

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

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«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

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ. РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

Составитель:

к.и.н., доцент И.А. Русецкая

УТВЕРЖДЕНО

Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1.	Пояснительная записка	4
1.1.	Цель и задачи дисциплины	4
1.2.	Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций	4
1.3.	Место дисциплины в структуре образовательной программы	5
2.	Структура дисциплины	5
3.	Содержание дисциплины	5
4.	Образовательные технологии	9
5.	Оценка планируемых результатов обучения	11
5.1	Система оценивания	11
5.2	Критерии выставления оценки по дисциплине	12
5.3	Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	13
6.	Учебно-методическое и информационное обеспечение дисциплины	15
6.1	Список источников и литературы	15
	Дополнительная	Ошибка! Закладка не определена.
6.2	Перечень ресурсов информационно-телекоммуникационной сети «Интернет».	16
6.3	Профессиональные базы данных и информационно-справочные системы	16
7.	Материально-техническое обеспечение дисциплины	16
8.	Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов	17
9.	Методические материалы	18
9.1	Планы практических занятий	18
	Приложение 1. Аннотация рабочей программы дисциплины	25

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины - формирование представлений о теоретических и методологических основах организационного проектирования, порядка построения, оценки и совершенствования систем защиты информации предприятия (организации) в целом и службы защиты информации.

Задачи дисциплины: рассмотрение сущности и задач организационного проектирования систем защиты информации, методов исследования, принципов организации проектирования и этапов разработки проекта, технологию организации службы защиты информации.

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 УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Знать: нормативно-правовые основы организационного проектирования в области защиты информации и методы управления процессом организационного проектирования. Уметь: поддерживать функционирование системы управления информационной безопасностью на этапе внедрения результатов организационного проектирования защиты информации и службы защиты информации. Владеть: навыками обеспечения организации проектирования систем защиты информации и служб защиты информации.
УК-9. Способен использовать базовые дефектологические знания в социальной и профессиональной сферах	УК-9.1. Понимает содержание инклюзивной компетентности, ее компоненты и структуру УК-9.2. Знает особенности применения базовых дефектологических знаний в социальной и профессиональной сферах	Знать: нормативно-правовые основы. Уметь: поддерживать уровень знаний в социальной и профессиональной сферах Владеть: навыками применения базовых дефектологических знаний в социальной и профессиональной сферах
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 Знает принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией ОПК-8.2 Умеет обобщать, анализировать и систематизировать научную информацию в области	Знать: основные понятия в области организационного проектирования защиты информации и службы защиты информации; базовые содержательные положения в этой области. Уметь: проводить предпроектное обследование, проводить анализ экономической целесообразности проектирования систем защиты

	информационной безопасности; пользоваться информационно-справочными системами ОПК-8.3 Владеет навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов	информации и службы защиты информации. Владеть: методикой определения структурного построения и состава системы защиты информации и службы защиты информации.
--	---	--

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Комплексная защита объектов информатизации» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Правовое и организационное обеспечение информационной безопасности», «Основы управления информационной безопасностью».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения Преддипломной практики.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5 з.е., 180 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	22
7	Практические занятия	26
8	Лекции	26
8	Практические занятия	28
Всего:		102

Объем дисциплины в форме самостоятельной работы обучающихся составляет 78 академических часов.

3. Содержание дисциплины

Часть 1 (7 семестр). Организационное проектирование защиты информации

Тема 1. Введение. Понятие, назначение, состав и характеристика оргпроектирования систем защиты информации.

Предмет, задачи и содержание курса. Значение и место курса в подготовке бакалавров. Научная и учебная взаимосвязь курса и других дисциплин. Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения занятий. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы по курсу. Методика самостоятельной работы студентов по изучению курса. Знания и умения студентов, которые должны быть получены в результате изучения курса.

Общее понятие об оргпроектировании. Основные направления проектирования организации и технологии управления системой защиты информации.

Основные виды оргпроектирования. Состав проектных работ и факторы, определяющие их при рационализации системы ЗИ. Требования к проектированию. Системный подход к организации оргпроектирования. Состав и содержание процесса оргпроектирования. Основные стадии (этапы) оргпроектирования. Одностадийное и многостадийное проектирование. Выбор объекта организационного проектирования. Планирование и организация проектных работ. Предпроектное и детальное обследование (исследование) системы ЗИ. Техническое задание на проектирование. Технический (эскизный) проект. Рабочий проект. Внедрение проекта. Соотношение объемов проектных работ по стадиям. Технические требования к составу и содержанию работ на различных этапах оргпроектирования.

Тема 2. Методы оргпроектирования систем защиты информации.

Общая характеристика методов оргпроектирования. Цели и назначение методов оргпроектирования. Классификация научно-исследовательских методов оргпроектирования. Выбор и обоснование методики обследования. Методы исследования в оргпроектировании. Методы обследования (сбора исходных данных) системы защиты информации и службы ЗИ. Методы количественно-качественного анализа и синтеза полученной информации. Методы проектирования организации и технологии системы ЗИ. Обработка и обобщение материалов обследования.

Тема 3. Разработка документации оргпроцессов при проектировании систем защиты информации.

Состав документов оргпроекта. Классификация видов документов по каждому элементу системы управления ЗИ. Рабочая программа исследования. Разработка документации для сбора данных и подготовка методических указаний по их заполнению. Порядок разработки и оформления документов оргпроекта. Порядок внесения изменений в документы оргпроекта. Карты оргпроцессов. Представление результатов обследования различных подсистем изучаемой системы управления (технологические карты, блок-схемы, диаграммы, таблицы решений, матричные и графические модели документальные методы). Обследование документально-оформленного и фактического состояний объекта исследования. Обработка и обобщение материалов обследования.

Тема 4. Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно-нормативных документов, регламентирующих деятельность службы.

Условия и факторы, влияющие на структурное построение службы ЗИ. Организация и организационная структура службы защиты информации. Функции организации. Компоненты организационной структуры. Назначение организационной схемы. Проектирование организационной и функциональной модели службы ЗИ. Описание и графическое представление множества структурных, функциональных и информационных связей. Основные подходы и способы определения должностного состава службы ЗИ. Методика расчета штатной численности подразделений службы ЗИ.

Принципы исследования и проектирования систем документации. Основные виды и формы документов регламентирующих деятельность службы ЗИ. Порядок разработки положения о службе ЗИ. Разработка положений о структурных подразделениях службы ЗИ. Разработка штатного расписания службы ЗИ. Разработка должностных инструкций сотрудников службы ЗИ. Объективная необходимость управления системой организационно-нормативных документов.

Тема 5. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности.

Анализ и изучение оборудования и технических требований. Порядок выбора и распределения оборудования и технических средств в подразделениях. Однокритериальный и

многокритериальный подходы при выборе оборудования и технических средств. Разработка проекта оснащения рабочих мест сотрудников оборудованием и техническими средствами.

Понятие и содержание организации труда в организационных системах. Условия труда. Содержательность работ. Изучение планировки помещений и условий труда в подразделениях. Разработка предложений по созданию и совершенствованию условий и охране труда. Проектирование основных элементов труда сотрудников. Разработка и совершенствование требований по технике безопасности и пожарной безопасности.

Тема 6. Проектирование информационного обеспечения системы защиты информации.

Изучение видов и форм информационного обеспечения систем защиты информации. Интегрированные информационные системы как часть организационного проекта совершенствования системы защиты информации. Методы анализа информационных потоков. Общая структура информационного обеспечения. Множество моделей процессов обработки и передачи информации и их иерархическое строение. Технология информационного обеспечения системы ЗИ. Порядок и последовательность разработки проекта рационализации информационного системы ЗИ. Разработка предложений для обеспечения надежности и достоверности информационного обеспечения и защиты информации от различного рода угроз.

Тема 7. Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах».

Особенности работы системы ЗИ в «чрезвычайных ситуациях». Изучение, анализ и классификация возможных «чрезвычайных ситуаций» на предприятии.

Определение степени воздействия и оценка последствий «чрезвычайных ситуаций» на защищаемую информацию. Разработка проекта функционирования системы ЗИ в различных «чрезвычайных ситуациях».

Тема 8. Внедрение и оценка эффективности оргпроекта.

Содержание работ по внедрению проекта. Опытно-экспериментальная проверка проекта. Социально-психологическая и профессиональная подготовка сотрудников к внедрению оргпроекта. Организация процесса внедрения оргпроекта. Реализация мероприятий по организационному, технологическому, социально-психологическому, материально-техническому обеспечению внедрения проекта. Контроль за ходом внедрения. Методы комплексной оценки оргпроектов. Основные критерии оценки эффективности оргпроекта. Оптимизация проектных решений по экономическим, социальным критериям эффективности. Разработка методов оценки эффективности системы ЗИ.

Часть 2 (8 семестр). Управление службой защиты информации.

Тема 1. Введение. Место и роль службы защиты информации в системе защиты информации.

Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров по профилю «Организация и технология защиты информации». Научная и учебная взаимосвязь курса и других дисциплин специальности. Структура курса. Распределение тем по видам аудиторных занятий. Формы проведения практических занятий. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы по курсу. Методика самостоятельной работы студентов по изучению курса. Знания и умение студентов, которые должны быть получены в результате изучения курса.

Назначение службы защиты информации. Место службы защиты информации в системе безопасности предприятия. Служба защиты информации как составная часть системы защиты. Служба защиты информации как орган управления защитой информации. Служба защиты информации как координатор деятельности по обеспечению безопасности информации. Статус службы защиты информации в структуре предприятия.

Тема 2. Задачи и функции службы защиты информации. Организационные задачи и функции службы защиты информации.

Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.

Тема 3. Структура и штаты службы защиты информации.

Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты, функции сотрудников и уполномоченных службы защиты информации. Факторы, определяющие численность сотрудников службы защиты информации.

Тема 4. Организационные основы и принципы деятельности службы защиты информации.

Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации. Основные принципы организации и деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.

Тема 5. Подбор, расстановка кадров и обучение сотрудников службы защиты информации.

Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров. Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.

Тема 6. Организация труда сотрудников службы защиты информации.

Особенности содержания характера труда сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и содержание должностных инструкций сотрудников службы защиты информации. Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами). Обеспечение необходимых условий труда. Охрана труда. Культура труда. Карты организации трудового процесса.

Тема 7. Принципы и методы управления службой защиты информации.

Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой защиты информации.

Тема 8. Принципы и методы управления службой защиты информации.

Состав и содержание управленческих функций. Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Методы и формы контроля выполнения планов. Критерии эффективности работы службы защиты информации. Методы оценки качества работы службы защиты информации. Пути и способы повышения эффективности управления службой защиты информации.

4. Образовательные технологии

Часть 1 (7 семестр). Организационное проектирование защиты информации

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Понятие, назначение, состав и характеристика оргпроектирования систем защиты информации	Лекция Практическое занятие	Вводная лекция с использованием видеоматериалов Обсуждение поставленных вопросов
2	Методы оргпроектирования систем защиты информации	Лекция Практическое занятие	Лекция с разбором конкретных ситуаций Обсуждение поставленных вопросов
3	Разработка документации оргпроцессов при проектировании систем защиты информации	Лекция Практическое занятие	Лекция-визуализация Обсуждение поставленных вопросов
4	Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно-нормативных документов, регламентирующих деятельность службы	Лекция Практическое занятие	Лекция-визуализация Дискуссия
5	Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности	Лекция Практическое занятие	Лекция-визуализация Обсуждение поставленных вопросов
6	Проектирование информационного обеспечения системы защиты информации	Лекция Практическое занятие	Лекция-беседа Обсуждение поставленных вопросов
7	Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах»	Лекция Практическое занятие	Лекция-беседа Обсуждение подготовленных докладов, дискуссия,

8	Внедрение и оценка эффективности оргпроекта	Лекция Практическое занятие	Лекция-визуализация Проверка контрольной работы
---	---	--------------------------------	--

Часть 2 (8 семестр). Управление службой защиты информации.

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Место и роль службы защиты информации в системе защиты информации.	Лекция Практическое занятие	Вводная лекция с использованием видеоматериалов
2	Задачи и функции службы защиты информации.	Лекция Практическое занятие	Лекция с разбором конкретных ситуаций
3	Структура и штаты службы защиты информации.	Лекция Практическое занятие	Лекция-визуализация Консультирование и проверка выполнения практических заданий
4	Организационные основы и принципы деятельности службы защиты информации.	Лекция Практическое занятие	Лекция-визуализация Консультирование и проверка выполнения практических заданий
5	Подбор, расстановка кадров и обучение сотрудников службы защиты информации.	Лекция Практическое занятие	Лекция-визуализация Консультирование и проверка выполнения практических заданий
6	Организация труда сотрудников службы защиты информации.	Лекция Практическое занятие	Лекция-беседа Обсуждение подготовленных докладов, дискуссия, выполнение практического задания
7	Принципы и методы управления службой защиты информации.	Лекция Практическое занятие	Лекция-беседа Обсуждение подготовленных докладов, дискуссия,
8	Технология управления	Лекция	Лекция-визуализация

службой защиты информации.	Практическое занятие	Консультирование и проверка выполнения практического задания
----------------------------	----------------------	--

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

Часть 1 (7 семестр). Организационное проектирование защиты информации

Форма контроля	Максимальное количество баллов
Текущий контроль: - участие в дискуссии на семинаре - контрольная работа	50 баллов (5 баллов за каждый семинар) 10 баллов
Промежуточная аттестация (зачет)	40 баллов
Итого за семестр (дисциплину)	100 баллов

Часть 2 (8 семестр). Управление службой защиты информации

Форма контроля	Максимальное количество баллов
Текущий контроль: - участие в дискуссии на практическом занятии - доклад	50 баллов (5 баллов за каждый семинар) 10 баллов
Промежуточная аттестация (зачет с оценкой)	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	A

83 – 94		зачтено	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	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	хорошо/ зачтено	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	удовлетво- рительно/ зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	неудовлет- ворительно/ не зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

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

Часть 1 (7 семестр). Организационное проектирование защиты информации

Текущий контроль

Примерная тематика контрольных работ (проверка сформированности компетенций УК-2; ОПК-8):

- Цели и значение организационного проектирования систем.
- Виды и характеристика методов оргпроектирования систем ЗИ.
- Этапы разработки оргпроекта системы ЗИ.
- Критерии оценки эффективности оргпроекта.
- Основные этапы контроля за разработкой и внедрением оргпроекта.

Промежуточная аттестация (зачет) (проверка сформированности компетенций УК-2; ОПК-8):

Примерные контрольные вопросы к коллоквиуму:

1. Сущность и понятие оргпроектирования в области защиты информации.
2. Принципы оргпроектирования защиты информации.
3. Особенности оргпроектирования систем защиты информации.
4. Этапы процесса оргпроектирования защиты информации.
5. Отличия локального оргпроектирования от комплексного.
6. Направления оргпроектирования.
7. Основной состав требований к оргпроектированию защиты информации.
8. Методические документы, обеспечивающие процесс оргпроектирования защиты информации.
9. Методы, используемые в оргпроектировании защиты информации.
10. Диагностика объекта оргпроектирования защиты информации.
11. Методы, используемые для проведения диагностики системы защиты информации при оргпроектировании.
12. Методы сбора информации при оргпроектировании.
13. Отличия матричных методов проектирования от графических методов.
14. Понятие и состав объектов и субъектов оргпроектирования защиты информации.
15. Определение параметрической зависимости между элементами объекта и субъекта оргпроектирования.
16. Особенности иерархического построения службы ЗИ при оргпроектировании.
17. Методика расчета штатной численности подразделений службы ЗИ.
18. Порядок разработки положений о службе ЗИ и ее структурных подразделений.
19. Документационное обеспечение оргпроекта службы ЗИ.
20. Проектирование организационной и функциональной модели службы ЗИ.
21. Условия и факторы, влияющие на структурное построение службы ЗИ.
22. Особенности организационной и функциональной моделей оргпроекта системы ЗИ.
23. Основные элементы, подлежащие проектированию при разработке информационного обеспечения деятельности системы ЗИ.
24. Основные факторы, учитываемые при разработке проекта оснащения рабочих мест сотрудников ЗИ.
25. Требования к технике безопасности и пожарной безопасности при разработке проекта.
26. Особенности работы системы ЗИ в период чрезвычайных ситуаций.
27. Требования, предъявляемые к проекту функционирования системы ЗИ в период чрезвычайных ситуаций.
28. Состав оргпроекта технического оснащения системы ЗИ.
29. Особенности этапа внедрения оргпроекта на объекте.

30. Критерии оценки эффективности оргпроекта.
31. Методы оценки эффективности, используемые при оргпроектировании.
32. Контроль за разработкой и внедрением оргпроекта.
33. Разработка документации оргпроцессов при проектировании систем защиты информации.
34. Состав проектных работ и факторы, определяющие их при рационализации системы ЗИ.
35. Этапы организации процесса внедрения оргпроекта.
36. Сущность опытно – экспериментальной проверки оргпроекта.
37. Методы выявления элементов системы ЗИ, подлежащих проектированию.
38. Порядок разработки и оформления оргкарт.
39. Методы оргпроектирования, используемые при проектировании статических и динамических объектов оргпроекта.
40. Требования к проектированию организационной и функциональной модели службы ЗИ.

Часть 2 (8 семестр). Управление службой защиты информации

Текущий контроль

Примерная тематика докладов (проверка сформированности компетенций УК-2; ОПК-8):

1. Порядок и последовательность определения каналов утечки информации на предприятии.
2. Взаимосвязь и взаимодействие службы ЗИ с подразделениями предприятия.
3. Права, обязанности и ответственность сотрудников службы ЗИ.
4. Должностные характеристики руководителя службы ЗИ.
5. Планирование деятельности службы ЗИ.
6. Состав и содержание плана деятельности службы ЗИ.
7. Порядок организации текущей работы подразделений службы ЗИ.
8. Методы управления службой ЗИ.
9. Выбор стратегии управления службой ЗИ.
10. Контроль за деятельностью службы ЗИ.
11. Концепция кадровой политики службы ЗИ.

Промежуточная аттестация (зачет с оценкой)

Примерные контрольные вопросы к коллоквиуму (проверка сформированности компетенций УК-2; ОПК-8):

1. Назначение службы ЗИ на предприятии.
2. Место службы ЗИ в структуре предприятия.
3. Основные направления деятельности службы ЗИ.
4. Основные принципы организации службы ЗИ.
5. Основные требования, предъявляемые к службе ЗИ.
6. Факторы, определяющие выбор структуры службы защиты информации.
7. Цели и задачи деятельности службы ЗИ.
8. Основные этапы процесса организации службы ЗИ.
9. Основные функции службы ЗИ и ее подразделений.
10. Факторы, влияющие на организацию и функционирование службы ЗИ.
11. Типовая структура службы ЗИ.
12. Типовая структура кадрового состава службы ЗИ.
13. Квалификационные характеристики должностного состава службы ЗИ.
14. Методика расчета численности службы ЗИ и ее подразделений.
15. Организационно-правовые и нормативно-методические документы, регламентирующие деятельность службы ЗИ.

16. Ресурсное обеспечение деятельности службы ЗИ.
17. Информационные связи службы ЗИ на предприятии.
18. Основные угрозы безопасности информации на предприятии.
19. Особенности деятельности службы ЗИ во внестатных ситуациях.
20. Требования к сотрудникам службы ЗИ.
21. Влияние социально-психологических конфликтов на защищенность информации.
22. Управление конфликтами, возникающими в процессе деятельности службы ЗИ.
23. Критерии оценки эффективности работы службы ЗИ.
24. Социально-психологические факторы, влияющие на подбор и расстановку кадров в службах защиты информации.
25. Основные этапы разработки проекта службы ЗИ.
26. Структура и содержание положения о службе защиты информации.
27. Задачи, функции, права и ответственность руководителя службы защиты информации.
28. Организация рабочих мест сотрудников службы защиты информации.
29. Организация взаимодействия службы защиты информации и подразделений предприятия.
30. Технология управления службой защиты информации.
31. Административно-правовые методы управления службой ЗИ.
32. Экономические методы управления службой ЗИ.
33. Социально-психологические методы управления службой ЗИ.
34. Формы создания и способы поддержания необходимого микроклимата в коллективе службы ЗИ.
35. Формы повышения квалификации сотрудников службы ЗИ.
36. Служба защиты информации как составная часть системы защиты.
37. Служба защиты информации как орган управления защитой информации.
38. Служба защиты информации как координатор деятельности по обеспечению безопасности информации.
39. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ.
40. Основные направления совершенствования службы ЗИ.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Основные источники

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61798
2. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ http://www.consultant.ru/document/cons_doc_LAW_48699

Основная литература

3. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 186 с. - ISBN 978-5-9765-1271-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1843193>
4. Антонов, Г. Д. Стратегическое управление организацией : учебное пособие / Г.Д. Антонов, О.П. Иванова, В.М. Тумин. — Москва : ИНФРА-М, 2020. — 239 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/2861. - ISBN 978-5-16-006204-4. - Текст

: электронный. - URL: <https://znanium.com/catalog/product/1057763>

5. Баринов, В. А. Организационное проектирование : учебник / В.А. Баринов. — Москва : ИНФРА-М, 2021. — 384 с. — (Учебники для программы MBA). - ISBN 978-5-16-010992-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1222077>

6. Гришина, Н. В. Информационная безопасность предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ФОРУМ : ИНФРА-М, 2022. — 239 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-545-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1846437>

7. Организационное проектирование: реорганизация, реинжиниринг, гармонизация : учебное пособие / С.А. Лочан, Л.М. Альбитер, Ф.З. Семенова, Д.С. Петросян ; под ред. Д.С. Петросяна. — Москва : ИНФРА-М, 2021. — 196 с. — (Высшее образование: Магистратура). — www.dx.doi.org/10.12737/19670. - ISBN 978-5-16-011880-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1216467>

Дополнительная литература

8. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1036519>

9. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI [10.12737/monography_5d412ff13c0b88.75804464](https://doi.org/10.12737/monography_5d412ff13c0b88.75804464). - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1862651>

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:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

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

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

- 2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox

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, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Часть 1 (7 семестр). Организационное проектирование защиты информации

№1. Понятие, назначение, состав и характеристика оргпроектирования систем защиты информации (2 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение цели оргпроектирования, видов оргпроектирования, этапов процесса оргпроектирования.

Форма проведения занятия: выполнение практического задания.

Составить и заполнить таблицу, раскрывающую задачи и содержание конкретных видов работ, выполняемых проектантами на каждом этапе оргпроектирования.

Контрольные вопросы:

1. Что понимается под оргпроектированием?
2. В чем отличие оргпроектирования от технического проектирования?
3. В чем различие между комплексным и локальным оргпроектированием?
4. Из каких этапов состоит процесс оргпроектирования?
5. Какие работы необходимо проводить на этапе обследования объекта?
6. Из чего состоит этап разработки оргпроектирования?
7. Как осуществляется внедрение оргпроекта?

№ 2. Методы оргпроектирования систем защиты информации. Часть 1(4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение видов и характеристик методов оргпроектирования систем защиты информации и особенностей применения отдельных методов для решения различных классов задач.

Форма проведения занятия: выполнение практического задания, связанного с изучением затрат рабочего времени студента ФИСБ с помощью методов самофотографирования **Задание:** составить карту фотографии рабочего дня студента ФИСБ на выданном бланке.

Контрольные вопросы:

1. Какие методы используются при обследовании объекта оргпроектирования?

2. Каким образом осуществляется аналитико – синтетическая обработка полученных исходных данных?

Методы оргпроектирования систем защиты информации. Часть 2 (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение видов и характеристик методов оргпроектирования систем защиты информации и особенностей применения отдельных методов для решения различных классов задач.

Форма проведения занятия: выполнение практического задания, связанного с изучением затрат рабочего времени студента ФИСБ с помощью метода моментных наблюдений.

Задание: проанализировать рабочее время студента ФИСБ методом моментных наблюдений, записав результаты в таблицу; выводы представить в виде круговой или столбчатой диаграммы, отражающей распределение рабочего времени.

Контрольные вопросы:

1. Какие методы проектирования используются при разработке оргпроекта?
2. Какие методы оргпроектирования используются при проектировании статических и динамических объектов оргпроекта?

№ 3. Разработка документации оргпроцессов при проектировании систем защиты информации (2 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение особенностей разработки документации оргпроцессов при проектировании систем защиты информации, а также видов и характеристик документации.

Форма проведения занятия: выполнение практического задания.

Составить функциограмму распределения обязанностей исполнителей, работающих с конфиденциальными документами.

Контрольные вопросы:

- Какие элементы системы ЗИ подлежат проектированию?
- Какие виды документов соответствуют каждому из элементов системы ЗИ?
- Каковы основные документы, разрабатываемые на каждом этапе организационного проектирования защиты информации?

№ 4. Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно-нормативных документов, регламентирующих деятельность службы (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: развитие способности логически верно, аргументировано и ясно строить устную речь, публично представлять собственные и известные научные выводы на примере анализа методики определения (обоснования) структурного построения, расчета должностного и численного состава сотрудников службы ЗИ, а также разработки организационно – нормативных документов, регламентирующих деятельность службы ЗИ, ее подразделений и сотрудников.

Форма проведения занятия: дискуссия.

Правила проведения: дискуссия проводится после изучения материалов лекции по соответствующей теме, анализа литературы в ходе самостоятельной работы студентов с привлечением максимального числа участников — студентов группы.

Функции и схемы взаимодействия участников: студенты участвуют в устной дискуссии, помогающей раскрыть следующие вопросы:

1. Какие факторы и условия влияют на структурное построение службы ЗИ?
2. Как осуществляется проектирование организационной и функциональной модели службы ЗИ?
3. Какие существуют подходы для определения должностного состава службы ЗИ?
4. Как осуществляется расчет штатной численности службы ЗИ?
5. Каков порядок разработки положений о службе ЗИ и ее структурных подразделений?

6. Какие разделы должны быть включены в положение о службе ЗИ?
7. Какова структура и содержание штатного расписания службы ЗИ и ее подразделений?
8. Какова структура и содержание должностных инструкций сотрудников службы ЗИ?

Система оценки: см. раздел «Принципы оценки форм текущего контроля и промежуточной аттестации. Текущий контроль».

Список источников и литературы:

№ 5. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: освоение порядка выбора и распределения технических средств для оснащения рабочих мест сотрудников, изучение основных требований к проекту технического оснащения системы ЗИ, а также основных требований к охране труда, технике безопасности и пожарной безопасности.

Форма проведения занятия: выполнение практического задания.

Построить блок-схемы, отражающие взаимодействие службы защиты информации с другими подразделениями предприятия при:

- выборе оборудования и технических средств для оснащения рабочих мест сотрудников, разработке мероприятий по охране труда;
- разработке мероприятий по технике безопасности;
- разработке мероприятий по пожарной безопасности.

Контрольные вопросы:

1. Как определяются потребности использования технических средств на каждом рабочем месте?
2. Что входит в проект технического оснащения системы ЗИ?
3. Каков порядок изучения содержания труда и организации трудового процесса?
4. Какие требования предъявляются к помещениям при размещении подразделений службы ЗИ?
5. Какие требования предъявляются к технике безопасности и пожарной безопасности при разработке проекта деятельности системы ЗИ?
6. Как осуществляется охрана труда сотрудников?

№ 6. Проектирование информационного обеспечения системы защиты информации (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение цели информационного обеспечения системы ЗИ, видов, методов и средств информационного обеспечения системы ЗИ, а также основных этапов и методов проектирования информационного обеспечения системы ЗИ.

Форма проведения занятия: выполнение практического задания.

Составить проект информационного обеспечения:

- Образовательной коммерческой организации;
- Банка;
- Производственного предприятия.

Контрольные вопросы:

1. Какие существуют виды и формы информационного обеспечения системы ЗИ?
2. Каковы основные особенности информационного обеспечения системы ЗИ?
3. Как осуществляется разработка проекта информационного обеспечения системы ЗИ?

№ 7. Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах» (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: овладение навыками организации и планирования мероприятий по обеспечению функционирования системы ЗИ в «особом периоде» и в «чрезвычайных обстоятельствах».

Форма проведения занятия: выполнение практического задания.

Составить план деятельности службы защиты информации в чрезвычайных ситуациях:

- Образовательной коммерческой организации;
- Банка;
- Производственного предприятия.

Контрольные вопросы:

1. В чем заключается особенность работы системы ЗИ в «особом периоде» и в «чрезвычайных ситуациях»?
2. Какие требования предъявляются к проекту функционирования системы ЗИ в «особом периоде» и в «чрезвычайных ситуациях»?
3. Что должен включать план деятельности службы ЗИ в «особом периоде» и в «чрезвычайных ситуациях»?

№ 8. Внедрение и оценка эффективности оргпроекта (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение этапов внедрения оргпроекта и их характеристик; критериев и характеристик оценки эффективности оргпроекта.

Форма проведения занятия: выполнение практического задания, предполагающего следующие этапы работы:

1. Выделить возможные критерии оценки эффективности оргпроекта системы защиты информации.
2. Предложить методы оценки эффективности по выделенным критериям.
3. Перечислить предполагаемые результаты внедрения проекта системы защиты информации.
4. Составить таблицу, представляющую соотношение критериев, методов и результатов.

Контрольные вопросы:

1. В чем заключается сложность этапа внедрения проекта?
2. Для чего необходима опытно – экспериментальная проверка оргпроекта?
3. Как осуществляется контроль за ходом внедрения оргпроекта?
4. Какие существуют критерии оценки эффективности оргпроекта?
5. Какие методы оценки эффективности существуют?
6. В чем отличие количественных методов оценки эффективности от качественных?

Часть 2 (8 семестр). Управление службой защиты информации.

№1. Структура и штаты службы защиты информации (4 часа). (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение видов организационных структур службы защиты информации; состава подразделений, входящих в службу защиты информации; условий, влияющих на выбор организационной структуры службы защиты информации; типового должностного состава службы защиты информации; задач, функций руководителей и специалистов службы защиты информации; факторов, определяющих численность сотрудников службы защиты информации.

Форма проведения занятия: выполнение практического задания.

В качестве практического задания студентам предлагается разработать организационную структуру службы защиты информации для конкретного предприятия и определить ее должностной состав. Подробно рассматриваются вопросы зависимости должностного состава от характера выполняемых работ. В качестве раздаточного материала используются описания вариантов различных видов организационных структур и типовая структура штатов службы защиты информации.

Кроме того, студентам предлагается провести анализ различных организационных структур и определить достоинства и недостатки централизованной и децентрализованной структуры службы защиты информации.

В ходе проведения занятия внимание студентов обращается на разнообразие организационных структур службы защиты информации и ее должностного состава, а также на факторы, влияющие на определение численности сотрудников службы защиты информации.

Контрольные вопросы:

1. Какова общая структура и состав службы защиты информации?
2. Какие виды и типы организационных структур могут использоваться при организации службы защиты информации?
3. Что понимается под централизованной и децентрализованной структурой службы защиты информации?
4. Какие условия влияют на выбор организационных структур службы защиты информации?
5. Какова структура должностного состава сотрудников службы защиты информации?
6. Какие факторы влияют на определение должностного состава и численности сотрудников службы защиты информации?

№ 2. Организационные основы и принципы деятельности службы защиты информации (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение порядка создания службы защиты информации; состава и содержания нормативных документов, регламентирующих деятельность службы защиты информации; структуры и содержания положения о службе защиты информации; основных принципов организации и деятельности службы защиты информации; условий и факторов, влияющих на организацию работы службы защиты информации; порядка взаимодействия службы защиты информации с другими подразделениями предприятия и внешними службами защиты информации.

Форма проведения занятия: выполнение практического задания.

Студентам предлагается разработать структуру типового положения службы защиты информации и перечень других необходимых нормативных документов, регламентирующих деятельность службы защиты информации. Раздаточный материал методические указания по разработке типового положения и другие нормативные документы, регламентирующие деятельность службы.

Контрольные вопросы:

1. Каковы методологические принципы организации службы защиты информации?
2. Каков порядок создания службы защиты информации?
3. Какие нормативные документы регламентируют деятельность службы защиты информации?
4. Как осуществляется взаимодействие службы защиты информации с другими подразделениями предприятия?

№ 3. Подбор, расстановка и обучение сотрудников службы защиты информации (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: освоение основных положений теории кадровой политики в службе защиты информации.

Форма проведения занятия: опрос и выполнение практического задания.

Практическое занятие проводится в форме опроса студентов, обсуждаются различные методы получения информации о кандидатурах на должность, определяются их достоинства и недостатки.

Студентам предлагается разработать профессиограмму для работников службы защиты информации, а также протестировать себя на профпригодность для работы в службе защиты информации. Для выполнения задания студенты обеспечиваются необходимыми материалами.

В качестве раздаточного материала используются опросный лист профессиограммы и профориентационные тесты.

В процессе проведения занятия особое внимание обращается на методы профотбора, установления профессиональной пригодности работников службы защиты информации. Определяются требования, предъявляемые к работникам службы, при этом особо выделяются социально-психологические факторы, влияющие на работу сотрудников службы.

В ходе обсуждения внимание студентов обращается на социально-психологический климат в коллективе службы защиты информации, методы и способы решения конфликтных ситуаций и организации нормальной обстановки в службе для выполнения основных функций. Рассматриваются формы повышения квалификации сотрудников службы защиты информации. Определяются значимость и необходимость подготовки кадрового резерва службы защиты информации.

Контрольные вопросы:

1. Какие требования предъявляются к сотрудникам службы защиты информации?
2. В чем особенности подбора кадров для службы защиты информации?
3. Какие существуют методы получения информации о кандидатурах на должности в службу защиты информации?
4. Что понимается под формальными и неформальными методами сбора информации о кандидатурах на должности в службу защиты информации?
5. Какие социально-психологические факторы, влияют на подбор и расстановку кадров в службах защиты информации?
6. В чем заключаются особенности создания и поддержания необходимого микроклимата в коллективе службы защиты информации?
7. Что понимается под конфликтом в службе защиты информации?
8. Какие способы и методы управления конфликтами могут применяться в службе защиты информации?

№ 4. Организация труда сотрудников службы защиты информации (4 часа)
(проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: развитие способности логически верно, аргументировано и ясно строить устную речь, публично представлять собственные и известные научные выводы на примере анализа особенностей труда сотрудников службы защиты информации.

Форма проведения занятия: обсуждение подготовленных докладов, дискуссия по выдвинутым в ходе обсуждения вопросам; выполнение практического задания.

В качестве практического задания студентам предлагается разработать проект должностных инструкций сотрудников службы защиты информации, а также подготовить проект карты организации трудового процесса для конкретных сотрудников службы защиты информации. Раздаточным материалом служит типовая должностная инструкция и макет оргкарты.

В процессе проведения занятия особое внимание уделяется особенностям организации труда сотрудников службы защиты информации. Подробно разбираются вопросы, связанные с организацией рабочих мест сотрудников службы, охране их труда и контролю за организацией труда в службе защиты информации.

В процессе обсуждения внимание студентов обращается на культуру труда, ее значимость и необходимость в процессе выполнения сотрудниками своих должностных обязанностей.

Контрольные вопросы:

1. Чем определяются особенности труда сотрудников службы защиты информации?
2. Как осуществляется распределение обязанностей между сотрудниками службы защиты информации?
3. Что понимается под “персональной ответственностью”?

4. Как и чем обеспечивается персональная ответственность сотрудников службы защиты информации за сохранность носителей информации?
5. Какова структура и содержание должностных инструкций сотрудников службы защиты информации?
6. Каков порядок организации труда сотрудников службы защиты информации?
7. Как осуществляется организация рабочих мест сотрудников службы защиты информации?
8. Как обеспечивается охрана труда сотрудников службы защиты информации на предприятиях различных форм собственности?
9. Как осуществляется контроль за организацией труда сотрудников службы защиты информации?

№ 5. Принципы и методы управления службой защиты информации (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: освоение возможностей комплексного и системного применения методов управления службой защиты информации.

Форма проведения занятия: обсуждение подготовленных докладов, дискуссия по выдвинутым в ходе обсуждения вопросам.

В процессе занятия предполагаются выступления студентов с заранее подготовленными докладами.

В процессе проведения занятия особое внимание уделяется вопросам, связанным с системой методов управления, влияющих на эффективное функционирование службы защиты информации, а также с отдельными группами методов управления, их особенностями и возможностями применения на практике. Подробно рассматриваются вопросы комплексного применения методов управления в службе защиты информации. В ходе обсуждения вопросов внимание студентов обращается на разнообразие применяемых методов и правильность использования их в зависимости от стиля руководства, условий и целей управления.

Контрольные вопросы:

1. Какие существуют принципы управления службой защиты информации?
2. Какие существуют методы управления?
3. Что входит в состав административно-правовых методов управления?
4. Какие экономические методы могут применяться при управлении службой защиты информации?
5. В чем особенности применения социально-психологических методов управления?
6. Что понимается под комплексным и системным применением методов управления службой защиты информации?

№ 6. Технология управления службой защиты информации (4 часа) (проверка сформированности компетенций УК-2; ОПК-8).

Цель занятия: изучение критериев эффективности и методы оценки качества работы службы защиты информации, а также освоение путей и способов повышения эффективности управления службой защиты информации.

Форма проведения занятия: выполнение практического задания.

В качестве задания студентам предлагается разработать проект плана работы службы защиты информации и структурировать технологический процесс управления службой защиты информации. Раздаточным материалом служит типовая проект плана и схема структуризации процессов управления.

Контрольные вопросы:

1. Назвать функции управления службой защиты информации;
2. Проанализировать технологию принятия управленческих решений;
3. Изучить технологию управления службой защиты информации;
4. Изучить структуру и содержание плана работы службы защиты информации;

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Комплексное обеспечение безопасности объекта информатизации» реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Целью курса является формирование представлений о теоретических и методологических основах организационного проектирования, порядка построения, оценки и совершенствования систем защиты информации предприятия и служб защиты информации

Задачи: рассмотрение сущности и задач организационного проектирования систем защиты информации и служб защиты информации, методов исследования, принципов организации проектирования и этапов разработки проекта, технологию организации и служб защиты информации.

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:

УК-2.1: анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач

УК-2.2: способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения

- УК – 9 – Способен использовать базовые дефектологические знания в социальной и профессиональной сферах

УК-9.1. Понимает содержание инклюзивной компетентности, ее компоненты и структуру

УК-9.2. Знает особенности применения базовых дефектологических знаний в социальной и профессиональной сферах

- ОПК-8: способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности:

ОПК-8.1: знает принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией

ОПК-8.2: умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами

ОПК-8.3: владеет навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов.

В результате освоения дисциплины обучающийся должен:

Знать методы, технологию и принципы проектирования систем защиты информации и служб защиты информации;

Уметь проводить предпроектное обследование, проводить анализ экономической целесообразности проектирования систем защиты информации и служб защиты информации; разрабатывать документы, необходимые для внедрения и функционирования системы защиты информации и служб защиты информации.

Владеть методикой определения структурного построения и состава системы защиты информации и служб защиты информации, а также разработкой организационно-нормативных документов, регламентирующих их.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта (7 семестр), зачёта с оценкой (8 семестр).

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц.