МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)»,

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
Рабочая программа дисциплины

Составитель(и):
К.т.н, доцент, доцент, Н.В.Гришина

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

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 определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Знать: как организовать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Уметь: применять комплексный подход к обеспечению информационной безопасности
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую	Знать: основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации

	характеристику преступлений в сфере компьютерной информации и меры ответственности за утрату, разглашение, модификацию и уничтожение защищаемой информации	
	ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	Уметь: предпринимать необходимые меры по восстановлению нарушенных прав по защите информации
	ОПК-5.3 Владеет навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации	Владеть: навыками разрабатывать локальные правовые документы, регламентирующие работу по обеспечению информационной безопасности в организации
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации	Уметь: разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
	ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации	Владеть: навыками по разработке политики безопасности объекта информатизации

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части, формируемой участниками образовательных отношений блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Основы российского права, Менеджмент, Теория информации, Основы информационной безопасности, Основы управленческой деятельности.
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Преддипломная практика.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 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
7	Лекции	**26**
7	Практические занятия	**28**
	Всего:	**54**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 54 академических часа(ов).

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	ТЕМА 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	ТЕМА 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	ТЕМА 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	ТЕМА 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. Предпроктное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.
5	ТЕМА 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	ТЕМА 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	ТЕМА 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	ТЕМА 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	ТЕМА 9. СУЩНОСТЬ И СОДЕРЖАНИЯ КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ	Понятие и виды контроля функционирования СЗИ. Цель проведения контрольных мероприятий в СЗИ. Методы контроля. Особенности проведения контроля функционирования СЗИ. Анализ и использование результатов проведения контрольных мероприятий.
10	ТЕМА 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 раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1	Предмет, задачи и содержание курса	Лекция 1 Практическое занятие 1,2	Вводная лекция с использованием видеоматериалов
2	Определение условий функционирования системы защиты информации		Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
3	Разработка модели системы защиты информации	Лекция 2 Практическое занятие 3	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
4	Технологическое и организационное построение системы защиты информации	Лекция 3 Практическое занятие 4	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
5	Кадровое обеспечение функционирования системы защиты информации	Лекция 4 Практическое занятие 5	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
6	Материально-техническое и нормативно-методическое обеспечение системы защиты	Лекция 5	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством

	информации		электронной почты
7	Назначение, структура и содержание управления системой защиты информации	Лекция 6 Практическое занятие 6	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
8	Принципы и методы планирования функционирования системы защиты информации	Лекция 7 Практическое занятие 7	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
9	Сущность и содержание контроля функционирования системы защиты информации	Лекция 8 Практическое занятие 8	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты
10	Управление системой защиты информации в условиях чрезвычайных ситуаций	Лекция 9 Практическое занятие 9	Проблемная лекция Дискуссия Консультирование и проверка домашних заданий посредством электронной почты

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - практические задания (занятия 1-4, 6-7) - практические задания (занятия 5,8-9)	 8 баллов 5 балла	 45 баллов 15 баллов
Промежуточная аттестация – экзамен (экзамен по билетам)		40 баллов
Итого за семестр		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 оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе 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/ зачтено	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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	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	неудовлет-ворительно/ не зачтено	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

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

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

Примерное задание для практической работы по теме 3.

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 её элементы, тем существеннее зависимость её функционирования от разработки эффективной технологии управления. При этом под функционированием будет понимать: 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» (см. далее) 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

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.

Примерные контрольные вопросы к экзамену.

1. На конкретных примерах опишите взаимосвязь процессов планирования и контроля в комплексной системе защиты информации. Код контролируемой компетенции- УК-2
2. Разработайте пример реализации модели процесса контроля в конкретной системе защиты информации. Код контролируемой компетенции- ОПК-5
3. Роль мотивации в развитии теории и практики управления. Код контролируемой компетенции- ОПК-5

4. Каково значение обратной связи в процессе информационного обмена в системе защиты информации. Код контролируемой компетенции- УК-2
5. Основные способы и стадии планирования СЗИ. Код контролируемой компетенции- ОПК-6
6. Содержание основных задач планирования СЗИ. Код контролируемой компетенции- ОПК-6
7. Особенности структуры и содержания планов организации и функционирования СЗИ. Код контролируемой компетенции- УК-2
8. Факторы, влияющие на выбор принципов и способов планирования. Код контролируемой компетенции- УК-2
9. Организация сбора и обработки информации в процессе повседневной деятельности системы защиты информации. Код контролируемой компетенции- ОПК-6
10. Структура основных работ, подлежащих выполнению в процессе повседневной деятельности комплексной системы защиты информации. Код контролируемой компетенции- УК-2
11. Особенности оперативно-диспетчерского управления системы защиты информации. Код контролируемой компетенции- ОПК-5
12. Методы руководства выполнением плана деятельности системы защиты информации. Код контролируемой компетенции- ОПК-6
13. Сущность и виды контроля функционирования СЗИ. Код контролируемой компетенции-
14. Особенности контрольных процедур СЗИ. Код контролируемой компетенции- ОПК-6
15. Как понимается чрезвычайная ситуация с точки зрения организации и функционирования СЗИ? Код контролируемой компетенции- ОПК-5 Какие виды чрезвычайных ситуаций могут возникать при функционировании СЗИ? Код контролируемой компетенции- ОПК-6
16. Основные подходы к предупреждению, локализации и ликвидации последствий чрезвычайной ситуации. Код контролируемой компетенции- УК-2
17. Факторы, оказывающие влияние на принятие решений по ЗИ в условиях чрезвычайной ситуации. Код контролируемой компетенции- ОПК-5

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Федеральный закон РФ «О коммерческой тайне» от 29 июля 2004 года №98-ФЗ Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

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 (дата обращения: 12.05.2021). – 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 (дата обращения: 12.05.2021). – Режим доступа: по подписке.

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 (дата обращения: 12.05.2021). – 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

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
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

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 доской, компьютером или ноутбуком, проектором (стационарным или переносным) 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. Код контролируемой компетенции- УК-2
Тема 1. Определение условий функционирования системы защиты информации**.**
Вопросы для обсуждения:
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.

Задание:

Важное значение имеет правильное толкование основных понятий теории защиты информации, поэтому необходимо уточнить базовые определения. Это в первую очередь касается определений понятий «система защиты информации», «цели организации и функционирования СЗИ».

Необходимо письменно:

- на основе анализа приведенных определений понятия «система» (смотри ниже) выделить основные свойства систем;
- сформулировать свой вариант определения понятия «комплексная система защиты информации»;
- сформулировать свой вариант определения понятия «цель организации и функционирования СЗИ»;
- разработать пирамиду целей СЗИ;
- определить основные классы задач СЗИ и дать их краткую и обобщенную характеристику.

Определения понятия «система»:

1. «...все, состоящее из связанных друг с другом частей, мы будем называть системой» (Ст. Бир).
2. «Система — это комплекс взаимодействующих компонентов» (Л. Берталанфи).
3. «Система — это множество взаимосвязанных элементов... не существует одного подмножества элементов, не связанного с другим подмножеством» (Р. Акофф).
4. «Система — это не просто совокупность единиц... а совокупность отношений между этими единицами» (А. Рапопорт).
5. «И хотя понятие системы определяется по-разному, обычно все-таки имеется в виду, что система представляет собой определенное множество взаимосвязанных элементов, образующих устойчивое единство и целостность, обладающее интегральными свойствами и закономерностями» (В. П. Кузьмин).
6. «Мы можем определить систему как нечто целое, абстрактное или реальное, состоящее из взаимосвязанных взаимодействующих или взаимозависимых частей» (Ф. Ханика).
7. «Любой комплекс, любая форма распределения активности в цепи, рассматриваемая каким-либо наблюдателем как закономерное, является системой» (Г. Паск).
8. «Система — это то, что получается в результате оптимизации конструкций путем всестороннего анализа взаимосвязанных факторов, влияющих на ее существенные характеристики» (Б. Байцер).
9. «Системой можно назвать только такой комплекс избирательно вовлеченных компонентов, у которых взаимодействие и взаимоотношение приобретают характер взаимодействия компонентов на получение фокусированного полезного результата» (П. К. Анохин).

Занятие 2. Код контролируемой компетенции- УК-2

Тема 1. Определение условий функционирования системы защиты информации**.**

Вопросы для обсуждения:
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.
Задание:
Студентам предлагается письменно сформулировать факторы, которые тем или иным образом влияют на организацию системы защиты информации. Обязательным показать каким образом и в какой степени указанные факторы влияют на организацию системы защиты информации.
Необходимо представить не менее 20 факторов с подробными комментариями.

Занятие 3. Код контролируемой компетенции- ОПК-5
Тема 2. Разработка модели системы защиты информации.
Вопросы для обсуждения:
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 сообщений по вопросам темы. Обсуждение сообщений дополняется проведением дискуссии в форме ответов на поставленные вопросы, а также выполнением практического задания.
Задания:
1.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 СЗИ и определяют основные функции системы;
в) проводится анализ взаимосвязи функциональной и организационной структуры СЗИ;
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.

2.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 4. Код контролируемой компетенции- УК-2

Тема 3. Технологическое и организационное построение системы защиты информации.

Вопросы для обсуждения:

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?
5. Какие компоненты входят в состав структуры СЗИ?
6. Какие критерии положены в основу классификации каждой группы средств, входящих в состав СЗИ?
7. Какие требования предъявляются к выбору методов и средств защиты при организации и функционировании СЗИ?
8. Как определяются условия функционирования СЗИ?

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 СЗИ, внимание студентов обращается на те аспекты, содержание и вес тех факторов, которые в данной предметной области подлежат учету.

1. Задание:

Многообразие угроз информации, исходящих от различных категорий нарушителей, и степень их опасности вызывает вопрос о том, каково их соотношение в практике деятельности подразделений СЗИ 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.1. следующего вида:

Таблица 1.

Категории нарушителей	Дестабилизирующие воздействия									
	Объекты защиты (Q_i...Q_n)									
	I	II								VII
		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 5. Код контролируемой компетенции- ОПК-5
Тема 4. Кадровое обеспечение функционирования системы защиты информации.
Вопросы для обсуждения:
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.
Задания:
1.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. Код контролируемой компетенции- ОПК-6

Тема 6. Назначение, структура и содержание управления системой защиты информации.
Вопросы для обсуждения:
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 СЗИ», «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.
Задания:
1. 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 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. Код контролируемой компетенции- ОПК-5
Тема 7. Принципы и методы планирования функционирования системы защиты информации**.**
Вопросы для обсуждения:
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.
Задания:
1. 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 общей, поэтапной программы действий (Таб 1.) охватывающей процесс организации СЗИ на любом предприятии;
- предложить свое содержательное наполнение разработанной структуры плана.

Таб.1 ПРОГРАММА ДЕЙСТВИЙ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

ЭТАПЫ	1. АНАЛИЗ состава и содержания информации	2. АНАЛИЗ ценности информации	3. ОЦЕНКА Уязвимости информации	4.ИССЛЕДОВАНИЕ действующей системы защиты информации
Какие вопросы надо решать?	Какие сведения следует охранять? Кого интересуют охраняемые сведения и когда? Почему они нуждаются в получении этих сведений?	Какие виды информации имеются? Какова ценность каждого вида информации? Какая защита необходима для информации?	Какие каналы утечки информации имеются? Какова степень уязвимости каналов утечки? Насколько уменьшится уязвимость информации при использовании системы и средств защиты?	Какие меры безопасности используются? Каков уровень организации защиты информации? Какова стоимость доступных мер защиты информации? Какова эффективность действующей системы защиты информации?
Ответственные исполнители	Руководство организации предприятия	Администрация	Специалисты отдела безопасности (ОБ)	Администрация, линейное руководство, ОБ

Какие мероприятия следует провести?	Обеспечить изучение вопросов состояния секретности и защиты информации Составить подробный обзор всех информационных потоков Проверить обоснованность и необходимость защиты информационных потоков	Установить правовые и законодательные требования Разработать принципы определения ценности информации Определить ценность каждого вида информации	Составить перечень каналов утечки информации Составить перечень уязвимых помещений Определить характер охраняемых сведений и приоритеты. Классифицировать информацию по приоритетам и ценности	Составить аналитический обзор действующей системы защиты информации Оценить затраты и степень риска при действующей системе защиты информации
Что особенно нужно учитывать?	Оценить необходимость накопленной информации	Законодательную ответственность администрации за ЗИ. Степень ущерба при раскрытии, потере, ошибках в информации Наличие нормативных документов	Распределение приоритетов при организации защиты. Определить степень уязвимости и секретности информации	Усиление безопасности не остановит злоумышленника Чем новая технология может быть эффективнее по критерию эффективность/стоимость
Какие документы разрабатываются?	Информационная модель организации, предприятия	Структура классификации информации, принципы Классификации информации Законодательные требования инструкции, нормы	Классификатор информации Классификатор каналов утечки информации	Аналитический обзор действующей СЗИ и ее безопасность
ЭТАПЫ	5. ОЦЕНКА Затрат на разработку новой службы ЗИ	6.ОРГАНИЗАЦИЯ мер защиты информации	7.ЗАКРЕПЛЕНИЕ персональной ответственности за защиту информации	8.РЕАЛИЗАЦИЯ технологии защиты информации

Какие вопросы надо решать?	Какова стоимость новой системы защиты? Какой уровень организации новой системы? Насколько она доступна ? Какой выигрыш будет получен при новой системе?	Какие проявляются новые функции? Какой потребуется новый персонал? Какая квалификация необходима для выполнения новых обязанностей?	Какие конкретно сотрудники имеют доступ к охраняемым сведениям? Проверены ли эти сотрудники на благонадежность ?	Каков приоритет секретной информации и изделий? Какие дополнительные ресурсы потребуются? Кто отвечает за согласование проекта СЗИ с партнерами? Замысел реализации проекта.
Ответст-венные исполни тели	Администрация, планово-финансовая служба	Администрац ия, линейное руководство, ОБ	Линейное руководство, ОБ	Администрация, группа реализации проекта, ОБ, линейное руководство
Какие мероприятия следует провест и?	Разработать план реализации замысла на создание новой системы защиты информации Изыскать необходимые ресурсы	Определить ответственнос ть за безопасность информации в каждом подраз-делении Подготовить инст-рукцию по органи-зации ЗИ.	Проверить персонал, обрабатывающий секретную информацию Подготовить перечни секретных сведений для всех сотрудников	Разработать реализации проекта новой системы защиты информации Определить контрольные сроки и позиции их выполнения
Что особенн о нужно учитыва ть?	Установить требования по финансированию и его источники	Важность организацион ных мер защиты информации	Необходимость регулярного контроля за работой СЗИ.	Полноту реализации требований новой системы защиты информации
Какие докумен ты разрабат ываются ?	Средства служба ЗИ Бюджет на разра-ботки, внедрение и сопровождение новой службы ЗИ	Организацион но-функ-циональная схема СЗИ Порядок и правила работы в новых условиях	Профили секретности сотрудников и линейных подразделений	Подробный бюджет проекта новой СЗИ

ЭТАПЫ	9. СОЗДАНИЕ обстановки созна-тельного отношения к ЗИ	10. КОНТРОЛЬ И ПРИЕМ в эксплуатацию новой системы защиты
Какие	Ориентирована ли политика	Какой должен быть состав специальной

вопросы надо решать?	органи-зации на защиту информации? Имеется ли программа подготовки и обучения сотрудников организации в новых условиях работы с СЗИ?	группы приема системы? Имеются ли стандарты безопасности и секретности информации? Насколько эффективна новая система защиты информации? Какие улучшения можно произвести?
Ответственные испол-нители	Линейное руководство, ОБ, ответственные за безопасность информации	Группа ревизии, приема и контроля работы служба ЗИ
Какие мероприятия следует провести?	Разработать программы подготовки сотрудников Оценить личные качества сотрудников по обеспечению безопасности инф-ции	Утвердить состав группы ревизии Рассмотреть законодательные требования Переоценить уязвимость информации и степень риска Оценить точность и полноту реализации проекта
Что особенно нужно учитывать?	Необходимость комплексной защиты информации Сознательное отношение к защите информации и бдительность всего персонала	Оценить реальную эффективность новой системы защиты Необходимость систематического контроля за работой служба ЗИ
Какие документы разрабатываются?	Руководство по защите конфиденциальной информации Программа обучения сотрудников	Отчет и рекомендации, выработанные группой ревизии

Занятие 8. Код контролируемой компетенции- ОПК-6
Тема 8. Сущность и содержание контроля функционирования системы защиты информации.
Задания:
1.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. 2.).

Таблица 2.

Характеристики видов контроля	Значения характеристик
Периодичность проведения	Оперативный

	Периодический Эпизодический
….	…..

Занятие 9. Код контролируемой компетенции- ОПК-6

Тема 9. Управление системой защиты информации в условиях чрезвычайных ситуаций.

Вопросы для обсуждения:

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.

Задания:

1. 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. 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;
- 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

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

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 корпоративной информационной системы , функциональных системах управления и мониторинге безопасности корпоративной информационной системы;

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

Дисциплина направлена на формирование следующих компетенций:

- УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
- ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен:

Знать

- 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;

-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 формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и экономической целесообразности.

Уметь

- принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;
- применять комплексный подход к обеспечению информационной безопасности;
- собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

Владеть

- методами выявления угроз безопасности информации;
- навыками организации работы малого коллектива исполнителей с учетом требований защиты информации;

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

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.