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.05 Методология анализа информационных рисков

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. – 4
Часов по учебному плану – 144

Формы промежуточной аттестации в семестрах:
экзамен 8

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**54**	**54**
– лекции	18	**18**
– практические (семинарские)	36	**36**
Самостоятельная работа	**54**	**54**
Экзамен	**36**	**36**
Итого	**144**	**144**

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

1	Раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации.
2	Определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации.

1.2 Задачи освоения дисциплины

1	Изучить понятие «информационных активов» как основной характеристики системы оценки информационных рисков хозяйствующего субъекта.
2	Определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия.
3	Оценить существующие методические подходы к оценке информационных рисков для выявления возможностей совершенствования данной деятельности.
4	Изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта.
5	Освоить методические положения по совершенствованию деятельности в сфере оценки информационных рисков хозяйствующих субъектов.
6	Освоить методические подходы к оценке эффективности деятельности по защите информационных активов предприятия.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.

Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

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

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

Изучение дисциплины «Методология анализа информационных рисков» основывается на знаниях и умениях обучающихся, полученных при изучении следующих дисциплин:

1	Б1.Б.1.22 Основы информационной безопасности
2	Б1.В.ДВ.07.01 Экономика защиты информации
3	Б1.В.ДВ.07.02 Методология определения ценности информации

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.В.06 Комплексная защита в информационных системах персональных данных
2	Б1.Б.1.30 Управление информационной безопасностью
3	Б2.Б.04(Н) Производственная - научно-исследовательская работа
4	Б2.Б.06(Пд) Производственная - преддипломная
5	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-3: способностью проводить анализ защищенности автоматизированных систем	
Минимальный уровень освоения компетенции	
Знать	цели и задачи анализа и управления информационной безопасностью; актуальность и необходимость обеспечения и поддержания информационной безопасности на предприятии;
Уметь	определять уровень значимости и критичности информации;
Владеть	методами оценки уровня значимости и критичности информационных активов предприятия.
Базовый уровень освоения компетенции	
Знать	свойства защищенности информации и методы их оценки; принципы создания защищенных информационных (автоматизированной) систем;
Уметь	определять класс защищенности информационной (автоматизированной) системы предприятия;
Владеть	методы определения класса защищенности информационной (автоматизированной) системы предприятия.
Высокий уровень освоения компетенции	
Знать	методы анализа, критерии и требования к защищенности (безопасности) информационных (автоматизированной) систем;
Уметь	проводить комплексный (системный) анализ защищенности информационных (автоматизированной) систем;
Владеть	методологией оценки безопасности (защищенности) информационных технологий по общим критериям.

ПК-4: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	нормативно-правовую базу информационной безопасности, отечественные и международные требования по информационной безопасности;
Уметь	описывать существующие активы, в том числе информационные) предприятия; ранжировать активы по степени ценности; выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия (разрабатывать модели уязвимостей);
Владеть	методами определения ценности материальных и нематериальных активов предприятия, возможного ущерба при реализации угрозы информационной безопасности;
Базовый уровень освоения компетенции	
Знать	виды угроз информационной безопасности, способы их реализации и источники;
Уметь	разрабатывать модели угроз и нарушителя информационной безопасности автоматизированной системы;
Владеть	существующими подходами к построению моделей угроз и моделей нарушителя информационной безопасности автоматизированной системы.
Высокий уровень освоения компетенции	
Знать	типовые модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
Уметь	описывать жизненный цикл и профиль угрозы информационной безопасности; разрабатывать комплекс мероприятий по организации защиты информационной (автоматизированной системы) предприятия;
Владеть	методами определения затрат на информационную безопасность с учетом требуемого уровня защищенности.

ПК-5: способностью проводить анализ рисков информационной безопасности автоматизированной системы
Минимальный уровень освоения компетенции

Знать	уязвимости автоматизированной (информационной) системы; слабости системных утилит, команд и сервисов; слабости современных технологий программирования;
Уметь	выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты, в том числе риски информационной безопасности автоматизированной системы;
Владеть	стандартами в области анализа и управления рисками информационной безопасности автоматизированной системы.
Базовый уровень освоения компетенции	
Знать	понятие аудита безопасности; методы анализа данных при аудите информационной безопасности;
Уметь	проводить анализ рисков информационной безопасности предприятия и имеющейся автоматизированной системы;
Владеть	системным подходом к анализу и управлению рисками информационной безопасности автоматизированной системы;
Высокий уровень освоения компетенции	
Знать	основные подходы к анализу рисков информационной безопасности автоматизированной системы; методы оценивания уровней информационных рисков.
Уметь	определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия;
Владеть	навыками работы со специальными программными системами управления информационными рисками предприятия.

В результате освоения дисциплины обучающийся должен

Знать	
1	роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;
2	существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов;
3	особенности и проблемы организационного направления в деятельности по защите информационных активов;
4	методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков;
5	основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия.
Уметь	
1	определять состав, важность и ценность конфиденциальной информации применительно к видам тайны;
2	выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты;
3	разрабатывать модели угроз и нарушителя информационной безопасности предприятия;
4	определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия;
5	планировать все этапы управления информационными рисками предприятия, а также затраты на внедрение контрмер.
6	организовывать системное обеспечение защиты информации.
Владеть	
1	основами информационной безопасности и защиты информации; специальной профессиональной терминологией;
2	основными методами выявления информационных рисков реализации угроз конфиденциальной информации;
3	методами определения уровня информационных рисков;
4	методами оценки возврата инвестиций от реализации контрмер по защите информации, и их эффективности;
5	навыками работы со специальными программными комплексами управления информационными рисками предприятия.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»

	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.				
1.1	Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л4.1
1.2	Построение диаграммы Исикавы – инструмента анализа качества и безопасности, в данном контексте – информационной системы. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Э2, Э3
1.3	Построение модели нарушителя. Структурный метод Каппнера-Трего. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Э2, Э3
1.4	Термины и определения в области управления информационными рисками. /Ср/	8	4	ПК-3, ПК-4, ПК-5	Л4.1, Э2, Э3
1.5	Антология кибератак. Наихудшие сценарии кибератак. /Ср/	8	2	ПК-3, ПК-4, ПК-5	Л4.1
	Раздел 2. Основные этапы и элементы управления рисками и их оценки.				
2.1	Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э2, Э3
2.2	Идентификация активов (описание бизнес-процессов). /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
2.3	Определение ценности активов (критерии оценки ущерба, таблица ценности активов). /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
2.4	Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э2, Э3
2.5	Анализ угроз. Описание угроз безопасности. Профиль и жизненный цикл угрозы. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
2.6	Анализ уязвимостей. Идентификация организационных уязвимостей. идентификация технических уязвимостей. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
2.7	Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM.	8	4	ПК-3, ПК-4, ПК-5	Л4.1, Э3

	/Ср/				
2.8	Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. распределение ответственности за управление рисками. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э2, Э3
2.9	Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков. /Пр/	8	4	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
2.10	Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э3
2.11	Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3
2.12	Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций. /Пр/	8	4	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э2, Э3
2.13	Декларация о применимости механизмов контроля. /Ср/	8	2	ПК-3, ПК-4, ПК-5	Л4.1, Э2, Э3
	Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.				
3.1	Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э2, Э3
3.2	Качественная оценка информационного риска по трехфакторной модели с помощью специального программного средства. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л4.2

3.3	Программные продукты для управления рисками информационной безопасности. /Ср/	8	4	ПК-3, ПК-4, ПК-5	Л3.1, Л4.1
3.4	Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л3.1, Э3
3.5	Исследование организационной защиты информационных активов предприятия. /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л3.1, Э3
3.6	Оценка процессов СУИБ на соответствие ISO 27001 /Пр/	8	2	ПК-3, ПК-4, ПК-5	Л3.1, Л4.1, Э1
3.7	Законодательные и нормативные акты Российской Федерации в области защиты информации. /Ср/	8	2	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1
3.8	Изучение документов ГТК (защита от несанкционированного доступа к информации). /Ср/	8	2	ПК-3, ПК-4, ПК-5	Э1
3.9	BS ISO/IEC 27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 И ISO/IEC 27005:2008 /Ср/	8	8	ПК-3, ПК-4, ПК-5	Л3.1, Л4.1, Э1, Э2, Э3
	Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.				
4.1	Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л3.1, Л4.1
4.2	Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность. /Пр/	8	6	ПК-3, ПК-4, ПК-5	Л3.1
4.3	Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта. /Лек/	8	2	ПК-3, ПК-4, ПК-5	Л2.2, Л3.1, Л4.1, Э3
4.4	Методические подходы к оценке затрат на	8	2	ПК-3, ПК-4,	Л2.2, Л3.1,

	обеспечение защищенности информационных активов хозяйствующего субъекта. /Пр/			ПК-5	Л4.1
4.5	Проработка лекционного материала. Подготовка к промежуточному тестированию. /Ср/	8	8	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э1, Э2, Э3, Э4, Э5, Э6, Э7
4.6	Подготовка к экзамену. /Ср/	8	18	ПК-3, ПК-4, ПК-5	Л1.1, Л2.1, Л2.2, Л2.3, Л3.1, Л4.1, Э1, Э2, Э3, Э4, Э5, Э6, Э7
4.7	Экзамен.	8	36		

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	Никитин И.А., Цулая М.Т.	Процессы анализа и управления рисками в области ИТ : учебное пособие. - 2-е изд. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=429089	М. : ИНТУИТ, 2016.	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке / 100% онлайн
Л2.1	Аверченков В.И.	Аудит информационной безопасности : учебное пособие для вузов. - 2-е изд. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=93245	М. : Флинта, 2011.	100 % онлайн
Л2.2	Анисимов А.А.	Менеджмент в сфере информационной безопасности : курс лекций. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=232981	М. : Интернет-Университет ИТ, 2009	100 % онлайн
Л2.3	Нестеров С.А.	Анализ и управление рисками в информационных системах на базе	М. : Интернет-Университет	100 % онлайн

		операционных систем : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id =234529	ИТ, 2009.	
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке / 100% онлайн
Л3.1	Н.И. Глухов	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: ИрГУПС, 2013.	67
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	Астахов А.М.	Искусство управления информационными рисками : учебное пособие.	М.: ДМК Пресс, 2010. / Личный кабинет	100% онлайн
Л4.2	Краковский Ю.М.	Методика определения информационных рисков	Личный кабинет	100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	
Э.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
Э.2	Википедия: свободная энциклопедия. https://ru.wikipedia.org/wiki/Заглавная_страница
Э.3	Национальный открытый университет ИНТУИТ http://www.intuit.ru
Э.4	Средства защиты информации http://www.suritel.ru
Э.5	Код безопасности. Средства защиты информации http://www.securitycode.ru
Э.6	Методики и технологии управления информационными рисками http://citforum.ru/security/articles/risk/
Э.7	Искусство управления информационной безопасностью http://www.iso27000.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	Не предусмотрено
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система Консультант Плюс http://www.consultant.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, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины.

	Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: Microsoft Office 2010, Open Office 3.0.1, 7-zip, Borland Delphi 7, Adobe Reader XI, Microsoft Security Essentials.
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.

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.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Решение задач на закрепление практических навыков. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях и коллоквиумах. Контроль качества усвоения пройденного материала.
Самостоятельная работа	Эффективное освоение дисциплины предполагает самостоятельную внеаудиторную работу, которая включает в себя изучение предлагаемого в рабочей программе и самостоятельно найденного материала по соответствующим разделам и темам для дополнения конспектов лекций, подготовки к практическим занятиям. Для более глубокого освоения дисциплины рекомендуется пользоваться учебной литературой, приведенной в рабочей программе дисциплины. Если какие-либо разделы и темы освоить не удается, а также возникают трудности в выполнении практических работ, необходимо пройти консультацию у преподавателя.
Тест	Тест – система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Итоговый тест по дисциплине включает 18 вопросов. Максимальное число баллов 100. Отводимое время на тест – 80 минут.
Конспект	Конспект – средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Основу конспекта составляет лекционный материал. Основа должна быть дополнена самостоятельно проработанным материалом. Конспект может быть использовано для оценки знаний и умений обучающихся. Преподаватель на лекции доводит до сведения обучающихся тему конспекта и указывает необходимую учебную литературу. Темы и перечень литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспекты должны быть выполнены в установленный преподавателем срок. Конспекты сдаются на проверку. Предусматривается выполнение конспектов по всем темам дисциплины.
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.05 «Методология анализа информационных рисков»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

Б1.В.05 «Методология анализа информационных рисков»

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

Дисциплина «Информационная безопасность открытых систем» участвует в формировании компетенции:

ПК-3: способностью проводить анализ защищенности автоматизированных систем;

ПК-4: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

ПК-5: способностью проводить анализ рисков информационной безопасности автоматизированной системы.

1.1 Таблица траекторий формирования у обучающихся компетенций ПК-3; ПК-4; ПК-5 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-3	способностью проводить анализ защищенности автоматизированных систем	Б1.В.05 Методология анализа информационных рисков	8	1
		Б2.Б.04(Н) Производственная - научно-исследовательская работа	А	2
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Б1.Б.1.22 Основы информационной безопасности	3	1
		Б1.В.05 Методология анализа информационных рисков	8	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.04(Н) Производственная - научно-исследовательская работа	А	4
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	Б1.В.ДВ.07.01 Экономика защиты информации	7	1
		Б1.В.ДВ.07.02 Методология определения ценности информации	7	1
		Б1.В.05 Методология анализа информационных рисков	8	2
		Б2.Б.04(Н) Производственная - научно-исследовательская работа	А	3
		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

1.2 Таблица соответствия уровней освоения компетенций ПК-3; ПК-4; ПК-5 планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-3	способностью проводить анализ защищенности автоматизированных систем	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия. Раздел 2. Основные этапы и элементы управления рисками и их оценки. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов. Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.	Минимальный уровень	**Знать:** цели и задачи анализа и управления информационной безопасностью; актуальность и необходимость обеспечения и поддержания информационной безопасности на предприятии. **Уметь:** определять уровень значимости и критичности информации. **Владеть:** методами оценки уровня значимости и критичности информационных активов предприятия.
			Базовый уровень	**Знать:** свойства защищенности информации и методы их оценки; принципы создания защищенных информационных (автоматизированной) систем. **Уметь:** определять класс защищенности информационной (автоматизированной) системы предприятия. **Владеть:** методы определения класса защищенности информационной (автоматизированной) системы предприятия.
			Высокий уровень	**Знать:** методы анализа, критерии и требования к защищенности (безопасности) информационных (автоматизированной) систем. **Уметь:** проводить комплексный (системный) анализ защищенности

				информационных (автоматизированной) систем. **Владеть**: методологией оценки безопасности (защищенности) информационных технологий по общим критериям.
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия. Раздел 2. Основные этапы и элементы управления рисками и их оценки. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов. Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.	Минимальный уровень	**Знать**: нормативно-правовую базу информационной безопасности, отечественные и международные требования по информационной безопасности. **Уметь**: описывать существующие активы, в том числе информационные) предприятия; ранжировать активы по степени ценности; выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия (разрабатывать модели уязвимостей). **Владеть:** методами определения ценности материальных и нематериальных активов предприятия, возможного ущерба при реализации угрозы информационной безопасности.
			Базовый уровень	**Знать**: виды угроз информационной безопасности, способы их реализации и источники. **Уметь**: разрабатывать модели угроз и нарушителя информационной безопасности автоматизированной системы. **Владеть**: существующими подходами к построению моделей угроз и моделей нарушителя информационной безопасности автоматизированной системы.

			Высокий уровень	**Знать**: типовые модели угроз и модели нарушителя информационной безопасности автоматизированной системы. **Уметь**: описывать жизненный цикл и профиль угрозы информационной безопасности; разрабатывать комплекс мероприятий по организации защиты информационной (автоматизированной системы) предприятия. **Владеть**: методами определения затрат на информационную безопасность с учетом требуемого уровня защищенности.
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия. Раздел 2. Основные этапы и элементы управления рисками и их оценки. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов. Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.	Минимальный уровень	**Знать:** уязвимости автоматизированной (информационной) системы; слабости системных утилит, команд и сервисов; слабости современных технологий программирования. **Уметь:** выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты, в том числе риски информационной безопасности автоматизированной системы. **Владеть:** стандартами в области анализа и управления рисками информационной безопасности автоматизированной системы.
			Базовый уровень	**Знать:** понятие аудита безопасности; методы анализа данных при аудите информационной безопасности. **Уметь:** проводить анализ рисков информационной безопасности предприятия и имеющейся автоматизированной системы.

				Владеть: системным подходом к анализу и управлению рисками информационной безопасности автоматизированной системы.
			Высокий уровень	**Знать:** основные подходы к анализу рисков информационной безопасности автоматизированной системы; методы оценивания уровней информационных рисков. **Уметь:** определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия. **Владеть:** навыками работы со специальными программными системами управления информационными рисками предприятия.

1.3 Программа контрольно-оценочных мероприятий за период изучения дисциплины

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.

№	Неделя	Наименование оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
1	2	3	4	5	6
1	2, 3	Текущий контроль	Тема «Понятие риск. Информационные риски киберпространства».	ПК-3; ПК-4; ПК-5	Конспект (письменно). Собеседование (устно)
2	4, 5	Текущий контроль	Тема «Основные элементы управления рисками информационной безопасности».	ПК-3; ПК-4; ПК-5	Конспект (письменно). Собеседование (устно)
3	6, 7	Текущий контроль	Тема «Система управления информационными рисками».	ПК-3; ПК-4; ПК-5	Конспект (письменно). Собеседование (устно)
4	8	Текущий контроль	Тема «Обработка рисков информационной безопасности».	ПК-3; ПК-4;	Конспект (письменно)

				ПК-5	
5	9, 10	Текущий контроль	Тема «Методические подходы к оценке информационных рисков хозяйствующих субъектов».	ПК-3; ПК-4; ПК-5	Конспект (письменно). Собеседование (устно)
7	11	Текущий контроль	Тема «Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта».	ПК-3; ПК-4; ПК-5	Собеседование (устно)
	12	Текущий контроль	Тема «Многофакторная модель оценки информационных рисков хозяйствующего субъекта».	ПК-3; ПК-4; ПК-5	Конспект (письменно)
8	13-16	Текущий контроль	Тема «Обзор методов и инструментальных средств управления рисками».	ПК-3; ПК-4; ПК-5	Сообщение, доклад, презентация (интерактивная форма)
9	2-17	Текущий контроль	«Оценка рисков информационной безопасности».	ПК-3; ПК-4; ПК-5	Комплект разно-уровневых задач и заданий (письменно)
15	18	Промежуточный контроль – экзамен	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия. Раздел 2. Основные этапы и элементы управления рисками и их оценки. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов. Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.	ПК-3; ПК-4; ПК-5	Собеседование (устно), комплект экзаменационных билетов

1.4 Перечень используемых оценочных средств для текущего контроля успеваемости с описанием показателей и критериев оценивания результатов обучения, описанием шкал оценивания, типовыми контрольными заданиями и методическими материалами, определяющими процедуру оценивания результатов

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. Текущий контроль позволяет получать первичную информацию о ходе и качестве усвоения учебного материала, а также стимулировать регулярную целенаправленную работу обучающихся.

В ходе текущего контроля проводится оценивание результатов усвоения отдельных тем. Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Результаты оценивания заносятся преподавателем в журнал и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

В ходе текущего контроля успеваемости используются различные формы оценочных средств, соответствующие программе контрольно-оценочных мероприятий на период изучения дисциплины.

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
Текущий контроль успеваемости			
1	Конспект	Средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Рекомендуется для оценки знаний и умений обучающихся	Темы конспектов по дисциплине
2	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Рекомендуется для оценки знаний, умений и владений обучающихся	Комплект вопросов для устного опроса учащихся по разделам / темам дисциплины
3	Сообщение, доклад и презентация	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.	Темы докладов, сообщений.
4	Разноуровневые задачи и задания	Различают задачи и задания: – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; – реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением при- чинно-следственных связей; – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разноуровневых задач и заданий

Конспект

Преподаватель не мене, чем за неделю до срока выполнения конспекта должен довести до сведения обучающихся тему конспекта и указать необходимую учебную литературу. Темы и перечень необходимой учебной литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспект должен быть выполнены в установленный преподавателем срок. Конспекты в назначенный срок сдаются на проверку.

Типовые контрольные задания

Темы конспектов, предусмотренных рабочей программой дисциплины:

Тема «Понятие риск. Информационные риски киберпространства»:

1. Понятие риска.
2. Риски, породившие мировой финансовый кризис.
3. Кибертерроризм: риски промышленных систем; риски утечки информации; риски электронных расчетов.
4. Точка зрения правоохранительных органов на киберугрозы.
5. Оценка рисков как основа корпоративного управления.

Тема «Основные элементы управления рисками информационной безопасности».

1. Стандарты в области управления рисками информационной безопасности (ИБ).
2. Оценка риска.

2.1. Количественное определение величины риска.

2.2. Качественное определение величины риска.

3. Информационная составляющая бизнес-рисков
4. Активы организации как ключевые факторы риска.
5. Подходы к управлению рисками.

5.1. Уровни зрелости бизнеса в отношении рисков.

5.2. Анализ факторов риска.

Тема «Система управления информационными рисками».

1. Структура документации по управлению рисками.
2. Политика и контекст управления рисками.
3. Структура системы управления рисками.
4. Непрерывная деятельность по управлению рисками.

4.1. Сопровождение и мониторинг механизмов безопасности.

4.2. Анализ со стороны руководства.

4.3. Пересмотр и переоценка риска.

4.4. Взаимосвязь процессов аудита и управления рисками.

4.5. Управление документами и записями.

4.6. Корректирующие и превентивные меры.

4.7. Коммуникация рисков.

5. Аутсорсинг процессов управления рисками.
6. Распределение ответственности за управление рисками.

Тема «Обработка рисков информационной безопасности».

1. Процесс обработки рисков.
2. Способы обработки риска.

2.1. Принятие риска.

2.2. Уменьшение риска.

2.3. Передача риска.

2.4. Избежание риска.

3. Оценка возврата инвестиций в информационную безопасность.
4. Принятие решения по обработке риска.
5. План обработки рисков.
6. Декларация о применимости механизмов контроля.

Тема «Многофакторная модель оценки информационных рисков хозяйствующего субъекта»

1. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков.
2. Этапы многофакторной оценки информационных рисков предприятия:

1 этап. Подготовительный этап.

2 этап. Оценка рисков информационной безопасности.

3 этап. Управление информационными рисками

4 этап. Создание комплексной системы защиты информационных активов (КСЗИА) хозяйствующего субъекта

5 этап. Реализация программы обеспечения информационной безопасности компании.

6 этап. Анализ эффективности вложений в информационную безопасность.

Тема «Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта».

1. Категории затрат на безопасность информационных активов.
2. Экономическое обоснование затрат на защищенность.
3. Определение эффекта от внедрения системы информационной защищенности.

Учебная литература представлена в Пункте 6.1 Рабочей программы дисциплины «Теория языков программирования и методы трансляции».

Критерии и шкала оценивания конспекта

Оценка	Критерий оценки
«отлично»	Конспект полный. В конспектируемом материале выделена главная и второстепенная информация. Установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий, приведены примеры, схемы.
«хорошо»	Конспект полный. В конспектируемом материале выделена главная и второстепенная информация. Установлена не в полном объеме логическая связь между элементами конспектируемого материала. Даны определения основных понятий. Примеры приведены частично.
«удовлетворительно»	Конспект не полный. В конспектируемом материале не выделена главная и второстепенная информация. Не установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий. Примеры отсутствуют
«неудовлетворительно»	Конспект не удовлетворяет ни одному из критериев, приведенных выше

Собеседование

Собеседование с обучающимися проходит на семинарских занятиях. В момент проведения собеседования пользоваться учебниками, справочниками, конспектами лекций запрещено.

Преподаватель заранее оглашает учащимся перечень вопросов, ответы на которые необходимо подготовить учащимся самостоятельно.

Задачи проведения собеседования с обучающимися:

- проверка и контроль полученных знаний по изученной теме;
- расширение проблематики в рамках дополнительных вопросов по изученной теме;
- углубление знаний;
- формирование навыков беседы, декларирования знаний и рассуждения.

Типовые контрольные задания

Тема «Понятие риск. Информационные риски киберпространства».

1. Какой подход к оценке рисков используется в вашей организации?
2. Какие категории информационных рисков охватывает используемый вами подход?
3. Какие сотрудники вашей организации участвуют в процессах управления рисками и как распределяются между ними роли?Кто и на основании какой информации принимает решения по обработке рисков?
4. К какой категории специалистов, с точки зрения отношения к оценке
5. рисков, вы сами относитесь?
6. Какие информационные риски представляют наибольшую опасность для вашей организации?

Тема «Основные элементы управления рисками информационной безопасности».

1. Какие процессы включает в себя система управления рисками и как эти процессы связаны с другими процессами системы управления (СУИР) ИБ?

2. Какие виды активов важнее для бизнеса вашей организации и почему?
3. Какие информационные риски вы рассматриваете в качестве основных?
4. В каких случаях область действия СУИР может охватывать не всю организацию?
5. Каковы отличительные признаки системного подхода к управлению рисками?
6. Какие виды нормативных и рабочих документов требуются для управления рисками в организации?
7. Каким образом могут распределяться обязанности и ответственность за управление рисками в организации?*Тема «Система управления информационными рисками».*
1. Какие факторы влияют на решение о принятии риска?
2. На основании каких данных определяется вероятность угрозы?
3. Назовите основные источники уязвимостей.
4. Перечислите основные и вспомогательные бизнес-процессы ФГБОУ ВО ИрГУПС.
5. Какие этапы включает в себя оценка риска?
6. Какие параметры могут использоваться для описания бизнес-процессов организации?
7. Какие категории требований безопасности необходимо учитывать при оценке рисков?
8. Как можно определить ценность тех или иных активов?
9. Как связаны между собой оценка рисков и планирование непрерывности бизнеса?

Тема «Методические подходы к оценке информационных рисков хозяйствующих субъектов».

1. Раскройте сущность комплексной системы защиты информационных активов предприятий.
2. Опишите особенности система защиты информационных активов хозяйствующего субъекта.
3. Исследуйте особенности организационного направления в деятельности по защите информационных активов предприятия.
4. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.
5. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?
6. Суть методики оценки возможного ущерба при реализации угроз безопасности?
7. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.
8. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.
9. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.

Тема «Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта».

1. Изложите суть экспертных методов по определению ценности защищаемых информационных активов.
2. Изложите суть методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.
3. Изложите суть эффективности оценки информационных рисков.

Критерии и шкала оценивания собеседования

Оценка	Критерий оценки
«отлично»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, приведены примеры.
«хорошо»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Частично даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, не приведены примеры.
«удовлетворительно»	Полные ответы на предложенные вопросы не даны (приведены только определения основных терминов).
«неудовлетворительно»	Учащийся не смог ответить на поставленные вопрос и дополнительные вопросы по заданной теме.

Сообщение, доклад и презентация

Темы сообщений/докладов предоставляются обучающимся вначале семестра для того, чтобы у них была возможность выбора наиболее интересной, понравившейся темы.

Доклады должны сопровождаться презентацией и длиться не более 30 минут.

Типовые контрольные задания

Тема «Обзор методов и инструментальных средств управления рисками».

1. Нужен ли для управления рисками специальный программный инструментарий? Выбор инструментария для оценки рисков.
2. Общие недостатки и ограничения коммерческих программных продуктов.
3. OCTAVE.
4. CRAMM.
5. RiskWatch.
6. COBRA.
7. RA2 the art of risk.
8. vsRisk.
9. Callio Secura 17799.
10. Proteus Enterprise.

Критерии и шкала оценивания сообщения, доклада и презентации

Оценка	Критерий оценки
«отлично»	Учащийся в докладе полностью раскрыл тему, ответил на все дополнительные вопросы, использовал демонстративный материал, который отлично оформлен, и прекрасно в нем ориентировался.
«хорошо»	Учащийся в докладе полностью раскрыл тему, использовал демонстративный материал, который хорошо оформлен, но есть незначительные неточности, и хорошо в нем ориентировался.
«удовлетворительно»	Учащийся не полностью раскрыл тему, демонстративный материал либо не использовался, либо учащийся в нем не достаточно хорошо ориентировался.
«неудовлетворительно»	Учащийся не подготовил доклад.

Разноуровневые задачи и задания

Выполнение разноуровневых заданий, предусмотренных рабочей программой дисциплины, проводятся во время практических занятий.

Типовые контрольные задания

Тема «Идентификация активов предприятия»

Важные активы внутри области действия системы управления информационной безопасности (СУИБ) должны быть четко идентифицированы и должным образом оценены, а реестры, описывающие различные виды активов, должны быть взаимоувязаны и поддерживаться в актуальном состоянии. Для того чтобы быть уверенным в том, что ни один из активов не был пропущен или забыт, должна быть определена область действия СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий.

Идентификация активов включает:

- формирование модели бизнес-процессов;
- инвентаризация активов;
- формирование реестров активов;
- определение взаимосвязей между реестрами активов;
- построение модели активов;

- определение владельцев активов и их обязанностей;
- делегирование обязанностей по обеспечению безопасности активов;
- классификация и категорирование активов;
- определение правил допустимого использования активов.

Важно идентифицировать не только информационные активы, но другие активы, с которыми они связаны. Взаимосвязи между активами описываются моделью активов. Активы надо структурировать, категорировать и классифицировать по уровню конфиденциальности, критичности и другим признакам. Группирование похожих или связанных активов позволяет упростить процесс оценки рисков.

Нельзя обеспечить адекватный уровень информационной безопасности без установления подотчетности за активы.

Задание 1. Провести идентификацию активов предприятия/организации *(порядковый номер варианта выбрать в соответствии с номером учащегося в списке группы, либо выбрать организацию самостоятельно):*

1. Банк.
2. Супермаркет/магазин.
3. Научно-исследовательский институт.
4. Медицинское учреждение.
5. Торговая фирма.
6. Налоговая инспекция.
7. Агентство недвижимости.
8. Учебное заведение.
9. IT-компания.
10. Центр занятости населения.

Допускается осуществить идентификацию активов не всей организации (если она слишком велика), а один или несколько взаимодействующих между собой отделов/подразделений.

Задание 2. Осуществите расчет совокупной стоимости владения (TCO).

Тема «Анализ угроз и уязвимостей»

Задание 1. Построить модель угроз информационной безопасности (ИБ) предприятия / организации / подразделения.

Задание 2. Описать уязвимости информационной безопасности.

Задание 3. Построить модель нарушителя ИБ.

Задание 4. Опишите профиль и жизненный цикл для одной из следующих угроз:

1. Заражение компьютерным вирусом.
2. Атака на отказ в обслуживании.
3. Несанкционированный доступ к системе и хищение конфиденциальной информации.
4. Выход из строя файлового сервера.
5. Пожар в офисе.

Постарайтесь дать как широкое определение угрозе, включающее в себя большое количество различных сценариев инцидентов, так и более узкое определение, включающее в себя лишь один конкретный сценарий реализации угрозы.

Задание 5. Оцените вероятности угроз.

Тема «Определение величины риска»

Задание 1. Постройте матрицу величины риска.

Задание 2. Откалибруйте шкалу оценки рисков.

Задание 3. Осуществите расчет риска информационной безопасности на основе модели угроз и уязвимостей.

Тема «Обработка рисков информационной безопасности»

Задание 1. Рассчитайте затраты на контрмеры (прямые и косвенные).

Задание 2. Осуществите расчет возврата инвестиций (ROI).

Задание 3. Подготовьте отчет об оценке рисков.

Отчет об оценке рисков необходим для руководства и всех заинтересованных сторон, вовлеченных в процесс управления рисками. Другими словами, этот документ нужен для коммуникации рисков.

Краткая структура отчета об оценке рисков:

1. Введение

2. Основания, общие сведения
3. Цели и задачи
4. Методология и результаты
5. Идентификация активов и требований
6. Оценка активов и последствий
7. Анализ угроз и уязвимостей
8. Вычисление и оценивание рисков
9. Резюме рисков для руководства
10. Описание самых высоких рисков и причин их существования
11. Приложения
12. Реестры активов, требований и рисков
13. Таблицы определения ценности активов и ущерба для бизнеса

Критерии и шкала оценивания разноуровневых задач и заданий

Оценка	Критерий оценки
«отлично»	Обучающийся полностью и правильно выполнил задания. Показал отличные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Отчет оформлен аккуратно и в соответствии с предъявляемыми требованиями. Ответил на все дополнительные вопросы на защите
«хорошо»	Обучающийся выполнил задания с небольшими неточностями. Показал хорошие знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Есть недостатки в оформлении отчета. Ответил на большинство дополнительных вопросов на защите
«удовлетворительно»	Обучающийся выполнил задания с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Качество оформления отчета имеет недостаточный уровень. При ответах на дополнительные вопросы на защите было допущено много неточностей
«неудовлетворительно»	При выполнении заданий обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала. Обучающийся неспособен пояснить полученные результаты. При ответах на дополнительные вопросы на защите было допущено множество неточностей

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии определения сформированности компетенций на различных этапах их формирования даны в пункте 1.2. Шкалы и критерии оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета, а также шкала для оценивания уровня освоения компетенций представлена в нижеследующей таблице.

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.	Высокий

	Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

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

Экзамен проходит в устной и/или письменной формах по предложенным ниже вопросам. В программу зачета включен материал по изученным разделам дисциплины «Методология анализа информационных рисков».

Перечень вопросов к экзамену

1. Что такое информация ограниченного доступа?
2. В каких аспектах экономической деятельности, может выступать конфиденциальная информация?
3. Дайте характеристику понятия «информационные активы организации».
4. Какова взаимосвязь понятий «информационных активов» и «системы оценки рисков информационной безопасности хозяйствующего субъекта»?
5. Определите место и роль системы защиты информационных активов в системе управления деятельностью предприятия.
6. В чем заключается суть тревожных симптомов в сфере обеспечения безопасности информационных активов?
7. В чем заключается суть тенденции увеличения количества внутренних угроз, исходящих от сотрудников организаций (инсайдеров)?
8. Рассмотрите сущность основных видов организационных каналов несанкционированного доступа к информационным активам.
9. В чем заключается суть аналитической работы по обнаружению организационных каналов несанкционированного доступа к информационным активам?

10. Раскройте сущность комплексной системы защиты информационных активов предприятий.
11. Раскройте особенности система защиты информационных активов хозяйствующего субъекта.
12. Опишите особенности организационного направления в деятельности по защите информационных активов предприятия.
13. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.
14. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?
15. Опишите методику оценки возможного ущерба при реализации угроз безопасности.
16. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.
17. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.
18. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.
19. Какие показатели включены в основу методики оценки информационных рисков предприятия?
20. Охарактеризуйте сущность методики и состав показателей типичной многофакторной модели оценки информационных рисков предприятия.
21. Охарактеризуйте сущность частной методики оценки надежности персонала в рамках общей методики многофакторной модели оценки информационных рисков предприятия.
22. Охарактеризуйте сущность частной методики оценки надежности технических и программно-аппаратных средств обработки информации.
23. Охарактеризуйте сущность частной методики организационно-режимных мер защиты с использованием программных комплексов анализа и управления рисками информационной системы «ГРИФ» и «КОНДОР».
24. Охарактеризуйте сущность экспертных методов по определению ценности защищаемых информационных активов.
25. Охарактеризуйте сущность методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.
26. Охарактеризуйте сущность эффективности оценки информационных рисков.

Критерии и шкала оценивания экзамена

Оценка	Критерий оценки
«отлично»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого экзаменационного вопроса.
«хорошо»	Дан неполный ответ на теоретический вопрос. Даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого экзаменационного вопроса (возможно допущение незначительных неточностей в ответах на дополнительные вопросы).
«удовлетворительно»	Не даны полные ответы на предложенные вопросы (приведены только определения основных терминов).
«неудовлетворительно»	Если ответ на теоретический вопрос не дан, или ответы не удовлетворяют ни одному из критериев, приведенных выше. Учащийся не смог ответить на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса.

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

Задание для текущего контроля и проведения промежуточной аттестации должны быть направлены на оценивание:

– уровня освоения теоретических понятий, научных основ профессиональной деятельности;

– степени готовности обучающегося применять теоретические знания и профессионально значимую информацию, сформированности когнитивных умений;

– приобретенных умений, профессионально значимых для профессиональной деятельности.

Задания для оценивания когнитивных умений (знаний) должны предусматривать необходимость проведения аттестуемым интеллектуальных действий:

– по дифференциации информации на взаимозависимые части, выявлению взаимосвязей между ними и т.п.;

– по интерпретации и творческому усвоению информации из разных источников, ее системного структурирования;

– по выявлению значения предмета учебной дисциплины для достижения конкретной цели, на основе проникновения в суть общественных явлений и процессов;

– по комплексному использованию интеллектуальных инструментов дисциплины для решения учебных и практических проблем.

При составлении заданий необходимо иметь в виду, что они должны носить практико-ориентированный комплексный характер, быть направлены на формирование и закрепление общекультурных и профессиональных компетенций.

Промежуточная аттестация в форме экзамена проводится путем устного собеседования и/или письменного решения задания по билетам. Билеты составлены таким образом, что в каждый попали вопросы, контролирующие уровень сформированности всех компетенций, закрепленных за дисциплиной.

Билет содержит три вопроса для оценивания результатов обучения в виде знаний, умений и навыков.

Образец экзаменационного билета

ИРГУПС **20__ – 20__** **уч. год**	**Экзаменационный билет №** 1 по дисциплине «Методология анализа информационных рисков» __ семестр	Утверждаю: Заведующий кафедрой **«ИСиЗИ» ИрГУПС** _____
1. Что входит в понятие «информационные активы организации». **2.** Раскройте сущность комплексной системы защиты информационных активов предприятий. **3.** Какие показатели включены в основу методики оценки информационных рисков предприятия? Каким образом они оцениваются?		

Перечень вопросов и заданий разного уровня сложности обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Распределение вопросов по экзаменационным билетам находится в закрытом для обучающихся доступе. На экзамене обучающийся вытаскивает билет случайным образом. Для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 50 минут. После ответа на вопросы билета, преподаватель, как правило, задает обучающемуся дополнительные вопросы.