборудования). |

## 8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

| Вид учебной деятельности | Организация учебной деятельности обучающегося |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, |

| | |
|---|---|
| | выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. 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. Уделить внимание следующим понятиям (перечисление понятий) и др. |
| 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 задание на самостоятельную работу и выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины. |
| Реферат | Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу.<br>Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер.<br>Ознакомиться со структурой и оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции). |
| Самостоятельная работа | Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине. |
| Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. | |

**Приложение 1 к рабочей программе по дисциплине**
**Б1.В.ДВ.08.02 «Инструментарий анализа информационных рисков»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
## для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.В.ДВ.08.02 «Инструментарий анализа информационных рисков»

# 1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «Инструментарий анализа информационных рисков» участвует в формировании компетенций:

**ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;**

**ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности**

**Таблица траекторий формирования у обучающихся компетенций ПК-7, ПК-10 при освоении образовательной программы**

| Код компе-тенции | Наименование компетенции | Индекс и наименование дисциплин / практик, участвующих в формировании компетенции | Семестр изучения дисциплины | Этапы формирования компетенции |
|---|---|---|---|---|
| ПК-7 | способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | Б1.Б.32 Основы кибернетики | 5 | 1 |
| | | Б1.В.07 Аудит информационной безопасности | 6 | 2 |
| | | Б1.В.ДВ.04.02 Эффективность информационных систем | 6 | 2 |
| | | Б1.В.ДВ.08.01 Методология анализа информационных рисков | 6 | 2 |
| | | Б1.В.ДВ.08.02 Инстументарий анализа информационных рисков | 6 | 2 |
| | | Б2.В.03(П) Производственная практика - эксплуатационная | 6 | 2 |
| | | Б1.В.ДВ.07.01 Экономика защиты информации | 8 | 3 |
| ПК-10 | способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности | Б1.В.02 Теоретические основы компьютерной безопасности | 3 | 1 |
| | | Б1.В.07 Аудит информационной безопасности | 6 | 2 |
| | | Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем | 8 | 3 |
| | | Б2.В.04(Пд) Производственная практика - преддипломная | 8 | 3 |
| | | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | 8 | 3 |

**Таблица соответствия уровней освоения компетенций ПК-7, ПК-10 планируемым результатам обучения**

| Код компе-тенции | Наименование компетенции | Наименования разделов дисциплины | Уровни освоения компетенций | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции) |
|---|---|---|---|---|
| ПК-7 | способность проводить анализ исходных данных для проектирования подсистем и | Раздел 1. Теоретические подходы к анализу информационных рисков<br>Раздел 2. Практика | Минимальный уровень | Знать: Состав минимального набора необходимых мер по обеспечению ИБ в зависимости от специфики функционирования АС;<br>Уметь: Формировать проект |

| | | | | |
|---|---|---|---|---|
| | средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | и технология анализа информационных рисков на предприятии. Раздел 3. Контроль знаний | | минимального набора необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС; |
| | | | | Владеть: Навыками проектирования минимального набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС; |
| | | | Базовый уровень | Знать: методики проведения аудита АС ОИ; |
| | | | | Уметь: Провести аудит АС ОИ по необходимым требованиям ИБ; |
| | | | | Владеть: Навыками проектирования базового набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС; |
| | | | Высокий уровень | Знать: Методики разработки политики информационной безопасности организации; |
| | | | | Уметь: Провести аудит АС ОИ по требованиям ИБ с формированием соответствующих проектных решений; |
| | | | | Владеть: Навыками проектирования полного набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования АС. |
| ПК-10 | способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности | Раздел 1. Теоретические подходы к анализу информационных рисков Раздел 2. Практика и технология анализа информационных рисков на предприятии. Раздел 3. Контроль знаний | Минимальный уровень | Знать: Законодательную базу, нормативно-методические документы и российские стандарты в области ИБ; |
| | | | | Уметь: Анализировать направления развития информационных технологий в области ИБ; |
| | | | | Владеть: Навыками анализа нормативно-методических документов и российских стандартов в области ИБ; |
| | | | Базовый уровень | Знать: Средства и системы обеспечения ИБ объектов информатизации в соответствии с российскими стандартами; |
| | | | | Уметь: Анализировать эффективность функционирования ИТ в области ИБ; |
| | | | | Владеть: Навыками применения расчетов эффективности функционирования ИТ в области ИБ. |
| | | | Высокий уровень | Знать: Методы анализа информационной безопасности объектов и систем обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; |

| | | | | |
|---|---|---|---|---|
| | | | | Уметь: Анализировать и оценивать риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ; |
| | | | | Владеть: Навыками анализа и оценки риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ. |

## Программа контрольно-оценочных мероприятий за период изучения дисциплины

| № | Неделя | Наименование контрольно-оценочного мероприятия | Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.) | | Наименование оценочного средства (форма проведения) |
|---|---|---|---|---|---|
| **6 семестр** | | | | | |
| 1 | 1 | Текущий контроль | Тема «Понятие и сущность информационных активов предприятия. Деловая репутация организации (гудвилл)» | ПК-10 | Реферат (письменно) |
| 2 | 2 | Текущий контроль | Тема «Понятие и сущность информационных активов предприятия. Деловая репутация организации (гудвилл)» | ПК-10 | Доклад, сообщение (устно) |
| 3 | 3 | Текущий контроль | Тема «Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия» | ПК-7 | Реферат (письменно) |
| 4 | 4 | Текущий контроль | Тема «Понятие информационных рисков. Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия» | ПК-7 | Доклад, сообщение (устно) |
| 5 | 5 | Текущий контроль | Тема «Методические подходы к оценке информационных рисков на современном этапе» | ПК-10 | Реферат (письменно) |
| 6 | 5 | Текущий контроль | Тема «Методические подходы к оценке информационных рисков на современном этапе» | ПК-10 | Доклад, сообщение (устно) |
| 7 | 7 | Текущий контроль | Тема «Подбор квалифицированного персонала как одна из особенностей и проблем в деятельности по защите информационных активов предприятия» | ПК-7, ПК-10 | Реферат (письменно) |
| 8 | 8 | Текущий контроль | Тема «Подбор квалифицированного персонала как одна из особенностей и проблем в деятельности по защите информационных активов предприятия» | ПК-7, ПК-10 | Доклад, сообщение (устно) |
| 9 | 9 | Текущий контроль | Тема «Методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков» | ПК-7, ПК-10 | Реферат (письменно) |
| 10 | 10 | Текущий контроль | Тема «Методический подход к оценке защищенности | ПК-7, ПК-10 | Доклад, сообщение (устно) |

| | | | | | |
|---|---|---|---|---|---|
| | | | информационных активов хозяйствующего субъекта на основе учета информационных рисков» | | |
| 11 | 11 | Текущий контроль | Тема «Методика определения степени надежности персонала, как составная часть методики оценки информационных рисков хозяйствующего субъекта» | ПК-7, ПК-10 | Реферат (письменно) |
| 12 | 12 | Текущий контроль | Тема «Методика определения степени надежности персонала, как составная часть методики оценки информационных рисков хозяйствующего субъекта» | ПК-7, ПК-10 | Доклад, сообщение (устно) |
| 13 | 13 | Тест | Изученный материал | | Перечень тестовых заданий |
| 14 | 14 | Текущий контроль | Тема «Основные направления по применению защитных мероприятий по увеличению рискозащищенности информационных активов предприятия» | ПК-7, ПК-10 | Реферат (письменно) |
| 15 | 15 | Текущий контроль | Тема «Основные направления по применению защитных мероприятий по увеличению рискозащищенности информационных активов предприятия» | ПК-7, ПК-10 | Доклад, сообщение (устно) |
| 16 | 16 | Текущий контроль | Тема «Управление информационными рисками ценных информационных активов» | ПК-7, ПК-10 | Реферат (письменно) |
| 17 | 17 | Текущий контроль | Тема «Управление информационными рисками ценных информационных активов» | ПК-7, ПК-10 | Доклад, сообщение (устно) |
| 18 | 18 | Промежуточная аттестация – зачет | Разделы:<br>1. Теоретические подходы к анализу информационных рисков<br>2. Практика и технология анализа информационных рисков на предприятии.<br>3. Контроль знаний | ПК-7, ПК-10 | Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста. |

## 2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, 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/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

| № | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в ФОС |
|---|---|---|---|
| 1 | Реферат | Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.<br>Может быть использовано для оценки знаний и умений обучающихся | Темы рефератов |
| 2 | Сообщение, 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, сообщений |
| 3 | Тест | 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 |
| 4 | Зачет (дифференцированный 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 (билетов) к зачету |

**Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена, а также шкала для оценивания уровня освоения компетенций**

| Шкалы оценивания | Критерии оценивания | Уровень освоения компетенций |
|---|---|---|
| «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 |
| | 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 |
| | Обучающийся с существенными неточностями ответил на теоретические | Минимальный |

| | | |
|---|---|---|
| | 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 | |
| «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 | Компетенции не сформированы |

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

Реферат

| Шкала оценивания | Критерии оценивания |
|---|---|
| «отлично» | Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы |
| «хорошо» | Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы |
| «удовлетворительно» | Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод |
| «неудовлетворительно» | Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.<br>Реферат обучающимся не представлен |

Доклад, сообщение

| Шкала оценивания | Критерии оценивания |
|---|---|
| «отлично» | Доклад создан с использованием компьютерных технологий (презентация Power Point, 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 Power Point, 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» | 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 сообщения не передана |

Тест (структура теста по компетенциям)

| Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций) | Минимальное количество тестовых заданий на один раздел программы | Рекомендуемые формы тестовых заданий |
|---|---|---|
| Минимальный уровень освоения компетенции | 30 | Тестовые задания с выбором одного правильного ответа из нескольких |
| | | Тестовые задания с выбором нескольких правильных ответов из множества ответов |
| | | Тестовые задания на установление соответствия |
| | | Тестовые задания на установление правильной последовательности |
| Базовый уровень освоения компетенции | 7 | Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры) |
| Высокий уровень освоения компетенции | 3 | Тестовые задания со свободно конструируемым ответом (интервью, эссе)<br>Структурированный тест<br>Кейсы |

Тест (шкала и критерии оценивания, уровни освоения)

| Шкалы оценивания | | Критерии оценивания | Уровень освоения компетенции |
|---|---|---|---|
| «отлично» | «зачтено» | Обучающийся при тестировании набрал 93-99 баллов | Высокий |
| «хорошо» | | Обучающийся при тестировании набрал 76-92 баллов | Базовый |
| «удовлетворительно» | | Обучающийся при тестировании набрал 60-75 баллов | Минимальный |
| «неудовлетворительно» | «не зачтено» | Обучающийся при тестировании набрал 0-59 баллов | Компетенция не сформирована |

# 3 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

## 3.1 Перечень типовых тем рефератов

1. Структура и факторы общественного производства;
2. Место информации в структуре общественного производства, как важнейший ресурс экономики;
3.Влияние развития рыночной экономики на информационные ресурсы;
4. Информация как товар, цена информации, основные характеристики продукта как товара, классификация товаров, особенности товара «информация», стоимость товара, принципы ее определения;
5. Составляющие стоимости информационных массивов;
6. Проблемы определения стоимостных оценок результатов интеллектуального труда;

7. Стоимостная оценка результатов противоправного использования информации. Методы расчетов, учитывающие характер и особенности производства и реализации контрафактной продукции, созданной с использованием информации, приобретенной противоправным путем;
8. Стоимостная оценка ущерба, нанесенного владельцу информации в связи с утратой прав на ее коммерческую реализацию на основе лицензионных соглашений;
9. Экономическая эффективность реализации инвестиционных проектов, особенности инвестиций в защиту информации;
10. Отбор инвестиционных проектов для реализации на конкурсной основе. Оценочные критерии;
11. Балльный метод сравнительной оценки инвестиционных проектов по созданию комплексных систем защиты информации;
12. Рыночная политика предприятия как потребитель и источник экономической информации, подлежащей защите;
13. Особенности экономической информации о продукции, определение целесообразности ее защиты на разных этапах жизненного цикла товара;
14. Экономическая целесообразность защиты ценовой информации в зависимости от рыночной конъюнктуры. Финансовая и сбытовая деятельность фирмы как источник охраняемой экономической информации;
15. Бизнес-план организации как потребитель и источник экономической информации, подлежащей защите;
16. Понятие о рисках и их классификация. Управление рисками при хозяйственно-экономической деятельности. Оценка рисков при защите информации;
17. Содержание и функции страхования. Виды и способы страхования. Особенности и методы страхования информации. Применение различных видов и методов страхования в целях повышения уровня и надежности защиты информации;

### 3.2 Перечень типовых тем докладов, сообщений

1. Анализ современных подходов к обеспечению информационной безопасности предприятия
2. Методологические подходы к организации комплексной системы защиты информационных активов предприятия
3. Современная концепция и структура защиты информации.
4. Комплексная система защиты информации на предприятии.
5. Принципы организационной защиты информационных активов как подсистемы управления информационной безопасностью предприятия.
6. Работа с персоналом.
7. Организация режимных мер и регламентация использования технических средств информационной безопасности.
8. Информационно-аналитическая деятельность по выявлению внутренних и внешних угроз, оценка и управление информационными рисками.
9. Сравнительный анализ методов оценки рисков информационной безопасности предприятия в системе защиты информационных активов.
10. Уровни зрелости организаций в области информационной безопасности.
11. Этапы управления рисками информационной безопасности.
12. Методики полного анализа рисков информационной безопасности организаций.
13. Разработка методики оценки и управления безопасностью информационных активов.
14. Исследование моделей оценки рисков в системе управления безопасностью информационных активов.
15. Методики оценки рисков информационной безопасности.
16. Влияние различных факторов на величину риска.

17. Разработка методики управления безопасностью информационных активов с учетом рисков в предпринимательской деятельности.
18. Практическое применение методики оценки и управления безопасностью информационных активов и формирование модели информационной системы предприятия.
19. Методические подходы к оценке затрат на обеспечение информационной безопасности информации с учетом рисков реализации угроз.
20. Соотношение стоимости и эффективности некоторых технологий и средств защиты информационных активов

### 3.3 Тест

**1. В каких единицах измеряется риск?**

**а) в стоимостном выражении**

б) во временном выражении

в) в процентах в уровнях

**2. Анализ информационных рисков предназначен для:**

**а) оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность**;

б) оценки технического уровня защищенности информационной системы

в) получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз;

г) убеждения руководства компании в необходимости вложений в систему обеспечения информационной безопасности и для инструментальной проверки защищенности информационной системы

**3. Политика информационной безопасности, прежде всего, необходима для:**

а) успешного прохождения компанией регулярного аудита по ИБ;

б) обеспечения реального уровня защищенности информационной системы компании;

**в) понимания персоналом важности требований по ИБ**;

г) обеспечения адекватной защиты наиболее важных ресурсов компании

**4. Политика информационной безопасности в общем случае является**

а) руководящим документом для администраторов безопасности и системных администраторов

б) руководящим документом для ограниченного использования руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов

**в) руководящим документом для всех сотрудников компании**

**5. Предположим, информационная система компании надежно защищена комплексом средств информационной защиты (межсетевые экраны, антивирусы, системы защиты от НСД, системы обнаружения атак и т.д.). Выберите, как на существующий уровень рисков влияет реализация требований политики безопасности:**

а) информационная система сама по себе надежно защищена комплексом средств защиты, поэтому реализация требований политики безопасности не оказывает существенного влияния на уровень рисков;

б) политика безопасности, как документ для непосредственного использования, отсутствует, что не оказывает существенного влияния на уровень рисков из-за высокого <технологического> уровня защищенности информационной системы;

в) политика безопасности является формальным, не используемым на практике документом, и это не оказывает серьезного влияния на существующий уровень рисков реализация требований политики безопасности

**г) существенно влияет на уровень рисков, так как <технологический> фактор защищенности информационной системы является лишь необходимым, но не достаточным условием обеспечения безопасности**

**6. Выберите, невыполнение, какого из следующих требований политики безопасности, на Ваш взгляд, может наибольшим образом повысить существующие в системе информационные риски:**

а) регулярное обновление антивирусных баз создание и поддержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ

б) **классификация ресурсов по степени важности с точки зрения ИБ завершение активной сессии пользователя по окончании работы**

**7. Международный стандарт управления информационной безопасностью ISO 17799 предъявляет:**

а) требования, предъявляемые только для узкого круга крупнейших мировых компаний

**б) базовые требования по обеспечению ИБ повышенные требования по обеспечению безопасности информационной системы**

в) требования, которые не соответствуют законам стран СНГ в области информационной безопасности

**8. Одной из рекомендаций ISO 17799 является :**

а) четкая регламентация настроек межсетевых экранов

б) применение антивирусных продуктов ведущих производителей

в) проведение анализа рисков и регулярных тестов на проникновение сторонней компанией

**г) необходимость прохождения руководством компании регулярных тренингов по ИБ**

**9. Для проведения анализа информационных рисков, прежде всего, необходимо:**

а) градация информационных рисков

б) построение полной модели информационной системы с точки зрения информационной безопасности

**в) модель нарушителя вероятностные оценки угроз безопасности**

**10. Основной задачей теста на проникновение, прежде всего, является:**

а) оценка возможности обнаружения атаки службой ИБ компании

б) проверка времени реакции службы обеспечения информационной безопасности

**в) оценка возможности осуществления атаки из Интернет на информационную систему компании**

**г) оценка возможных потерь при реализации атаки из Интернет**

**11. Тест на проникновение позволяет (выберите наиболее полное и точное определение)**

а) убедить руководство компании в реальной опасности вторжения из Интернет и обосновать необходимость инвестиций в ИБ

б) снизить вероятные риски вирусной атаки на корпоративную сеть

в) обеспечить должный уровень отношения руководства компании к проблеме обеспечения ИБ

**г) убедиться в способности службы ИБ противостоять возможным атакам злоумышленников из Интернет**

**12. Укажите в общем случае возможные типовые пути воздействия при получении удаленного доступа пользователя к информации на сервере**

а) атака на канал передачи, атака на сервер, атака на пользовательскую группу

б) вирусная атака на корпоративную сеть атака на станцию пользователя, атака на канал передачи

**в) атака на сервер, проникновение злоумышленника в сеть компании из Интернет**

**13. Какой метод обычно используется профессиональными взломщиками при информационной атаке?**

а) атака на наиболее защищенную цель

б) атака на промежуточную цель

**в) атака на наименее защищенную цель**

г) атака осуществляется без целенаправленного выбора цели

**14. Выберите наиболее оптимальную стратегию управления рисками в следующем случае: Веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости**

**а) уменьшение риска и уклонение от риска**

б) принятие риска

в) изменение характера риска и уклонение от риска

г) изменение характера риска и уменьшение риска

**15. Для оценки ущерба по угрозе <целостность> необходимо:**

**а) оценить полную стоимость информации оценить какой ущерб понесет компания в случае изменения информации**

б) оценить какой ущерб понесет компания в случае осуществления несанкционированного доступа к информации

в) оценить возможность осуществления атаки на ресурс, на котором хранится информация

**16. Выберите наиболее полное описание методов, которые применяются при оценке ущерба в случае нарушения конфиденциальности информации**

а) оценка стоимости затрат на реабилитацию подмоченной репутации, престижа, имени компании стоимость упущенной выгоды (потерянный контракт) стоимость затрат на поиск новых клиентов, взамен более не доверяющих компании

б) оценка стоимости контрмер по уменьшению ущерба от нарушения конфиденциальности информации;

**в) оценка прямого ущерба от нарушения конфиденциальности информации**

**17. В случае анализа рисков базового уровня необходимо:**

**а) провести тесты на проникновение проверить выполнение требований соответствующего стандарта, например ISO 17799**

б) провести полный аудит информационной безопасности, включая тесты на проникновение построить полную модель информационной системы с точки зрения информационной безопасности

**Средний**

**1. Пользователь осуществляет удаленный доступ к информации на сервере. Пусть условный уровень защищенности информации на сервере - 24 единицы; условный уровень защищенности рабочего места пользователя - 10 единиц. Оцените условный уровень защищенности удаленного доступа пользователя к информации на сервере:**
Ответ _____ (**34 единицы)**

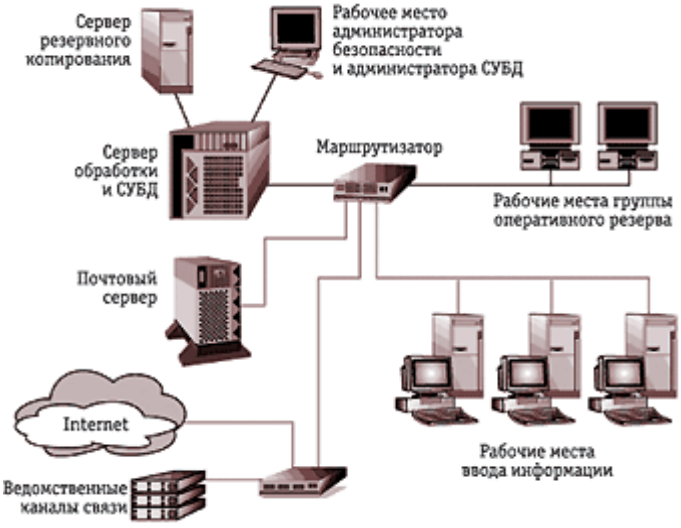
2. Восстановите алгоритм оценки рисков информационной безопасности:

а) идентификация активов;
б) разработка модели угроз;
в) определение допустимого уровня риска;
г) определение риска несоответствия требований законодательства;
д) процедура количественного определения рисков;

**3. Восстановите алгоритм количественного оценивая риска ИБ:**

а) определение ценности актива
б) выбор актуальных угроз ИБ частной модели угроз
в) вычисления значения риска
г) определение ценности актива
д) определение возможности использования организационных и технических уязвимостей

**4. Выделите основные элементы системы**




**Ответ (**

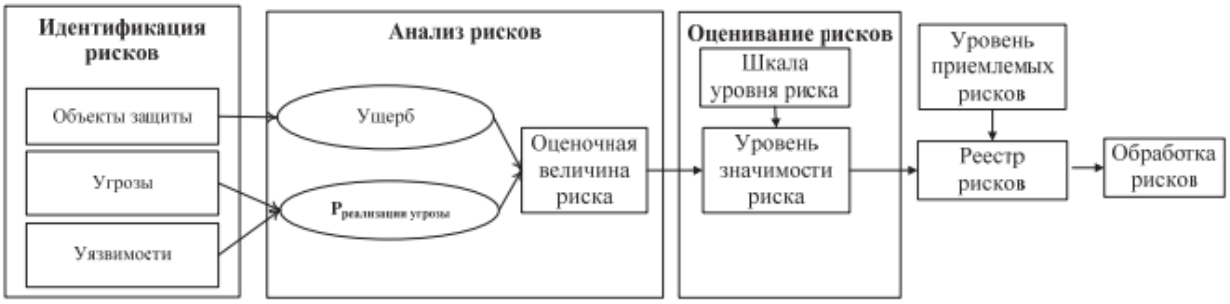
• рабочие места, на которых операторы вводят информацию, поступающую из внешнего мира;
• почтовый сервер, на который информация поступает с удаленных узлов сети через Интернет;
• сервер обработки, на котором установлена СУБД;
• сервер резервного копирования;
• рабочие места группы оперативного реагирования;
• рабочее место администратора безопасности;
• рабочее место администратора БД.))

**5. COBRA** это методика позволяющая выполнить в _____ (Ответ автоматизированном) режиме простейший вариант _____ (Ответ оценивания) информационных рисков любой компании. Для этого предлагается _____ (Ответ использовать) специальные электронные базы _____ и _____ (Ответ знаний и процедуры) логического вывода, ориентированные на требования ISO 17799.

6. Методика и одноименное инструментальное средство RA Software Tool основаны на требованиях международных стандартов _____ и _____ (Ответ ISO 17999 и ISO 13335).

**Высокий**

1. Раскройте значение каждого элемента формулы $R = P_{угр} R_n C \frac{K_o + K_i}{2} 100\%$
2. Дайте развернутую характеристику информационному активу – программно-аппаратные средства.
3. Раскройте методику управления рисками CRAMM
4. Дайте развернутую характеристику процессу оценки информационных рисков представленному на рисунке




5.

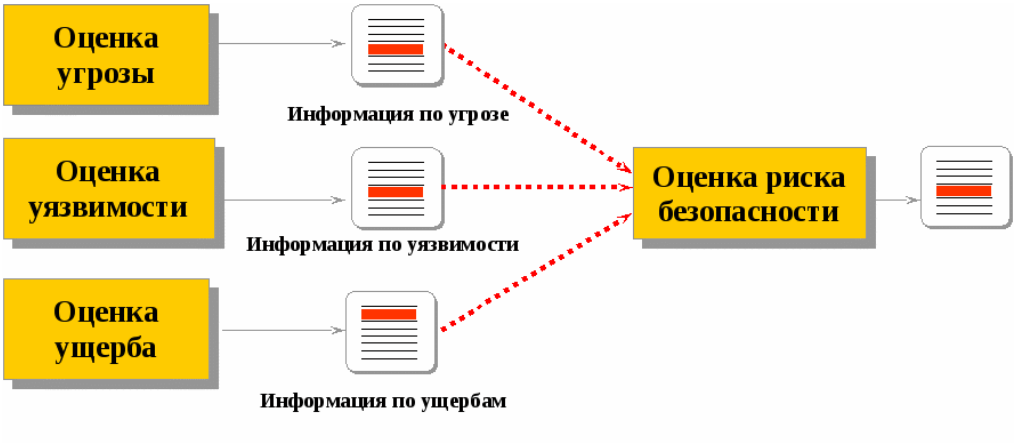
### 3.4 Перечень теоретических вопросов к зачету

1. Сущность понятий «неопределенность» и «риск».
2. Элементы и функции риска.
3. Классификация рисков.
4. Понятие и особенности информационных рисков.
5. Виды информационных угроз и соответствующие бизнес-риски
6. Классификация информационных рисков.
7. Процесс анализа информационных рисков.
8. Источники возникновения информационных рисков.
9. Идентификация информационных рисков: особенности.
10. Основные источниками угроз ценной корпоративной информации
11. Методы идентификации информационных рисков.
12. Методы оценки информационных рисков.
13. Измерение рисков: критерии, формулы, допустимый уровень риска.
14. Сущность информационных активов предприятия-терминология
15. Характеристика зарубежных стандартов управления информационными рисками.
16. Особенности управления информационными рисками в России.
17. Информация как экономическая категория
18. Основные виды организационных каналов утечки информации
19. Методики управления информационными рисками.
20. Содержание областей и элементов информационного рынка
21. Взаимосвязь информационных активов в защищаемой зоне хозяйствующего субъекта
23. Аудит безопасности
24. Программные средства управления рисками базового уровня.
25. Системы полного анализа риска.
26. Требования к защите информационных активов хозяйствующего субъекта

### 3.5 Перечень типовых простых практических заданий к зачету

**Задание 1**

Изучив предложенную схему подготовить информацию, ответить на следующие вопросы:




1. Прочитать схему, объяснив принцип действия.
2. Определить область применения.
3. Отметить наиболее важные аспекты и их влияние на безопасность информационной системы
4. Выводы о целесообразности и месте применения данного механизма.

**Задание 2**

Используя требования ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности.» Часть 3 «Методы менеджмента безопасности информационных технологий» Выберите один из различных информационных актива организации представленных ниже

1. Отделение коммерческого банка
2. Поликлиника
3. Колледж
4. Офис страховой компании
5. Рекрутинговое агентство
6. Интернет-магазин

1. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
2. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

3. Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

4. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

**Задание 3**

Выбрать средства и методы для проведения полного анализа и управления рисками на примере страховой компании.

Какие сложные проблемы необходимо решить при выполнении полного анализа рисков страховой компании?

**Задание 4**

Представить основные этапы полного анализа рисков министерства социальной защиты, при работе его сотрудников с системой обработки персональных данных.

## 4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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 |
|---|---|
| Реферат | Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения |
| Сообщение, доклад | Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения |
| Тест | Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения |

Для организации и проведения промежуточной аттестации (в форме зачета) 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 к зачету для оценки знаний;

– перечень типовых простых практических заданий к зачету для оценки умений;

– перечень типовых практических заданий к зачету для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету 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. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. 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 | Оценка |
|---|---|
| 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 в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.