Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков
« 04 » сентября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Прогнозирование рисков информационной безопасности
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: магистратура
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 216 (6)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности.
Задачи дисциплины:
- изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности;
- изучение предпосылок для управления информационными рисками;
- изучение основных требований по управлению рисками информационной безопасности;
- изучение состава системы управления информационными рисками;
- формирование умений оценки рисков информационной безопасности;
- формирование умений обработки рисков информационной безопасности;
- формирование навыков по оценке угроз безопасности информации в технологии оценки рисков;
- формирование навыков подбора инструментальных средств для управления рисками информационной безопасности.

1.2. Изучаемые объекты дисциплины

- современные информационные риски и их особенности;
- стандарты управления рисками;
- стандарты в области управления рисками информационной безопасности;
- система управления информационными рисками;
- порядок оценки рисков информационной безопасности;
- анализ угроз и уязвимостей;
- профиль и жизненный цикл угрозы;
- описание угроз безопасности;
- способы классификации угроз;
- уязвимости информационной безопасности;
- идентификация организационных и технических уязвимостей;
- оценка угроз и уязвимостей;
- определение величины риска;
- процесс и способы обработки рисков;
- инструментальные средства для управления рисками.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.1	ИД-1ПК-1.1	Знает основные риски безопасности информации в автоматизированных системах	Знает способы реализации угроз безопасности в автоматизированных системах	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.1	ИД-2ПК-1.1	Умеет анализировать возможные риски, связанные с обработкой информации в информационных системах	Умеет анализировать возможные уязвимости информационных систем	Защита лабораторной работы
ПК-1.1	ИД-3ПК-1.1	Владеет навыками систематизации оценки и обработки рисков информационной безопасности	Владеет навыками систематизации результатов проведенных исследований	Защита лабораторной работы
ПКО-2	ИД-1ПКО-2	Знает подходы к построению и исследованию моделей оценки и обработки рисков информационной безопасности в автоматизированных системах	Знает подходы к построению и исследованию моделей процессов защиты информации в автоматизи-рованных системах	Защита лабораторной работы
ПКО-2	ИД-2ПКО-2	Умеет разрабатывать модели оценки рисков и доказывать адекватность данных моделей для использования в системе защиты информации	Умеет разрабатывать и доказывать адекватность моделей систем защиты информации	Защита лабораторной работы
ПКО-2	ИД-3ПКО-2	Владеет навыками применения программного обеспечения для оценки обработки рисков в задачах моделирования и исследования моделей систем защиты информации	Владеет навыками применения программного обеспечения в задачах моделирования и исследования моделей систем защиты информации	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)	32	32
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)		
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	126	126
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	216	216

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
3-й семестр				
Введение в дисциплину	2	0	0	14
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Особенности формирования терминологии науч-ной дисциплины. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература.				
Предпосылки для управления информационными рисками	2	4	0	14
Современные информационные риски и их особенности. Кибертерроризм. Риски промышленных систем. Риски утечки информации. Риски электронных расчетов. Стандарты управ-ления рисками. Государственное регулирование. Оценка рисков как основа корпоративного управления.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Основные требования по управлению рисками информационной безопасности	2	4	0	14
Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Информационная составляющая бизнес - рисков. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Уровни зрелости бизнеса в от-ношении рисков. Анализ факторов риска. Методика оценки рисков приватности, включая персональные данные				
Система управления информационными рисками	2	4	0	14
Преимущества системного подхода к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками. Процессная модель управления рисками. Непрерывная деятельность по управлению рисками. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства. Пересмотр и переоценка риска. Взаимосвязь процессов аудита и управления рисками. Управление документами и записями. Корректирующие и превентив-ные меры. Коммуникация рисков. Аутсорсинг процессов управления рисками. Распределе-ние ответственности за управление рисками. Требования к риск-менеджеру. Требования к эксперту по оценке рисков.				
Оценка рисков информационной безопасности	2	4	0	14
Идентификация активов. Описание бизнес-процессов. Идентификация требований безопасности. Реестр требований безопасности. Требования законодательства и нормативной базы. Контрактные обязательства. Требования бизнеса. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов. Особенности интервьюирования бизнес-пользователей. Определение приоритетов аварийного восстановления.				
Оценка угроз безопасности информации в технологии оценки рисков	2	4	0	14
Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы. Описание угроз безопасности. Способы классификации угроз. Уязвимости информационной безопасности. Идентификация организационных уязвимостей. Идентификация технических уязвимостей. Оценка				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки рис-ка. Пример оценки риска. Отчет об оценке рисков.				
Обработка рисков информационной безопасности	2	4	0	14
Процесс обработки рисков. Способы обработки риска. Принятие риска. Уменьшение риска. Передача риска. Избегание риска. Оценка возврата инвестиций в информационную безопасность. Принятие решения по обработке риска. План обработки рисков. Декларация о применимости механизмов контроля. Профили рисков информационной безопасности.				
Инструментальные средства для управления рисками	2	4	0	14
Актуальность программного сопровождения процедуры оценки рисков. Выбор программного обеспечения для оценки рисков. Общие недостатки и ограничения коммерческих про-граммных продуктов. Обзор методов и инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.				
Внедрение системы прогнозирования и управления рисками информационной безопасности	2	4	0	14
Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками. Обучение членов экспертной группы. Проведение полной оценки рисков по всем активам. Жизненный цикл управления рисками.				
ИТОГО по 3-му семестру	18	32	0	126
ИТОГО по дисциплине	18	32	0	126

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Анализ требований и стандартов в области управления рисками информационной безопасности.
2	Исследование современных информационных рисков и их особенностей.
3	Исследование рисков различных информационных систем.
4	Количественное и качественное определение величины риска.
5	Разработка системы управления информационными рисками.
6	Оценка угроз безопасности информации в технологии оценки рисков.

№ п.п.	Наименование темы лабораторной работы
7	Применение технологий обработки рисков информационной безопасности.
8	Методы и инструментальные средства управления рисками.

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Егоров А. Ф. Анализ риска, оценка последствий аварий и управление безопасностью химических, нефтеперерабатывающих и нефтехимических производств : учебное пособие для вузов / А. Ф. Егоров, Т. В. Савицкая. - Москва: КолосС, 2010.	8

2	Милославская Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.	15
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2	Шапкин А. С. Теория риска и моделирование рисковых ситуаций : учебник для вузов / А. С. Шапкин, В. А. Шапкин. - М.: Дашков и К, 2007.	10
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	В. А. Горев Надежность технических систем и техногенный риск : Учебно-методическое пособие к практическим работам для обучающихся по направлению подготовки / В. А. Горев. - Москва: МИСИ-МГСУ, Ай Пи Эр Медиа, ЭБС АСВ, 2018	http://elib.pstu.ru/Record/iprbooks88475	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Персонльный компьютер	10
Лекция	Мультимедийный проектор	1

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Прогнозирование рисков информационной безопасности»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) образовательной программы: Комплексные системы информационной безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2 **Семестр**: 3

Трудоёмкость:
Кредитов по рабочему учебному плану: 6 ЗЕ
Часов по рабочему учебному плану: 216 ч.

Форма промежуточной аттестации:
Экзамен: 3 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (3-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает основные риски безопасности информации в автоматизированных системах; подходы к построению и исследованию моделей оценки и обработки рисков информационной безопасности в автоматизированных системах		ТО1 ТО2 ТО3		Т1 Т2 Т3		ТВ
Освоенные умения						
У.1 Умеет анализировать возможные риски, связанные с обработкой информации в информационных системах; разрабатывать модели оценки рисков и доказывать адекватность данных моделей для использования в системе защиты информации			ОЛР1 ОЛР2 ОЛР3 ОЛР4 ОЛР5 ОЛР6 ОЛР7 ОЛР8			ПЗ
В.1 Владеет навыками систематизации оценки и обработки рисков информационной безопасности; применения программного обеспечения для оценки обработки рисков в задачах моделирования и исследования моделей систем защиты информации				КР		КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1.1: Оценка рисков как основа корпоративного управления.

Тема 2.1: Методика оценки рисков приватности, включая персональные данные.

Тема 2.2: Требования к риск-менеджеру и к эксперту по оценке рисков.

Тема 3.1: Определение приоритетов аварийного восстановления.
Тема 3.2: Идентификация технических уязвимостей.
Тема 3.3: Декларация о применимости механизмов контроля.
Тема 3.4: Общие недостатки и ограничения коммерческих программных продуктов оценки рисков.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 8 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.2.1. Защита отчетов по индивидуальным заданиям

Всего запланировано 3 индивидуальных задания по тематике модулей учебной дисциплины, выполняемых по вариантам. Они представляют собой практическое задание по формированию навыков подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности. Темы индивидуальных заданий:

Модуль 1

1. Термины и определения в области управления информационными рисками
2. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 7799-3:2006 и ISO/IEC 27005:2008.
3. Антология кибератак.
4. Наихудшие сценарии кибератак.
5. Определение степени критичности систем по методу CRAMM.
6. Типовые угрозы информационной безопасности.
7. Типовые уязвимости информационной безопасности.
8. Законодательные и нормативные акты Российской Федерации в области защиты информации.
9. Типовые документы для управления рисками информационной безопасности.

Модуль 2

1. Определение величины риска.
2. Калибровка шкалы оценки риска.
3. Пример оценки риска.
4. Отчет об оценке рисков.
5. Калибровка шкалы оценки риска.

Модуль 3

1. Начальные условия для внедрения СУИР.
2. Организационная структура управления рисками.
3. Обучение членов экспертной группы.
4. Реализация пилотного проекта по оценке рисков.
5. Проведение полной оценки рисков по всем активам.
6. Жизненный цикл управления рисками.

Защита отчета по индивидуальному заданию проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Современные информационные риски и их особенности. Кибертерроризм.
2. Риски промышленных систем. Риски утечки информации. Риски электронных расчетов.
3. Стандарты управления рисками.
4. Государственное регулирование деятельности по оценке рисков.
5. Оценка рисков как основа корпоративного управления.
6. Стандарты в области управления рисками информационной безопасности.
7. Количественное определение величины риска.
8. Качественное определение величины риска.
9. Информационная составляющая бизнес - рисков.
10. Активы организации как ключевые факторы риска.
11. Подходы к управлению рисками.
12. Уровни зрелости бизнеса в отношении рисков.
13. Анализ факторов риска.
14. Методика оценки рисков приватности, включая персональные данные.
15. Преимущества системного подхода к управлению рисками.

16. Структура документации по управлению рисками.
17. Политика и контекст управления рисками.
18. Структура системы управления рисками.
19. Процессная модель управления рисками.
20. Непрерывная деятельность по управлению рисками.
21. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства.
22. Пересмотр и переоценка риска.
23. Взаимосвязь процессов аудита и управления рисками.
24. Управление документами и записями.
25. Корректирующие и превентивные меры.
26. Коммуникация рисков.
27. Аутсорсинг процессов управления рисками.
28. Распределение ответственности за управление рисками.
29. Требования к риск-менеджеру по оценке рисков.
30. Требования к эксперту по оценке рисков.
31. Идентификация требований безопасности. Реестр требований безопасности.
32. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов.
33. Особенности интервьюирования бизнес-пользователей.
34. Определение приоритетов аварийного восстановления.
35. Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы.
36. Уязвимости информационной безопасности.
37. Идентификация организационных уязвимостей.
38. Идентификация технических уязвимостей.
39. Оценка угроз и уязвимостей.
40. Определение величины риска.
41. Калибровка шкалы оценки риска.
42. Отчет об оценке рисков.
43. Процесс обработки рисков. Способы обработки риска.
44. План обработки рисков.
45. Декларация о применимости механизмов контроля.
46. Профили рисков информационной безопасности.
47. Актуальность программного сопровождения процедуры оценки рисков.
48. Обзор методов и инструментальных средств управления рисками.
49. Организационная структура управления рисками. Обучение членов экспертной группы.
50. Жизненный цикл управления рисками.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Современные информационные риски и их особенности.
2. Стандарты в области управления рисками информационной безопасности.
3. Система управления информационными рисками.
4. Оценка рисков информационной безопасности.

5. Инструментальные средства для управления рисками.

6.

7. Разработать алгоритм Процесса управления рисками информационной безопасностью на основании реализации модели PDCA.

8. Провести обработку рисков информационной безопасности на основании анализа и оценки рисков информационной безопасности и в соответствии с выбранной областью действия СУИБ и активами.

9. Сформировать требования по организации процесса мониторинга, коммуникации и пересмотра рисков ИБ.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.