

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.Б.1.30 Управление информационной безопасностью

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем

Специализация – Безопасность открытых информационных систем

Квалификация выпускника – Специалист по защите информации

Форма обучения – очная

Нормативный срок обучения – 5 лет

Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 180

экзамен 9 курсовая работа 9

Распределение часов дисциплины по семестрам

| Семестр | 9 | Итого |
|--|-------------------------|-------------------------|
| Число недель в семестре | 15 | |
| Вид занятий | Часов по учебному плану | Часов по учебному плану |
| Аудиторная контактная работа по видам учебных занятий | 72 | 72 |
| – лекции | 36 | 36 |
| – практические (семинарские) | 36 | 36 |
| Самостоятельная работа | 72 | 72 |
| Экзамен | 36 | 36 |
| Итого | 180 | 180 |

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.

00a73c5b7b623a969ccad43a81ab346d50 с 08.12.2022 14:32 по 02.03.2024 14:32 GMT+03:00

Подпись соответствует файлу документа



| 1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ | |
|--|---|
| 1.1 Цели освоения дисциплины | |
| 1 | изучение основных понятий, методологии и применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии |
| 1.2 Задачи освоения дисциплины | |
| 1 | приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность; |
| 2 | формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) |
| 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: | |
| <ul style="list-style-type: none"> – 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 | |
|--|--|
| 2.1 Требования к предварительной подготовке обучающегося | |
| 1 | Б1.Б.1.04 Правоведение |
| 2 | Б1.Б.1.06 Основы управленческой деятельности |
| 3 | Б1.Б.1.22 Основы информационной безопасности |
| 4 | Б1.Б.1.15 Безопасность жизнедеятельности |
| 5 | Б2.Б.02(П) Производственная - по получению профессиональных умений и опыта профессиональной деятельности |
| 2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее | |
| 1 | Б2.Б.05(П) Производственная - технологическая |
| 2 | Б2.Б.06(Пд) Производственная - преддипломная |
| 3 | 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-12: способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | |
| Минимальный уровень освоения компетенции | |
| Знать | Методику оценки рисков информационной безопасности |
| Уметь | Решать задачи по оценке рисков реализации угроз через уязвимости |
| Владеть | Методологией оценки рисков угроз информационной безопасности через уязвимости в системе защиты |
| Базовый уровень освоения компетенции | |
| Знать | Основные критерии, методы и меры определения надежности ИС |
| Уметь | Решать задачи по выявлению угроз информационной безопасности на предприятии |
| Владеть | Методиками оценки рисков информационной безопасности |
| Высокий уровень освоения компетенции | |

| | |
|---------|---|
| Знать | Основные средства и методы анализа угроз информационной безопасности |
| Уметь | Решать задачи по локализации угроз информационной безопасности на предприятии |
| Владеть | Навыками применения средств анализа безопасности ИС |

| | |
|---|--|
| ПК-19: способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы | |
| Минимальный уровень освоения компетенции | |
| Знать | Терминологию, основные руководящие и регламентирующие документы в области информационной безопасности |
| Уметь | Проводить анализ угроз безопасности информационных систем |
| Владеть | Профессиональной терминологией в области ИБ |
| Базовый уровень освоения компетенции | |
| Знать | Основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ |
| Уметь | Реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ |
| Владеть | Навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации |
| Высокий уровень освоения компетенции | |
| Знать | Организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации |
| Уметь | Разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации |
| Владеть | Навыками работы с нормативно-правовыми актами |

| | |
|---|--|
| ПК-28: способность управлять информационной безопасностью автоматизированной системы | |
| Минимальный уровень освоения компетенции | |
| Знать | Основные методы управления |
| Уметь | Применять основные методы управления |
| Владеть | Методологией управления |
| Базовый уровень освоения компетенции | |
| Знать | Основные методы системы управления информационной безопасностью |
| Уметь | Применять основные методы системы управления информационной безопасностью |
| Владеть | Методологией системы управления информационной безопасностью |
| Высокий уровень освоения компетенции | |
| Знать | Основные методы управления информационной безопасностью автоматизированной системы |
| Уметь | Применять основные методы управления информационной безопасностью автоматизированной системы |
| Владеть | Навыками применения основных руководящих документов в области управления информационной безопасностью автоматизированной системы |

| | |
|--|---|
| ПСК-4.3: способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы | |
| Минимальный уровень освоения компетенции | |
| Знать | Основы проектирования и эксплуатации систем управления |
| Уметь | Применять основные методы проектирования и эксплуатации систем управления |
| Владеть | Методологией управления информационной безопасностью открытой информационной системы |
| Базовый уровень освоения компетенции | |
| Знать | Нормативно-методические документы регламентирующие проектирование и эксплуатацию систем управления ИБ ОИС |
| Уметь | Применять методологию проектирования и эксплуатации систем управления ИБ ОИС |
| Владеть | Навыками проектирования и эксплуатации системы управления информационной безопасностью открытой информационной системы |
| Высокий уровень освоения компетенции | |
| Знать | Методологию проектирования, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы |
| Уметь | Применять методологию проектирования, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы |
| Владеть | Навыками применения основных руководящих документов по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы |

В результате освоения дисциплины обучающийся должен

| Знать | |
|----------------|--|
| 1 | Основные методы управления информационной безопасностью |
| 2 | Методы аттестации уровня защищенности информационных систем |
| 3 | Основные угрозы безопасности информации и модели нарушителя в информационных системах |
| 4 | Принципы формирования политики информационной безопасности в информационных системах |
| Уметь | |
| 1 | Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите |
| 2 | Разрабатывать модели угроз и нарушителей информационной безопасности информационных систем |
| 3 | Выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем |
| 3 | Оценивать информационные риски в информационных системах |
| 4 | Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем |
| 5 | Разрабатывать частные политики информационной безопасности информационных систем |
| 6 | Контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем |
| 7 | Разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем |
| Владеть | |
| 1 | Навыками анализа информационной инфраструктуры информационной системы и ее безопасности |
| 2 | Методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем |
| 3 | Методами управления информационной безопасностью информационных систем |
| 4 | Методами оценки информационных рисков |
| 5 | Навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем |
| 6 | Навыками участия в экспертизе состояния защищенности информации на объекте защиты |

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр | Часы | Код компетенции | Учебная литература, ресурсы сети «Интернет» |
|-------------|--|---------|------|------------------------------|---|
| | Раздел 1. Система управления информационной безопасностью | | | | |
| 1.1 | Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации /Лек/ | 9 | 4 | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 1.2 | Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» /Ср/ | 9 | 8 | ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 1.3 | Политика безопасности /Пр/ | 9 | 4 | ПК-12 | Л1.1 Л1.2 Л2.2 Э1 Э2 |
| 1.4 | Проработка материала «Политика безопасности» /Ср/ | 9 | 4 | ПК-12 | Л1.1 Л1.3 Л2.1 Э2 |
| 1.5 | Аудит информационной безопасности /Лек/ | 9 | 4 | ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 |
| 1.6 | Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/ | 9 | 4 | ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 1.7 | Организация обеспечения информационной безопасности | 9 | 4 | ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 |

| | | | | | |
|------|--|---|---|----------------|--------------------------------------|
| | автоматизированных систем /Пр/ | | | | Л2.2 Э1 Э2 |
| 1.8 | Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/ | 9 | 2 | ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 1.9 | Средства поддержки процессов управления информационной безопасностью /Лек/ | 9 | 4 | ПК-28, ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| | Раздел 2. Комплексная система защиты информации | | | | |
| 2.1 | Сущность и задачи комплексной системы защиты информации /Лек/ | 9 | 4 | ПСК-4.3 | Л1.2 Л2.1 Л2.2 Э2 |
| 2.2 | Проработка лекционного материала «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ» /Ср/ | 9 | 2 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.3 | Факторы, влияющие на организацию комплексной системы защиты информации. /Пр/ | 9 | 6 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.4 | Проработка материала «Факторы, влияющие на организацию комплексной системы защиты информации. Основные факторы, влияющие на организацию КСЗИ» /Ср/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.5 | Определение компонентов комплексной системы защиты информации /Лек/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л2.2 Э1 Э2 |
| 2.6 | Проработка лекционного материала «Определение компонентов комплексной системы защиты информации» /Ср/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.7 | Определение условий функционирования комплексной системы защиты информации. /Пр/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.8 | Проработка материала «Определение условий функционирования комплексной системы защиты информации» /Ср/ | 9 | 6 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.9 | Разработка модели комплексной системы защиты информации /Лек/ | 9 | 4 | ПК-12, ПК-19 | Л1.1 Л1.3 Л2.2 Э1 |
| 2.10 | Проработка лекционного материала «Разработка модели комплексной системы защиты информации» /Ср/ | 9 | 4 | ПК-12, ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.11 | Технологическое и организационное построение комплексной системы защиты /Пр/ | 9 | 4 | ПК-12, ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 2.12 | Проработка лекционного материала «Технологическое и организационное построение комплексной системы защиты» /Ср/ | 9 | 4 | ПК-12, ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| | Раздел 3. Управление комплексной системой защиты информации | | | | |
| 3.1 | Назначение, структура и содержание управления комплексной системой защиты информации /Лек/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.2 | Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.3 | Принципы и методы планирования комплексной системы защиты информации /Пр/ | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.4 | Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы | 9 | 4 | ПК-28 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |

| | | | | | |
|------|---|---|----|------------------------------------|--------------------------------------|
| | защиты информации» /Ср/ | | | | |
| 3.5 | Сущность и содержание контроля функционирования комплексной системы защиты информации /Лек/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.6 | Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.7 | Общая характеристика подходов к оценке эффективности систем защиты информации /Пр/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.8 | Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.9 | Методы и модели оценки эффективности комплексной системы защиты информации /Лек/ | 9 | 4 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.10 | Методы и модели оценки эффективности комплексной системы защиты информации /Ср/ | 9 | 2 | ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.11 | Проработка теоретической части курсовой работы /Ср/ | 9 | 6 | ПСК-4.3, ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.12 | Разработка практической части курсовой работы /Ср/ | 9 | 6 | ПСК-4.3, ПК-19 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| 3.13 | Защита курсовой работы /Пр/ | 9 | 6 | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |
| | Раздел 4. Контроль знаний | | | | |
| 4.1 | Экзамен | 9 | 36 | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1 Э2 |

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 | Ю.М. Краковский | Информационная безопасность и защита информации: учебное пособие | М: ИрГУПС, 2016 | 50 |
| Л1.2 | Ю.Н. Загинайлов | Теория информационной безопасности и методология защиты информации: учебное пособие [Электронный ресурс] | М. ; Берлин : Директ-Медиа, 2015 | 100% онлайн |

| | | | | |
|---|--|---|--|---------------------------------------|
| | | //biblioclub.ru/index.php?page=book&id=276557 | | |
| Л1.3 | О.В. Прохорова | Информационная безопасность и защита информации: учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331 | Самара: СГА-СУ, 2014 | 100% онлайн |
| 6.1.2 Дополнительная литература | | | | |
| | Авторы, составители | Заглавие | Издательство, год издания | Кол-во экз. в библиотеке/ 100% онлайн |
| Л2.1 | С.А. Нестеров | Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040 | СПб. : Политехнический университет, 2014 | 100% онлайн |
| Л2.2 | А.А. Афанасьев, Л.Т. Веденев, А.А. Воронцов, Э.Р. Газизова | Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/5114 | М. : Горячая линия-Телеком, 2012 | 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 | Глухов Н.И. | 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 (при необходимости) | | | | |
| 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. Помещения для самостоятельной работы обучающихся: – читальные залы; – 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; пометать 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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др. |
| Практическая работа (семинар) | Обобщение, расширение и углубление пройденного лекционного материала. Решение задач, позволяющих закрепить практические навыки студентов. Выступление с докладами (рефератами) по заданной преподавателем теме, формирование навыков самостоятельной работы, анализа основных и вспомогательных литературных источников, публичное выступление и аргументации собственного мнения, а также дискуссия. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в коллоквиумах. Контроль качества усвоения пройденного материала. |
| Курсовая работа | Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции). |
| 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. 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. Ознакомиться со структурой и оформлением реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции). |
| Самостоятельная работа студента | Для успешного выполнения самостоятельной работы, студенту необходимо обратиться к лекционному материалу, основным и дополнительным источникам литературы, указанным в рабочей программе. Если этого будет не достаточно для выполнения поставленного задания, необходимо в обязательном порядке посетить |

| | |
|--|-----------------------------|
| | консультацию преподавателя. |
|--|-----------------------------|

| |
|--|
| 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.Б.1.30 «Управление информационной безопасностью»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости
и промежуточной аттестации по дисциплине
Б1.Б.1.30 «Управление информационной безопасностью»

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

Дисциплина «Управление информационной безопасностью» участвует в формировании компетенций:

ПК-12: способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-19: способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;

ПК-28: способность управлять информационной безопасностью автоматизированной системы;

ПСК-4.3: способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы.

Таблица траекторий формирования у обучающихся компетенций ПК-12, ПК-19, ПК-28, ПСК-4.3 при освоении образовательной программы

| Код компетенции | Наименование компетенции | Индекс и наименование дисциплин, участвующих в формировании компетенции | Семестр изучения дисциплины | Этапы формирования компетенции |
|-----------------|---|--|-----------------------------|--------------------------------|
| ПК-12 | способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | Б1.Б.1.30 Управление информационной безопасностью | 9 | 1 |
| | | Б2.Б.05(П) Производственная - технологическая | А | 2 |
| | | Б2.Б.06(Пд) Производственная - преддипломная | А | 2 |
| | | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | А | 2 |
| ПК-19 | способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы | Б1.Б.1.30 Управление информационной безопасностью | 9 | 1 |
| | | Б2.Б.06(Пд) Производственная - преддипломная | А | 2 |
| | | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | А | 2 |
| ПК-28 | способность управлять информационной безопасностью автоматизированной системы | Б1.Б.1.30 Управление информационной безопасностью | 9 | 2 |
| | | Б2.Б.03(П) Производственная - эксплуатационная | 8 | 1 |
| | | Б2.Б.06(Пд) Производственная - преддипломная | А | 3 |
| | | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | А | 3 |
| ПСК-4.3 | Способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью | Б1.Б.1.30 Управление информационной безопасностью | 9 | 1 |
| | | Б1.Б.1.ДС.04 Виртуальные частные сети | 9 | 1 |

| | | | | |
|--|---------------------------------|--|---|---|
| | открытой информационной системы | Б2.Б.06(Пд) Производственная - преддипломная | A | 2 |
| | | Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты | A | 2 |

Таблица соответствия уровней освоения компетенций ПК-12, ПК-19, ПК-28, ПСК-4.3 планируемым результатам обучения

| Код компетенции | Наименование компетенции | Наименования разделов дисциплины | Уровни освоения компетенций | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции) |
|-----------------|---|--|-----------------------------|--|
| ПК-12 | способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | Раздел 1. Система управления информационной безопасностью Раздел 2. Комплексная система защиты информации Раздел 3. Управление комплексной системой защиты информации Раздел 4. Контроль знаний | Минимальный уровень | Знать: Методику оценки рисков информационной безопасности |
| | | | | Уметь: Решать задачи по оценке рисков реализации угроз через уязвимости |
| | | | | Владеть: Методологией оценки рисков угроз информационной безопасности через уязвимости в системе защиты |
| | | | Базовый уровень | Знать: Основные критерии, методы и меры определения надежности ИС |
| | | | | Уметь: Решать задачи по выявлению угроз информационной безопасности на предприятии |
| | | | | Владеть: Методиками оценки рисков информационной безопасности |
| | | | Высокий уровень | Знать: Основные средства и методы анализа угроз информационной безопасности |
| | | | | Уметь: Решать задачи по локализации угроз информационной безопасности на предприятии |
| | | | | Владеть: Навыками применения средств анализа безопасности ИС |
| ПК-19 | способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы | Раздел 1. Система управления информационной безопасностью Раздел 2. Комплексная система защиты информации Раздел 3. Управление комплексной системой защиты информации Раздел 4. Контроль знаний | Минимальный уровень | Знать: Терминологию, основные руководящие и регламентирующие документы в области информационной безопасности |
| | | | | Уметь: Проводить анализ угроз безопасности информационных систем |
| | | | | Владеть: Профессиональной терминологией в области ИБ |
| | | | Базовый уровень | Знать: Основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ |
| | | | | Уметь: Реализовывать политику ИБ, применять нормативно- |

| | | | | |
|-----------------|--|--|---------------------|---|
| | | | | <p>правовые акты и нормативно-правовые документы в области ИБ</p> <p>Владеть: Навыками разработки документирования, тестирования и отладки программного обеспечения</p> |
| | | | Высокий уровень | <p>Знать: Организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации</p> <p>Уметь: Разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации</p> <p>Владеть: Навыками работы с нормативно-правовыми актами</p> |
| ПК-28 | способность управлять информационной безопасностью автоматизированной системы | Раздел 1. Система управления информационной безопасностью Раздел 2. Комплексная система защиты информации Раздел 3. Управление комплексной системой защиты информации Раздел 4. Контроль знаний | Минимальный уровень | Знать: Основные методы управления |
| | | | | Уметь: Применять основные методы управления |
| | | | | Владеть: Методологией управления |
| | | | Базовый уровень | Знать: Основные методы системы управления информационной безопасностью |
| | | | | Уметь: Применять основные методы системы управления информационной безопасностью |
| | | | | Владеть: Методологией системы управления информационной безопасностью |
| Высокий уровень | Знать: Основные методы управления информационной безопасностью автоматизированной системы | | | |
| | Уметь: Применять основные методы управления информационной безопасностью автоматизированной системы | | | |
| | Владеть: Навыками применения основных руководящих документов в области управления информационной безопасностью автоматизированной системы | | | |
| ПСК-4.3 | Способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы | | Минимальный уровень | Знать: Основы проектирования и эксплуатации систем управления |
| | | | | Уметь: Применять основные методы проектирования и эксплуатации систем управления |
| | | | | Владеть: Методологией управления информационной безопасностью открытой информационной системы |
| | | | Базовый уровень | Знать: Нормативно-методические документы регламентирующие проектирование и эксплуатацию систем управления ИБ ОИС |
| | | | | Уметь: Применять методологию |

| | | | | |
|--|--|--|-----------------|--|
| | | | | проектирования и эксплуатации систем управления ИБ ОИС |
| | | | | Владеть: Навыками проектирования и эксплуатации системы управления информационной безопасностью открытой информационной системы |
| | | | Высокий уровень | Знать: Методологию проектирования, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы |
| | | | | Уметь: Применять методологию проектирования, эксплуатации и совершенствования системы управления информационной безопасностью открытой информационной системы |
| | | | | Владеть: Навыками применения основных руководящих документов по проектированию, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы |

**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) |
|------------------|--------|--|---|---------|---|
| 9 семестр | | | | | |
| 1 | 1 | Текущий контроль | Тема «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» | ПК-12 | Реферат (письменно) |
| 2 | 2 | Текущий контроль | Тема «Политика безопасности» | ПК-12 | Доклад, сообщение (устно) |
| 3 | 2 | Текущий контроль | Тема «Политика безопасности» | ПК-12 | Реферат (письменно) |
| 4 | 2 | Текущий контроль | Тема «Аудит информационной безопасности» | ПК-19 | Реферат (письменно) |
| 5 | 3 | Текущий контроль | Тема «Организация обеспечения информационной безопасности автоматизированных систем» | ПК-19 | Доклад, сообщение (устно) |
| 6 | 3 | Текущий контроль | Тема «Организация обеспечения информационной безопасности автоматизированных систем» | ПК-19 | Реферат (письменно) |
| 7 | 4 | Текущий контроль | Тема «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ» | ПСК-4.3 | Реферат (письменно) |
| 8 | 4 | Текущий контроль | Тема «Факторы, влияющие на организацию комплексной системы защиты информации» | ПСК-4.3 | Доклад, сообщение (устно) |
| 9 | 4 | Текущий контроль | Тема «Факторы, влияющие на организацию комплексной системы защиты информации» | ПСК-4.3 | Реферат (письменно) |

| | | | | | |
|----|----|------------------------------------|---|------------------------------|---|
| | | | Основные факторы, влияющие на организацию КСЗИ» | | |
| 10 | 5 | Текущий контроль | Тема «Определение компонентов комплексной системы защиты информации» | ПК-28 | Реферат (письменно) |
| 11 | 5 | Текущий контроль | Тема «Определение условий функционирования комплексной системы защиты информации» | ПК-28 | Доклад, сообщение (устно) |
| 12 | 5 | Текущий контроль | Тема «Определение условий функционирования комплексной системы защиты информации» | ПК-28 | Реферат (письменно) |
| 13 | 6 | Текущий контроль | Тема «Разработка модели комплексной системы защиты информации» | ПК-12, ПК-19 | Реферат (письменно) |
| 14 | 7 | Текущий контроль | Тема «Технологическое и организационное построение комплексной системы защиты» | ПК-12, ПК-19 | Доклад, сообщение (устно) |
| 15 | 8 | Текущий контроль | Тема «Технологическое и организационное построение комплексной системы защиты» | ПК-12, ПК-19 | Реферат (письменно) |
| 16 | 9 | Текущий контроль | Тема «Назначение, структура и содержание управления комплексной системой защиты информации» | ПК-28 | Реферат (письменно) |
| 17 | 10 | Текущий контроль | Тема «Принципы и методы планирования комплексной системы защиты информации» | ПК-28 | Доклад, сообщение (устно) |
| 18 | 11 | Текущий контроль | Тема «Принципы и методы планирования функционирования комплексной системы защиты информации» | ПК-28 | Реферат (письменно) |
| 19 | 12 | Текущий контроль | Тема «Сущность и содержание контроля функционирования комплексной системы защиты информации» | ПСК-4.3 | Реферат (письменно) |
| 20 | 16 | Текущий контроль | Тема «Общая характеристика подходов к оценке эффективности систем защиты информации» | ПСК-4.3 | Доклад, сообщение (устно) |
| 21 | 14 | Текущий контроль | Тема «Общая характеристика подходов к оценке эффективности систем защиты информации» | ПСК-4.3 | Реферат (письменно) |
| 22 | 15 | Тест | Изученный материал | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Перечень тестовых заданий |
| 23 | 16 | Текущий контроль | Тема «Методы и модели оценки эффективности комплексной системы защиты информации» | ПСК-4.3 | Реферат (письменно) |
| 24 | 17 | Текущий контроль | Защита курсовой работы /Пр/ | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Курсовая работа |
| 25 | 18 | Промежуточная аттестация – экзамен | Разделы: 1. Система управления информационной безопасностью 2. Комплексная система защиты информации 3. Управление комплексной | ПК-12, ПК-19, ПК-28, ПСК-4.3 | Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста. |

| | | | | |
|--|--|--|--|--|
| | | системой защиты информации 4. Контроль знаний | | |
|--|--|--|--|--|

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».

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. 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. 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. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | Фонд тестовых заданий |
| 4 | Курсовая работа | Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях | Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовую работу |
| 5 | Экзамен | Средство, позволяющее оценить знания, умения, навыки и | Перечень |

| | | |
|--|--|--|
| | (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся | теоретических вопросов и практических заданий (билетов) к экзамену |
|--|--|--|

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 |
|---------------------|--|------------------------------|
| «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 |

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. 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 |

Курсовая работа

| Шкала оценивания | Критерии оценивания |
|---------------------|---|
| «отлично» | Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы |
| «хорошо» | Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе |
| «удовлетворительно» | Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсовой работы |

| | |
|-----------------------|---|
| | обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы |
| «неудовлетворительно» | Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы. |

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 | Количество баллов за одно тестовое задание |
|---|--|---|--|
| Минимальный уровень освоения компетенции | 18 | Тестовые задания с выбором одного правильного ответа из нескольких | 18 |
| | | 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 | 9 | Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры) | 36 |
| Высокий уровень освоения компетенции | 6 | Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы | 42 |

Тест (шкала и критерии оценивания, уровни освоения)

| Шкалы оценивания | | Критерии оценивания | Уровень освоения компетенции |
|-----------------------|--------------|--|------------------------------|
| «отлично» | «зачтено» | Обучающийся при тестировании набрал 89-96 баллов | Высокий |
| «хорошо» | | Обучающийся при тестировании набрал 81-88 баллов | Базовый |
| «удовлетворительно» | | Обучающийся при тестировании набрал 73-80 баллов | Минимальный |
| «неудовлетворительно» | «не зачтено» | Обучающийся при тестировании набрал 0-72 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 Основные положения теории управления в системах организационно-технологического типа.
- 2 Основы методологии принятия управленческого решения в системах организационно-технологического типа.
- 3 Требования, предъявляемые к комплексной системе защиты информации.
- 4 Основные этапы разработки комплексной системы защиты информации.
- 5 Факторы, влияющие на организацию комплексной системы защиты информации.
- 6 Порядок нормативного закрепления состава защищаемой информации.
- 7 Определение объектов защиты с точки зрения управления.
- 8 Источники и способы дестабилизирующего воздействия на информацию.
- 9 Каналы и методы несанкционированного доступа к информации.
- 10 Определение компонентов комплексной системы защиты информации.
- 11 Условия функционирования комплексной системы защиты информации.
- 12 Функциональная модель комплексной системы защиты информации.
- 13 Организационная модель комплексной системы защиты информации.
- 14 Информационная модель комплексной системы защиты информации.
- 15 Стадии создания комплексной системы защиты информации.
- 16 Структура и содержание документационного обеспечения стадий создания комплексной системы защиты информации.
- 17 Кадровое обеспечение функционирования комплексной системы защиты информации.
- 18 Нормативно-методическое и материально-техническое обеспечение комплексной системы защиты информации.
- 19 Общая технология управления комплексной системой защиты информации.
- 20 Принципы и методы планирования деятельности комплексной системы защиты информации.
- 21 Принципы и методы контроля функционирования комплексной системы защиты информации.
- 22 Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций.
- 23 Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.
- 24 Вероятностный подход к оценке эффективности комплексной системы защиты информации.
- 25 Статистические и экспертные методы оценки эффективности системы защиты информации.
- 26 Показатели защищенности комплексной системы защиты информации.
- 27 Организация обеспечения информационной безопасности автоматизированных систем
- 28 Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии.

3.2 Перечень типовых тем докладов, сообщений

- 1 Принципы и условия отнесения информации к категории защищаемой;
- 2 Ресурсы предприятия, подлежащие защите с точки зрения ИБ;
- 3 Комплекс методов и средств защиты информации как объект управления ИБ;
- 4 Назначение и содержание политики ИБ предприятия;
- 5 Назначение и содержание структурных подразделений, частных политик безопасности. Средства их реализации;
- 6 Модель нарушителя политики безопасности;

- 7 Частная модель угроз информационной безопасности;
- 8 Типичные угрозы информации и уязвимости корпоративных информационных систем;
- 9 Содержание и организация процесса аудита ИБ;
- 10 Оценка рисков ИБ;
- 11 Отчетные документы по результатам аудита ИБ;
- 12 Выполнение рекомендаций по итогам проведения аудита ИБ;
- 13 Методология защиты информации как теоретический базис построения КСЗИ;
- 14 Принципы организации и этапы разработки комплексной системы защиты информации;
- 15 Принципы организации КСЗИ;
- 16 Основные требования, предъявляемые к КСЗИ;

3.3 Перечень типовых тем курсовых работ

- 1 Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии.
- 2 Основные положения теории управления в системах организационно-технологического типа.
- 3 Основы методологии принятия управленческого решения в системах организационно-технологического типа.
- 4 Требования, предъявляемые к комплексной системе защиты информации.
- 5 Основные этапы разработки комплексной системы защиты информации.
- 6 Факторы, влияющие на организацию комплексной системы защиты информации.
- 7 Порядок нормативного закрепления состава защищаемой информации.
- 8 Определение объектов защиты.
- 9 Источники и способы дестабилизирующего воздействия на информацию.
- 10 Каналы и методы несанкционированного доступа к информации.
- 11 Определение компонентов комплексной системы защиты информации.
- 12 Условия функционирования комплексной системы защиты информации.
- 13 Функциональная модель комплексной системы защиты информации.
- 14 Организационная модель комплексной системы защиты информации.
- 15 Информационная модель комплексной системы защиты информации.
- 16 Стадии создания комплексной системы защиты информации.
- 17 Структура и содержание документационного обеспечения стадий создания комплексной системы защиты информации.
- 18 Кадровое обеспечение функционирования комплексной системы защиты информации.
- 19 Нормативно-методическое и материально-техническое обеспечение комплексной системы защиты информации.
- 20 Общая технология управления комплексной системой защиты информации.
- 21 Принципы и методы планирования деятельности комплексной системы защиты информации.
- 22 Принципы и методы контроля функционирования комплексной системы защиты информации.
- 23 Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций.
- 24 Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.
- 25 Вероятностный подход к оценке эффективности комплексной системы защиты информации.
- 26 Статистические и экспертные методы оценки эффективности системы защиты информации.
- 27 Показатели защищенности комплексной системы защиты информации.
- 28 Организация обеспечения информационной безопасности автоматизированных систем

3.4 Тест

Низкий

1. Выберите функции управления

- а) Планирование+
- б) Организация+
- в) Мотивация+
- г) Развитие
- д) Контроль+

2 Методы анализа конфликт логических данных:

- статистический метод;+
- математический метод;+
- системно-экспертный метод;
- исторический анализ;+
- компаративный анализ.+

3 Выбрать стадии реализации системы управления информационной безопасностью:

- а) формирование политики в области рисков.+
- б) анализ бизнес-процессов.+
- в) согласование рисков с экспертами
- г) анализ рисков.+
- д) формирование целевой концепции.+

4. Какие пункты включает «Замкнутый жизненный цикл системы управления информационной безопасностью»

- а) Аудит СУИБ+
- б) Корректировка мер по минимизации рисков ИБ+
- в) планирование мер по минимизации рисков ИБ+
- г) согласование запланированных мер
- д) проверка +

5. СУИБ включает в себя:

- а) организационную структуру,+
- б) политики,+
- в) распределение прав и обязанностей,
- г) осуществление на практике,+
- д) процессы и ресурсы+

8. Назовите методы управления информационной безопасности

- а) административные+
- б) инженерно-технические+
- в) правовые+
- г) теоретические+
- д) экономические+
- е) социально-педагогические

9. Типы мотивов в коллективе

- а) мотив как внутренне осознанные потребности;+
- б) мотив как внешняя осознанная потребность;
- в) мотив как инструмент удовлетворения потребности +
- г) мотив как намерение, побуждающее поведение; +

10. Мероприятия для обеспечения защиты информации в автоматизированной системе управления

- а) формирование требований к защите информации в автоматизированной системе управления;+

- б) разработка системы защиты автоматизированной системы управления;+

- в) согласование системы защиты автоматизированной системы управления и ввод ее в действие;

- г) обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;+

- д) обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления. +

11 Разработка системы защиты автоматизированной системы управления включает

- а) проектирование системы защиты автоматизированной системы управления; +

- б) согласование системы защиты автоматизированной системы управления

- в) разработку эксплуатационной документации на систему защиты автоматизированной системы управления. +

12. Признаки конфликта

- а) наличие ситуации, которая воспринимается участниками как конфликтная; +

- б) неделимость объекта конфликта, т.е. объект конфликта не может быть поделено между участниками конфликтного взаимодействия; +

- в) желание участников прекратить конфликтную взаимодействие для достижения своих целей.

13 Угрозы безопасности информации определяются на каждом из уровней автоматизированной системы управления по результатам:

- а) оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей;+

- б) анализа возможных уязвимостей автоматизированной системы управления;+

- в) анализа возможных способов реализации угроз безопасности информации и последствий от нарушения как отдельных свойств безопасности информации, так и автоматизированной системы управления в целом;+

- г) анализа текущей модели нарушителя ИБ.

14 Методы руководства коллективом

- а) авторитарный+

- б) либерально-попустительский+

- в) демократический+

- г) власть провокации

- д) власть вознаграждения;+

- е) власть эксперта+

15. Основные требования к системе защиты автоматизированной системы управления должны содержать:

- а) класс защищенности автоматизированной системы управления; +

- б) перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления; +

- в) объекты защиты автоматизированной системы управления на каждом из ее уровней; +

- г) требования к мерам защиты информации, применяемым в автоматизированной системе управления;

- д) требования к защите информации при взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;

16. При проектировании системы защиты автоматизированной системы управления необходимо:

- а) определять типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места,

промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа); +

б) определять методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления; +

в) выбирать меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления; +

г) определять виды и типы средств защиты информации, обеспечивающие реализацию технических каналов утечки информации;

д) определять структуру системы защиты автоматизированной системы управления.

17. Внедрение системы защиты автоматизированной системы управления включает:

а) настройку программного обеспечения автоматизированной системы управления; +

б) согласование программного обеспечения автоматизированной системы управления с ФАПСИ;

в) разработку документов, определяющих правила и процедуры (политики), реализуемые оператором для обеспечения защиты информации в автоматизированной системе управления в ходе ее эксплуатации; +

г) внедрение организационных мер защиты информации; +

18. Методы сбора конфликтологической информации

а) Наблюдение; +

б) изучение документов; +

в) опрос; +

г) метод case-study-probably;

д) экспертная оценка +

ж) оценка возможности реализации угроз безопасности информации в автоматизированной системе управления.

Средний

1 «Управление информационной безопасностью» это _____ (Ответ циклический) процесс, включающий осознание _____ (Ответ степени необходимости) защиты информации и постановку задач; сбор и анализ данных о _____ (Ответ состоянии) информационной безопасности в организации; оценку информационных _____ (Ответ рисков); планирование мер по обработке рисков; _____ и _____ (Ответ реализацию и внедрение) соответствующих механизмов _____ (Ответ контроля), распределение ролей и ответственности, _____ и _____ (Ответ обучение и мотивацию) персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов _____ (Ответ контроля), оценку их эффективности и соответствующие корректирующие воздействия.

2 Основная цель СУИБ это _____ (Ответ защита) бизнес-процессов и _____ (Ответ знаний компании) от уничтожения или утечки

3 Оценка эффективности системы управления информационной безопасностью это _____ (Ответ системный процесс) получения и _____ (Ответ оценки объективных) данных о текущем состоянии систем, действиях и событиях происходящих в ней, устанавливающий уровень их соответствия определенным критериям

4 Рекомендации аудитора должны быть _____ и _____ (Ответ конкретными и применимыми) к данной информационной системе, _____ (Ответ экономически) обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности.

5 Социальный конфликт это _____ или _____ (явное или скрытое) состояние противоборства объективно расходящихся интересов, _____ и _____ (Ответ целей и

тенденций) развития социальных объектов, _____ и _____ (Ответ прямое и косвенное) столкновение социальных сил на почве противодействия существующему общественному порядку, особая форма исторического движения к новому социальному единству.

6 Систем управления информационной безопасностью это часть системы _____ (Ответ менеджмента), основанная на анализе _____ (Ответ рисков) и предназначенная для _____, _____ (Ответ создания, внедрения) выполнения, мониторинга, пересмотра, поддержания и повышения уровня ИТ-безопасности.

7 Методы управления информационной безопасностью — это совокупность _____ и _____ (Ответ приемов и способов) воздействия на _____ (Ответ управляемый) объект для достижения поставленных целей.

8 «Управление информацией» в системе обработки информации – это функция _____ (ответ управления) получением, _____, (Ответ анализом,) сохранением, обновлением и распределением информации.

9 «Социально-психологические методы» это способы осуществления _____ (Ответ управленческих) воздействий на _____ (Ответ персонал), основанные на использовании закономерностей _____ и _____ (Ответ социологии и психологии).

Высокий

- 1 Дайте развернутую характеристику руководителю среднего звена
- 2 раскройте разновидности подходов в управлении (не менее 3 разновидностей):
- 3 Процедуры выбора
4. Охарактеризуйте CRAMM
6. Охарактеризуйте методы мотивации как функцию управленческой деятельности

3.5 Перечень теоретических вопросов к зачету

- 1 Сущность организации производства.
- 2 Промышленное предприятие как система.
- 3 Функции, уровни и общие принципы организации управления предприятием.
- 4 Информационное обеспечение системы управления.
- 5 Информационные ресурсы и конфиденциальность информации.
- 6 Офисная деятельность как особый вид управленческой деятельности
- 7 Структура и функции офисной деятельности
- 8 Сущность и задачи комплексной системы защиты информации
- 9 Организация и особенности основных функций управления в комплексной системе защиты информации.
- 10 Этапы работы по созданию КСЗИ на предприятии.
- 11 Факторы, влияющие на организацию КСЗИ.
- 12 Порядок действий по нормативному закреплению состава защищаемой информации.
- 13 Определение и нормативное закрепление состава защищаемой информации.
- 14 Определение объектов защиты.
- 15 Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.

3.6 Перечень типовых простых практических заданий к зачету

- 1 Проведение аудита информационной безопасности организации ООО «ВСЦ ЕВРААС» для оценки ее состояния защищенности.
- 2 Оценка рисков реализации угроз через уязвимости в системе защиты информационных ресурсов ООО «ВСЦ ЕВРААС».
- 3 Оценка эффективности состояния защищенности информационных ресурсов ООО «ВСЦ ЕВРААС».
- 4 Разработка концепции информационной безопасности ООО «ВСЦ ЕВРААС».

5 Разработка локальных нормативно-правовых актов ООО «ВСЦ ЕВРААС».

3.7 Перечень теоретических вопросов к экзамену

- 1 Определение потенциальных каналов и методов несанкционированного доступа к информации.
- 2 Определение возможностей несанкционированного доступа к защищаемой информации.
- 3 Определение компонентов КСЗИ.
- 4 Определение условий функционирования КСЗИ.
- 5 Разработка модели КСЗИ
- 6 Методика добывания информации для предприятия.
- 7 Методы отбора информации.
- 9 Методы анализа информации.
- 10 Образцы документов при добывании информации.
- 11 Технологическое и организационное построение КСЗИ
- 12 Кадровое обеспечение функционирования КСЗИ
- 13 Материально-техническое и нормативно-методическое обеспечение КСЗИ
- 14 Назначение, структура и содержание управления КСЗИ
- 15 Принципы и методы планирования функционирования КСЗИ
- 16 Сущность и содержание контроля функционирования КСЗИ
- 17 Управление КСЗИ в условиях чрезвычайных ситуаций
- 18 Общая характеристика подходов к оценке эффективности систем защиты информации
- 19 Методы и модели оценки эффективности КСЗИ
- 20 Основные цели и задачи проведения аудита
- 21 Анализ рисков компании.
- 22 Как оценить уровень безопасности КИС
- 23 Возможные виды аудита безопасности
- 24 Возможные методики аудита безопасности КИС
- 25 Стандарты информационной безопасности
- 26 Структура СТБК
- 27 Структура стандарта ГОСТ Р ИСО/МЭК 17799 -2005

3.8 Перечень типовых простых практических заданий к экзамену

- 1 Разработка отдельных разделов политики ИБ городской администрации г. Иркутска
- 2 Подготовка стадий создания комплексной системы защиты информации ООО «ВСЦ ЕВРААС».
- 3 Подготовка ТЗ на создание КСЗИ аппарата Губернатора Иркутской области и Правительства Иркутской области
- 4 Построение частной модели угроз защищаемой информации на ООО «Рога и Копыта» коммерческой структуры Северного Кавказа для обеспечения потребностей населения в сувенирах с выделкой рогов диких животных. Установлен режим коммерческой тайны. Необходимо проанализировать состояние защищенности коммерческих сведений с выделением уязвимостей и угроз.
- 5 Подготовка модели внутреннего нарушителя ООО «ВСЦ ЕВРААС».
- 6 Подготовка модели внешнего нарушителя ООО «ВСЦ ЕВРААС».
- 7 Подбор и отбор персонала для работы с конфиденциальными документами аппарата Губернатора Иркутской области и Правительства Иркутской области

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 | Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат или по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,2; предоставляет реферат преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся. |
| Сообщение, доклад | Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся. |
| Тест | Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся. |
| Курсовая работа | Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся. |

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) 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/экзамену для оценки знаний;
- перечень типовых простых практических заданий к зачету/экзамену для оценки умений;
- перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену 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. Билеты составлены таким образом, что в 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; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье 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 ФОС на бумажном носителе в составе ФОС по дисциплине.

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.

Образец экзаменационного билета

| | | |
|---|---|--|
|  <p>ИрГУПС 20__-20__ учебный год</p> | <p>Экзаменационный билет № 1 по дисциплине «Управление информационной безопасностью» __ семестр</p> | <p>Утверждаю: Заведующий кафедрой «ИСИЗИ» ИрГУПС _____</p> |
| <ol style="list-style-type: none"> 1. Определение потенциальных каналов и методов несанкционированного доступа к информации. 2. Основные цели и задачи проведения аудита. 3. Подготовка модели внутреннего нарушителя ООО «ВСЦ ЕВРААС» | | |

В разделе «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» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.