МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Управление информационной безопасностью
Рабочая программа дисциплины

Составитель:
к.т.н, доцент, доцент, Н.В. Гришина

Ответственный редактор
к.и.н., доцент, заведующая кафедрой, Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 10 от 30.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: формирование знаний о процессах управления всеми средствами защиты информации и мониторинге безопасности информационной системы.

Задачи дисциплины:

-освоение знаний об архитектуре управления информационной безопасностью (ИБ) корпоративной информационной системы (КИС), функциональных системах управления и мониторинге безопасности КИС;

-приобретение практических навыков по использованию соответствующих нормативно-правовых документов и программных инструментариев для управления ИБ.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 – Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 -Знает методы управления проектами; этапы жизненного цикла проекта УК-2.2 -Умеет разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ УК-2.3 Владеет навыками разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах	Знать: теоретические основы процессного подхода в организации, содержание общенаучных и конкретных методов управления бизнес-процессами; методы контроллинга и мониторинга бизнес-процессов. Уметь: моделировать, анализировать и совершенствовать бизнес-процессы в сфере информационной безопасности с использованием изученных стандартов, технологий и нотаций моделирования. Владеть: практическими навыками моделирования, анализа и документирования бизнес-процессов с помощью инструментальных сред
УК-4 Знает современные коммуникативные технологии на государственном и	УК-4.1 Знает современные коммуникативные технологии на государственном и	Знать: как формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и

иностранном языках; закономерности деловой устной и письменной коммуникации	иностранном языках; закономерности деловой устной и письменной коммуникации УК-4.2 Умеет применять на практике коммуникативные технологии, методы и способы делового общения УК-4.3 Владеет методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств	экономической целесообразности; как организовать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации; как определить виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия ; Уметь: принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия; собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; применять комплексный подход к обеспечению информационной безопасности Владеть: навыками работы с нормативными правовыми актами; навыками организации работы малого коллектива исполнителей с учетом требований защиты информации.
ОПК- 3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов ОПК-3.2 Уметь разрабатывать	Знать: как формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и экономической целесообразности Уметь: собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности Владеть: навыками организации работы малого коллектива исполнителей с учетом требований защиты информации

	технические задания на создание подсистем обеспечения информационной безопасности ОПК-3.3 Владеть навыками разработки политик безопасности различных уровней	

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к обязательной части учебного плана.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Управление информационной безопасностью в интернет-проектах».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 з. е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	28
2	Практические работы	36
	Всего:	64

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _62__ академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Предмет, задачи и содержание курса	Основные понятия и термины дисциплины. Базовые аспекты управления информационной безопасностью. Основные задачи системы управления средствами информационной безопасности предприятия.
2.	Определение условий функционирования системы защиты информации	Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.

3.	Разработка модели системы защиты информации	Понятие модели объекта, основные виды моделей и их характеристика. Модель как инструмент количественного и качественного анализа СЗИ. Значение моделирования процессов СЗИ. Выбор структуры СЗИ, ее зависимость от объектов защиты, характера и условий функционирования предприятия. Функциональная модель СЗИ. Организационная модель СЗИ. Информационная модель СЗИ.
4.	Технологическое и организационное построение системы защиты информации	Общее содержание работ по организации СЗИ. Характеристика основных стадий создания СЗИ. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.
5.	Кадровое обеспечение функционирования системы защиты информации	Определение состава кадрового обеспечения функционирования СЗИ. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.
6.	Материально-техническое и нормативно-методическое обеспечение системы защиты информации	Значение материально-технического обеспечения функционирования СЗИ. Определение состава материально-технического обеспечения, его зависимость от структуры СЗИ. Значение нормативно-методического обеспечения функционирования СЗИ. Перечень вопросов, требующих документационного закрепления. Состав нормативно-методических документов по обеспечению функционирования СЗИ, их назначение, структура и содержание. Порядок разработки и внедрения документов.
7.	Назначение, структура и содержание управления системой защиты информации	Понятие и цели управления СЗИ. Сущность процессов управления СЗИ. Принципы управления СЗИ. Основные стили управления. Структура и содержание общей технологии управления СЗИ.
8.	Принципы и методы планирования функционирования системы защиты информации	Понятие и задачи планирования функционирования СЗИ. Способы и стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов организации и функционирования СЗИ. Методы сбора, обработки и изучения информации, необходимой для планирования. Организация выполнения планов.
9.	Сущность и содержания контроля функционирования комплексной системой защиты	Понятие и виды контроля функционирования СЗИ. Цель проведения контрольных мероприятий в СЗИ. Методы

	информации	контроля. Особенности проведения контроля функционирования СЗИ. Анализ и использование результатов проведения контрольных мероприятий.
10.	Управление системой защиты информации в условиях чрезвычайных ситуаций	Понятие и основные виды чрезвычайных ситуаций. Технология принятия решений в условиях чрезвычайной ситуации. Факторы, влияющие на принятие решений в условиях чрезвычайной ситуации. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.

4. Образовательные технологии

№ п/п	Наименование темы	Виды учебной работы	Образовательные технологии
1	Предмет, задачи и содержание курса	Лекция 1 Практическое занятие 1,2,3	Лекция
2	Определение условий функционирования системы защиты информации		Лекция-дискуссия Практическое занятие
3	Разработка модели системы защиты информации	Лекция 2 Практическое занятие 4	Практическое занятие
4	Технологическое и организационное построение системы защиты информации	Лекция 3,4 Практическое занятие 4	Лекция-дискуссия Практическое занятие
5	Кадровое обеспечение функционирования системы защиты информации	Лекция 5 Практическое занятие 5	Лекция-дискуссия Практическое занятие
6	Материально-техническое и нормативно-методическое обеспечение системы защиты информации	Лекции 6	Лекция-дискуссия
7	Назначение, структура и содержание управления системой защиты информации	Лекция 7 Практическое занятие 6	Лекция-дискуссия Практическое занятие
8	Принципы и методы планирования функционирования системы защиты информации	Лекция 8 Практическое занятие 7	Лекция Практическое занятие
9	Сущность и содержание контроля функционирования комплексной системы защиты информации	Лекция 9 Практическое занятие 7	Лекция-дискуссия Практическое занятие

№ п/п	Наименование темы	Виды учебной работы	Образовательные технологии
10	Управление системой защиты информации в условиях чрезвычайных ситуаций	Лекция 10 Практическое занятие 8	Лекция Практическое занятие

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - участие в дискуссии по темам 1,3; - тестирование по темам 5, 6; - самостоятельной работы на семинаре по темам 2, 4- 8;	 5 балл 9 баллов 7 баллов	 10 баллов 18 баллов 42 балла
Промежуточная аттестация *(экзамен по билетам)*		*40 баллов*
Итого за семестр *экзамен*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	**Традиционная шкала**		**Шкала ECTS**
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценок

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A, B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные вопросы тестирования

(проверка сформированности компетенций УК-2)

1. Какой ГОСТ содержит свод норм и правил менеджмента информационной безопасности?
2. Кто в соответствии с ГОСТ Р ИСО/МЭК 27002— 2021 должен устанавливать политику информационной безопасности?
3. В соответствии с ГОСТ Р ИСО/МЭК 27002— 2021 ……. содержит цели информационной безопасности или обеспечивает основу для их установления.
4. В соответствии с ГОСТ Р ИСО/МЭК 27002— 2021 организация должна определить и обеспечить наличие ……., необходимых для создания, внедрения, поддержки и постоянного улучшения системы менеджмента информационной безопасности.
5. Что значит снизить риск?
6. В соответствии с ГОСТ Р ИСО/МЭК 27005-2010 менеджмент риска ИБ должен быть…
7. Часть системы с однозначно определёнными свойствами, выполняющие определённые функции и не подлежащие дальнейшему разбиению в рамках решаемой задачи (с точки зрения исследователя).
8. Элементы, осуществляющие непосредственное взаимодействие между элементами (или подсистемами) системы, а также с элементами и подсистемами окружения, это?
9. Связи, предназначенные для заданной функциональной передачи вещества, энергии, информации или их комбинаций — от одного элемента к другому в направлении основного процесса – это?
10. Связи, выполняющие осведомляющие функции, отражая изменение состояния системы в результате управляющего воздействия на нее, это?

Примерные вопросы тестирования

(проверка сформированности компетенций УК-4)

1. Дайте определение психологической теории принятия решения решений
2. Как называется деятельность, направленная на координирование действий персонала организации?
3. Свойство систем, обусловливающее появление новых свойств и качеств, не присущих элементам, входящих в состав системы.
4. Какое свойство системы означает, что каждый элемент системы вносит вклад в реализацию целевой функции системы.
5. Упорядоченность системы, определенный набор и расположение элементов со связями между ними.
6. Что такое способность системы противостоять внешним возмущающим воздействиям?

7. Разделение систем на части, с последующим самостоятельным рассмотрением отдельных частей.
8. Возможность осуществлять заданные мероприятия в правовом поле, т. е. при строгом соблюдении законодательных актов РФ, международных обязательств, уставных и других документов самой компании.
9. По ширине охвата управленческие решения можно разделить на …
10. Дайте определение метода экспертных оценок.
11. Расставить по возрастанию сложности ситуации, в которых принимаются решения

Стандартные
Слабо структурированные
Неструктурированные

12. Расставьте по порядку элементы реализации комплексного (системного) подхода к построению любой системы

изучение объекта внедряемой системы
оценку экономической целесообразности
соотношение всех внутренних и внешних факторов

Примерные вопросы тестирования

(проверка сформированности компетенций ОПК-3)

1. Расставьте процессы цикла управления **по порядку**

Планирование
Прогнозирование
Моделирование

2. Расставьте в порядке уменьшения зависимости от имеющихся ресурсов

Перспективное планирование.
Среднесрочное планирование.
Текущее

3. Первым шагом в цикле управления является…
4. Метод научно-обоснованного предвидения возможных направлений будущего развития организации, рассматриваемой в тесном взаимодействии с окружающей ее средой
5. Как называется метод планирования в зависимости от длительности планового периода сроком на 5 и более лет ?
6. Планирования в зависимости от длительности планового периода сроком от 1 года до 5 лет – это…
7. Планирования в зависимости от длительности планового периода сроком от 1 месяца до 1 года– это…
8. В какой момент необходимо оформить документ о неразглашении сведений конфиденциального характера с работником, допущенным к сведениям?

Промежуточная аттестация

Примерная тематика вопросов для экзамена

(проверка сформированности компетенций УК-2, УК-4, ОПК-3)

1. На конкретных примерах опишите взаимосвязь процессов планирования и контроля в комплексной системе защиты информации.
2. Разработайте пример реализации модели процесса контроля в конкретной

системе защиты информации.

3. Роль мотивации в развитии теории и практики управления.
4. Каково значение обратной связи в процессе информационного обмена в системе защиты информации.
5. Основные способы и стадии планирования КСЗИ.
6. Содержание основных задач планирования КСЗИ.
7. Особенности структуры и содержания планов организации и функционирования КСЗИ.
8. Факторы, влияющие на выбор принципов и способов планирования.
9. Организация сбора и обработки информации в процессе повседневной деятельности системы защиты информации.
10. Структура основных работ, подлежащих выполнению в процессе повседневной деятельности комплексной системы защиты информации.
11. Особенности оперативно-диспетчерского управления системы защиты информации.
12. Методы руководства выполнением плана деятельности системы защиты информации.
13. Сущность и виды контроля функционирования СЗИ.
14. Особенности контрольных процедур СЗИ.
15. Как понимается чрезвычайная ситуация с точки зрения организации и функционирования СЗИ?
16. Какие виды чрезвычайных ситуаций могут возникать при функционировании СЗИ?
17. Основные подходы к предупреждению, локализации и ликвидации последствий чрезвычайной ситуации.
18. Факторы, оказывающие влияние на принятие решений по ЗИ в условиях чрезвычайной ситуации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.
ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»

Литература

Основная:

Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю. - Москва :Гор. линия-Телеком, 2013. - 244 с. (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0271-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/560780 – Режим доступа: по подписке.

Белов, Е. Б. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - Москва : Гор. линия-Телеком, 2011. - 558 с.: ил.; . - (Специальность; Учебное пособие для высших учебных заведений). ISBN 5-93517-292-5, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/405159 – Режим доступа: по подписке.

Тихомирова, О. Г. Управление проектом: комплексный подход и системный анализ : монография / О.Г. Тихомирова. — Москва : ИНФРА-М, 2022. — 300 с. — (Научная мысль). — DOI 10.12737/673. - ISBN 978-5-16-006383-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1709593

Дополнительная

Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 – Режим доступа: по подписке.

Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 – Режим доступа: по подписке.

Гришина, Н. В. Основы управления информационной безопасностью : учебно-методическое пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 99 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-110048-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1859951

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Занятие 1. ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ (проверка сформированности компетенции УК-2)

Вопросы:

1. Структуризация объекта защиты и ее значение.
2. Влияние специфики деятельности предприятия на определение состава защищаемых объектов (элементов).
3. Методы выявления состава защищаемых элементов.
4. Персонал предприятия как объект защиты.

Занятие проводится путем заслушивания и обсуждения сообщений студентов по заранее подготовленным вопросам. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы.

Особое внимание в ходе обсуждения сообщений уделяется методике выявления состава носителей защищаемой информации. Подробно рассматриваются все виды объектов защиты, процедура выявления их состава на предприятии с учетом его специфики. Подчеркивается роль структуризации объекта при определении тех элементов, которые нуждаются в защите. Выявляются особенности решения задач защиты в отношении такого объекта как персонал предприятия.

В результате проведения занятия студенты должны знать;

- каким образом и с какой целью осуществляется структуризация объекта защиты;
- методы выявления защищаемых объектов (элементов);
- факторы, которые следует учитывать при выделении защищаемых элементов на предприятии;
- специфику объекта защиты персонала предприятия.

Занятие 2. АНАЛИЗ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ (проверка сформированности компетенции УК-2)

Вопросы:

1. Какими факторами определяется состав угроз защищаемой информации?
2. Какова процедура выявления каналов несанкционированного доступа к информации на предприятии?
3. Чем определяется состав нарушителей и как осуществляется их категорирование?
4. Каким образом может проводиться оценка степени уязвимости информации в результате действий нарушителей различных категорий?

Занятие проводится в форме непрерывного диалога между преподавателем и студентами, в ходе которого студенты отвечают на поставленные вопросы. В процессе занятия возможны выступления студентов с заранее приготовленными сообщениями,

раскрывающими в том или ином аспекте тематику занятия. Кроме того, студенты выполняют самостоятельно практическое задание. Практическое задание предусматривает выбор студентами критериев, по которым множество потенциальных угроз может быть классифицировано, и разработку классификационной структуры угроз безопасности гипотетического объекта защиты. Для выполнения задания студенты обеспечиваются необходимыми материалами.

В процессе проведения занятия особое внимание уделяется вопросам, связанным с выявлением источников дестабилизирующих воздействий и каналов несанкционированного доступа к информации на предприятии. Подробно обсуждаются предложенные при выполнении практического задания классификационные структуры угроз. В ходе рассмотрения вопросов, связанных с категорированием нарушителей и определением степени опасности их действий по отношению к процессам обеспечения функционирования КСЗИ, внимание студентов обращается на те аспекты, содержание и вес тех факторов, которые в данной предметной области подлежат учету.

В результате занятия студенты должны знать:

- факторы, определяющие состав угроз защищаемой информации;
- содержание процедуры выявления каналов несанкционированного доступа к информации на предприятии;
- методику анализа и оценки возможностей доступа нарушителей к защищаемой информации.

Задание студенту

Многообразие угроз информации, исходящих от различных категорий нарушителей, и степень их опасности вызывает вопрос о том, каково их соотношение в практике деятельности подразделений КСЗИ в рамках различных направлений защиты. Помимо этого возникает другой важный вопрос, касающийся средств (инструментов), позволяющих охарактеризовать состояние системы защиты на объекте и оценить степень опасности реализации тех или иных угроз различными категориями нарушителей.

Предлагается письменно:

- представить графическую схему, отражающую содержание основных этапов процедуры выявления угроз информации и основных категорий нарушителей;
- объяснить, каким образом действия нарушителей различных категорий оказывают влияние на обеспечение функционирования КСЗИ;
- заполнить табл. П1.1 следующего вида:

Таблица П1.1

Категории нарушителей	Дестабилизирующие воздействия				
	Объекты защиты (Q_i...Q_n)				
	I	II	...	VI	
	A	B		Z	

Угрозы (A, B, C, ..., Z)

A — вывод из строя основного оборудования;

B — перехват информации;

C — ...;

Z — физическое воздействие на информацию.

Объекты защиты (I, II, ..., X)

I — выделенные помещения;
II — средства обработки информации и связи;
III — ...;
X — системы обеспечения функционирования объекта.
Вербально-числовая оценка степени опасности дестабилизирующего воздействия
1 — незначительная;
2 — малая;
3 — средняя;
4 — высокая.
Категории нарушителей:
- специалисты функциональных подразделений;
- специалисты службы безопасности;
...
- вспомогательный (технический) персонал.

Занятие 3. ОПРЕДЕЛЕНИЕ СОСТАВА КОМПОНЕНТОВ И УСЛОВИЙ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (проверка сформированности компетенции УК-2)

Вопросы:
1. Какие компоненты входят в состав структуры СЗИ?
2. Какие критерии положены в основу классификации каждой группы средств, входящих в состав СЗИ?
3. Какие требования предъявляются к выбору методов и средств защиты при организации и функционировании СЗИ?
4. Как определяются условия функционирования СЗИ?
Занятие проводится в форме диалога между преподавателем и студентами, в ходе которого происходит обсуждение перечисленных вопросов. Диалог может прерываться краткими сообщениями студентов по отдельным аспектам общей темы занятия (тематика и содержание сообщения заранее согласовываются с преподавателем).
В процессе проведения занятия внимание студентов обращается на те положения, которые касаются факторов и обстоятельств, оказывающих влияние на качество защиты. Подчеркивается то обстоятельство, что защита должна быть обеспечена для всей совокупности выделенной информации во всех компонентах ее сбора, хранения, передачи и использования, а также в течение всего времени и при всех режимах функционирования систем ее обработки.
В результате проведения занятия студенты должны знать:
- определение, состав и структуру компонентов КСЗИ;
- факторы, оказывающие влияние на качество защиты;
- характеристику различных вариантов условий функционирования СЗИ;
- виды и характеристику систем защиты в зависимости от условий функционирования.

Занятие 4. РАЗРАБОТКА МОДЕЛИ, ТЕХНОЛОГИЧЕСКОЕ И ОРГАНИЗАЦИОННОЕ ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (проверка сформированности компетенции УК-4)

Вопросы:
1. В чем проявляется значение моделирования объектов и процессов защиты при построении СЗИ?
2. Какие компоненты входят в состав функциональной модели СЗИ?
3. Какие компоненты входят в состав организационной модели СЗИ?
4. Какие компоненты входят в состав информационной модели СЗИ?
5. Каково общее содержание схемы технологического и организационного построения СЗИ?

Занятие проводится в форме обсуждения подготовленных докладов по вопросам темы. Обсуждение докладов дополняется проведением дискуссии в форме ответов на поставленные вопросы, а также выполнением практического задания. В качестве практического задания студентам предлагается самостоятельно построить функциональную и организационную модели объекта, описание которого приведено в задании.

Задание выполняется следующим образом:

а) формируются группы из двух, трех человек с последующей постановкой задачи для каждой группы;

б) студенты самостоятельно выделяют элементы организационной структуры КСЗИ и определяют основные функции системы;

в) проводится анализ взаимосвязи функциональной и организационной структуры КСЗИ;

г) каждая группа самостоятельно строит организационную и функциональную модель объекта, описание которого дано в задании;

д) проводится обсуждение построенных моделей между группами, устранение недостатков и окончательное оформление результатов самостоятельной работы.

В процессе проведения занятия особое внимание уделяется вопросам, связанным с определением всех составляющих архитектуры системы защиты, содержанием основных компонентов моделей СЗИ. Подчеркивается важнейшая роль моделирования процессов защиты как единственного инструмента исследования этой слабоструктурированной области.

В процессе обсуждения вопросов, поставленных во время дискуссии и связанных с технологическим и организационным построением СЗИ, подчеркивается, что каждой стадии создания последней соответствует целый спектр разноплановых задач, имеющих свои специфические особенности. Каждая стадия требует соответствующих организационных и технических решений, а также нормативно-методического обеспечения и документации.

В результате проведения занятия студенты должны знать:

- факторы и условия, подлежащие учету при формировании моделей СЗИ;
- состав и специфические особенности элементов основных моделей СЗИ;
- общее содержание технологического цикла построения СЗИ и характеристику составляющих его стадий.

Задание студенту

Моделирование является одним из эффективных инструментов анализа сложных систем различной природы, и комплексные системы защиты в данном случае не являются исключением. Под моделью будем понимать описательно представленную систему, которая отображает объект исследования и способна замещать его так, что изучение этой системы дает адекватную информацию об объекте. Модели различаются по используемым средствам моделирования, формам и методам описания характеристик моделирования и некоторым другим критериям.

Необходимо письменно:

- представить состав основных функций и организационных элементов СЗИ;
- объяснить, как содержательно взаимосвязаны функциональная и организационная структуры СЗИ;
- построить и графически представить функциональную и организационную модели системы защиты информации объекта, описание которого приведено в приложении к заданию.

Приложение к заданию

Оцениваемый объект представляет собой научно-производственное предприятие, ориентированное на выпуск сложных, дорогостоящих изделий специального назначения. Предприятие обладает высоким техническим потенциалом, имеет сложное оборудование и квалифицированных специалистов. В состав предприятия входит специальное конструкторское бюро с собственной гражданской и оборонной

тематикой.
В условиях резкого сокращения оборонных заказов предприятие вынуждено было начать поиск внебюджетных источников инвестиций. Одним из таких источников стало производство электрохромных активных зеркал заднего вида для легковых автомобилей, предназначенных на свободную реализацию. Такие зеркала являются уникальными для России, обладают «ноу-хау» и имеют конкурентные преимущества высокого порядка, преодоление которых для конкурентов является сложной проблемой. Аналогичные изделия, которые поставляются в Россию, производятся еще только двумя американскими фирмами (Донелли и Гентакс). Потребителем их продукции в России является представительство фирмы Альфа-Ромео, офис которого находится рядом с центральным административным корпусом здания рассматриваемого предприятия.
Основные производственные помещения (цеха), где изготавливаются изделия, находятся в г. Чехове. Что касается представительства (центральный офис), в котором располагается руководящий аппарат, то он находится в центре Москвы. Рядом с основным корпусом административного здания находится строение, которое одновременно выполняет функции хранилища готовой продукции и выставочного комплекса.
Система защиты объекта построена по принципу выделения защищаемых зон и их декомпозиции. Внешняя зона защиты охватывает территорию от ограждения до периметра зданий (включая автостоянку).
Внутренняя зона разделена:
- на сектор защиты выделенных помещений в 1 комнату;
- сектор защиты хранилища и выставочного комплекса.

Для обеспечения безопасности внешней зоны установлено металлическое ограждение высотой 3 метра.
Безопасность внутренней зоны обеспечивается следующими средствами, методами и мероприятиями:
- при входе в каждый корпус осуществляется электронный контроль. Посетители и сотрудники проходят через специальные ворота, где определяется, нет ли при них оружия и опасных предметов. Кроме того, у сотрудника проверяется пропуск, а у посетителей — документ, удостоверяющий личность;
- имеется система теленаблюдения. Сигналы с ТВ-камер выводятся на цифровые анализаторы. При срабатывании сигналов тревоги изображения с тревожных камер выводятся на видеомагнитофон;
- установлена система охранной сигнализации с резервным и аварийным источниками питания;
- выделенные помещения оборудованы магнитными датчиками, реагирующими на прохождение человека с металлическим предметом достаточно большой массы;
- применяются заранее оговоренные условные фразы и кодовые выражения при ведении телефонных разговоров по городским каналам связи о времени и месте проведения важных деловых встреч и совещаний;
- в Устав и правила трудового распорядка, а также в контракты сотрудников внесены специальные разделы и пункты, касающиеся правил обеспечения защиты информации;
- ежегодно проводится обучение сотрудников правилам и процедурам работы с конфиденциальной информацией;
- определен круг лиц, которые в силу занимаемого служебного положения на предприятии имеют доступ к защищаемой информации;
- осуществляется взаимодействие с органами внутренних дел по вопросам обеспечения безопасности;
- в выделенных помещениях применяются звукопоглощающие облицовки и двойные оконные переплеты для защиты от прослушивания;
- используются светонепроницаемые стекла, занавески, драпировки и другие защитные

материалы для защиты от наблюдения и фотографирования.
Для защиты локально-вычислительной сети предусмотрено следующее:
- идентификация технических средств, файлов и аутентификация пользователей;
- регистрация и контроль работы технических средств и пользователей;
- уничтожение информации в ЗУ после использования;
- установлены специальные антивирусные средства;
- ведется учет носителей.

Координирует действия по обеспечению безопасности служба защиты информации, являющаяся самостоятельным структурным подразделением.

Занятие 5. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ (проверка сформированности компетенций УК-4, ОПК-3)

Вопросы:

1. Каковы требования, предъявляемые к сотрудникам, обеспечивающим функционирование СЗИ?
2. Как определяется состав и численность сотрудников, обеспечиваюших функционирование СЗИ?
3. Какие нормативные документы регламентируют деятельность и взаимодействие персонала по защите информации?
4. Каковы особенности мотивации деятельности персонала, связанного с защитой информации?

Занятие проходит в форме дискуссии по поставленным вопросам. Особое внимание уделяется вопросам определения состава кадрового обеспечения функционирования комплексных систем защиты и распределения функций по защите информации. Обращается внимание на сложность и многоплановость решения проблемы кадрового обеспечения СЗИ. В ходе занятия студентам предлагается сформировать пакет документов, регламентирующих деятельность персонала, обеспечивающего функционирование СЗИ. В рамках обсуждения вопросов, касающихся подбора персонала, рассматриваются различные психологические тесты, позволяющие выявить профессиональные и психологические особенности личности, а также инструменты воздействия на мотивационную сферу деятельности персонала, занятого защитой информации.

В результате проведения занятия студенты должны знать:
- состав кадрового обеспечения функционирования СЗИ;
- какие нормативные документы регламентируют деятельность персонала по комплексной защите;
- какие методы подбора, обучения, а также воздействия на мотивационную сферу деятельности персонала используются при обеспечении функционирования СЗИ.

Задание студенту

Анализируя статистические данные в отечественных и зарубежных публикациях можно сделать вывод, что около 70 % всех нарушений, связанных с безопасностью информации, совершаются именно сотрудниками предприятия. В этих условиях, когда кадровый фактор приобретает все большее значение для эффективности и успешности производственной и других видов деятельности любого предприятия, необходимо уделять особое внимание социально-психологическим аспектам при построении комплексных систем защиты информации.

Необходимо письменно:
- определить состав пакета документов, регламентирующих деятельность персонала по защите информации;
- сформулировать требования, которым должен соответствовать кандидат на должность начальника службы безопасности коммерческой фирмы. Требования необходимо структурировать по критериям:

— образование;
— интеллектуальные факторы;
— личностные факторы;

— физические характеристики;
— характер.

Занятие 6. СУЩНОСТЬ, СТРУКТУРА И СОДЕРЖАНИЕ ОБЩЕЙ ТЕХНОЛОГИИ УПРАВЛЕНИЯ СЗИ (проверка сформированности компетенции УК-2)

Вопросы:
1. Каково основное содержание, принципы и цели управления СЗИ?
2. Какова структура и содержание общей технологии управления и функционирования СЗИ?
3. Какими принципами руководствуются при управлении СЗИ?
4. Какие основные функции входят в состав технологии функционирования СЗИ?

Занятие проводится в форме диалога между преподавателем и студентами и выполнения практического задания. В качестве задания студентам предлагается в письменной форме сформулировать определения понятий «технология управления КСЗИ», «технология функционирования СЗИ» и сделать их сравнительный анализ. Для выполнения задания студенты обеспечиваются материалами, в которых приводится перечень существующих определений понятия «технология».

В процессе проведения занятия подробно разбираются положения, касающиеся сущности и особенностей процессов управления СЗИ, выбора стиля руководства деятельностью основных подразделений, специфики процедуры принятия управленческих решений. В процессе обсуждения вопросов акцент делается на сравнительном анализе содержания общих функций управления в организационных системах и системах, обеспечивающих комплексную защиту информации.

В результате проведения занятия студенты должны знать:

- определение и особенности технологии управления СЗИ; основные цели и принципы организации управления функционированием СЗИ;
- особенности технологии принятия решений по обеспечению функционирования СЗИ; состав и общее содержание функций управления СЗИ.

Задание студенту

Одним из важнейших условий повышения эффективности функционирования сложных организационно-технических систем является целенаправленное управление процессами, происходящими в этих системах. Чем больше масштабы системы и разнороднее ее элементы, тем существеннее зависимость ее функционирования от разработки эффективной технологии управления. При этом под функционированием будем понимать следующее: «нахождение системы в рабочем состоянии; выполнение системой своих функций». Подчеркнем, что для систем комплексной защиты чрезвычайно важны вопросы разработки технологии управления.

Предлагается письменно:

1. На основе обобщения приведенных интерпретаций определений понятия «технология» сформулировать свой вариант определения понятия «технология управления СЗИ» и «технология функционирования СЗИ».
2. Провести сравнительный анализ рассматриваемых понятий.
3. Определить, на какие этапы делится процедура принятия решения, учитывая, что оно (принятие решения) составляет основу технологии управления.

Перечень существующих определений понятия «технология»

1. Технология — любое средство преобразования исходных материалов, будь то люди, информация или физические материалы, для получения желаемых продукций или услуг.
2. Технология — (искусство, мастерство, умение) — совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или

полуфабриката, осуществляемых в процессе производства продукции.
3. Технология — процессы подготовки, передачи, накопления и обработки информации с помощью вычислительных машин.
4. Технология — система взаимосвязанных способов обработки материалов и приемов изготовления продукции в производственном процессе.
5. Технология — совокупность методов, производственных процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации для снижения трудоемкости процессов использования информационного ресурса, повышения их надежности и оперативности.
6. Технология — совокупность технологических элементов, например устройств или методов, используемых людьми для обработки информации.

Занятие 7. СУЩНОСТЬ И СОДЕРЖАНИЕ ФУНКЦИЙ ПЛАНИРОВАНИЯ И КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ СЗИ (проверка сформированности компетенции ОПК-3)

Вопросы:
1. Каковы основные способы и стадии планирования СЗИ?
2. Каково содержание основных задач планирования СЗИ?
3. В чем особенности структуры и содержания планов организации и функционирования СЗИ?
4. Какие факторы могут оказать влияние на выбор принципов и способов планирования?
5. Какие виды контроля функционирования СЗИ существуют?
6. В чем проявляются особенности контрольных процедур функционирования СЗИ?
Занятие проводится в форме обсуждения подготовленных сообщений, дискуссий по выдвинутым в ходе обсуждения вопросам и выполнения практического задания. В качестве практического задания студентам предлагается разработать структуру плана мероприятий по организации СЗИ. Для выполнения задания студенты обеспечиваются материалами, в которых приводится общая, поэтапная программа действий, охватывающая процесс организации системы защиты информации на любом предприятии. В процессе проведения занятия внимание студентов обращается на специфические особенности функций планирования и контроля функционирования СЗИ. В процессе обсуждения вопросов акцент делается на содержательном аспекте процессов планирования и контроля, разбираются факторы, влияющие на выбор принципов, способов планирования и видов контроля акционирования СЗИ. Подчеркивается, что при организации контроля очень большое значение имеет выбор информативных параметров контроля их значений.
В результате проведения занятия студенты должны знать:
- состав и содержание задач планирования СЗИ; структуру и содержание планов функционирования СЗИ;
- основные положения по организации контроля функционирования СЗИ;
- существующие формы контроля функционирования СЗИ и их особенности.

Задание № 1 студенту
Планирование является первичной функцией управления. Планирование обеспечивает основу для всех управленческих решений. Процесс планирования включает в себя несколько этапов и каждый этап имеет свое специфическое содержательное наполнение.
Необходимо письменно:
- определить, какие общие этапы включает в себя планирование организации комплексной системой защиты информации;
- разработать структуру плана организации СЗИ на основе предложенной общей,

поэтапной программы действий (см. Приложение 2), охватывающей процесс организации СЗИ на любом предприятии;

- предложить свое содержательное наполнение разработанной структуры плана.

Задание № 2 студенту

Контроль как функция управления не уступает по важности планированию, календарно-плановому руководству и позволяет видеть всю действительную картину состояния функционирования системы защиты. Место и значение контроля определяется тем, что он является способом организации обратной связи, благодаря которой субъект управления в СЗИ получает информацию о ходе выполнения его решения. Поэтому от эффективности контрольных процедур во многом зависит качество принимаемых решений и их своевременное исполнение.

Необходимо письменно:

- сформулировать определение понятия «контроль функционирования СЗИ»;
- определить, в чем заключаются особенности организации и контроля функционирования СЗИ и систем другого назначения (например, производственных, систем связи, АС и т. д.);
- графически представить алгоритм контроля в СЗИ;
- заполнить классификационную таблицу (табл. П1.2).

Таблица П1.2

Характеристики видов контроля	Значения характеристик
Периодичность проведения	Оперативный
	Периодический
	Эпизодический

Занятие 8. УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ (проверка сформированности компетенции УК-2, УК-4)

Вопросы:

1. Как понимается чрезвычайная ситуация с точки зрения организации и функционирования СЗИ?
2. Какие виды чрезвычайных ситуаций могут возникать при функционировании СЗИ?
3. Каковы основные подходы к предупреждению, локализации и ликвидации чрезвычайных ситуаций?
4. Какие факторы оказывают влияние на принятие решений по защите в условиях чрезвычайной ситуации?

Занятие проводится в форме обсуждения поставленных вопросов и выполнения практического задания. Для выполнения практического задания студенты обеспечиваются необходимыми методическими материалами. В задании студентам предлагается разработать паспорт «риска» объекта защиты. В качестве объекта защиты выступает фирма, описание которой приведено в задании. В методических материалах, которыми обеспечиваются студенты, приведены примеры программ действий в чрезвычайных обстоятельствах для систем обработки информации двух предприятий различного назначения.

В процессе проведения занятия внимание студентов обращается на содержательные аспекты понятия чрезвычайной ситуации с точки зрения защиты информации. Подчеркивается, что чрезвычайная ситуация может оказать влияние как на саму технологию организации защиты, так и на функционирование СЗИ в целом. В ходе

занятия подробно разбираются методические подходы к разработке процедур принятия решений в условиях чрезвычайной ситуации.

В результате проведения занятия студенты должны знать:

- определение чрезвычайной ситуации с точки зрения организации и обеспечения защиты;
- виды чрезвычайных ситуаций и характер их последствий для защиты;
- состав и содержание мероприятий по предупреждению, локализации и ликвидации чрезвычайных ситуаций;
- содержание процедуры принятия решений по обеспечению защиты в условиях возникновения и протекания чрезвычайной ситуации.

Задание студенту

Любая, даже очень эффективно организованная система защиты информации подвержена различного рода неблагоприятным воздействиям природного, технического и иного характера, которые имеют преднамеренный или случайный характер и могут привести к появлению так называемых чрезвычайных ситуаций (ЧС). Возникновение подобных ситуаций не зависит от чьих-либо желаний, финансовых и других возможностей организаций и предприятий, но неподготовленность к ним может иметь серьезные последствия, особенно с точки зрения обеспечения безопасности.

Предлагается письменно:

- на основе анализа определений различных понятий, относящихся к данной предметной области, сформулировать определение понятия «чрезвычайная ситуация» в отношении процессов защиты информации;
- определить критерии, по которым можно провести классификацию потенциально возможных чрезвычайных ситуаций, способных влиять на функционирование СЗИ;
- изучить предлагаемую статью, посвященную вопросам разработки программы действий в чрезвычайных ситуациях на примере банка, и самостоятельно сформировать:

— а) структуру паспорта риска объекта;

— б) структуру группы (комитета) по управлению в условиях ЧС и ликвидации их последствий.

Перечень определений различных понятий, относящихся к категории экстремальных (чрезвычайных) событий

Авария — опасное происшествие на хозяйствующем субъекте, транспорте или на линиях связи, представляющее угрозу жизни и здоровью людей либо приводящее к разрушению производственных помещений, повреждению или уничтожению оборудования, механизмов, транспортных средств, сырья и готовой продукции, а также к нарушению производственного процесса.

Катастрофа — внезапное бедствие, событие, влекущее за собой тяжелые последствия.

Кризисная ситуация — резкий, крутой перелом в чем-либо, тяжелое переходное состояние.

Риск — тип реализации опасностей определенного класса, который может быть определен как частота или как вероятность возникновения одного события при наступлении другого события.

Чрезвычайная ситуация — комплекс событий, протекание и результат наступления которых приводит к реализации в районе чрезвычайной ситуации, опасной для жизни и здоровья людей, а также материальных ценностей, нарушение экономической деятельности, нормального жизнеобеспечения, функционирования схем управления и связи, а также экологического равновесия.

Приложение 1 Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: формирование знаний о процессах управления всеми средствами защиты информации и мониторинге безопасности информационной системы.

Задачи дисциплины:

-освоение знаний об архитектуре управления информационной безопасностью (ИБ) корпоративной информационной системы (КИС), функциональных системах управления и мониторинге безопасности КИС;

-приобретение практических навыков по использованию соответствующих нормативно-правовых документов и программных инструментариев для управления ИБ.

Дисциплина направлена на формирование следующих компетенций:

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

УК-4 Знает современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации;

ОПК- 3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать: как формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и экономической целесообразности;

как организовать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

как определить виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

Уметь: принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

применять комплексный подход к обеспечению информационной безопасности

Владеть: навыками работы с нормативными правовыми актами;

навыками организации работы малого коллектива исполнителей с учетом требований защиты информации.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме выполнения практических заданий, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлена основная литература*	17.03.2023	***9***

Приложение 1
к листу изменений

Обновление основной литературы (2023 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:
1. Дополнить раздел **Основная литература**

Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В.И. Новосельцев, С.С. Кочедыков, Д.Е. Орлова, К.А. Плющик ; под ред. В.И. Новосельцева. — Москва : ИНФРА-М, 2023. — 235 с. — (Научная мысль). — DOI 10.12737/1921360. - ISBN 978-5-16-018194-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1921360

2. Дополнить раздел **Дополнительная литература**

Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1900721

Составитель:
К.т.н., доцент, доцент, Н.В.Гришина