Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2023 13:58:13
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.О.03.26 «ПРОЕКТИРОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ»

Направление подготовки:
10.03.01 «Информационная безопасность»

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

Квалификация выпускника: **бакалавр**

Тольятти 2023

Рабочая программа дисциплины «Проектирование комплексных систем безопасности» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Составители:

К.п.н., доцент	Сыротюк С.Д.
Старший преподаватель	Мунирова Ю.С.
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

«11» 10 2023 г., протокол № 3

Директор ВШИСиКТ	к.э.н., доцент	Филиппова О.А.
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование у обучающихся способности разрабатывать политику информационной безопасности и планировать согласованный комплекс организационных и технических мер на объекте защиты.

- формирование у обучающихся способности подготавливать исходные данные, формулировать требования к подсистемам безопасности и обосновывать проектные решения с учетом угроз, ресурсов и эксплуатационных ограничений.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	Основание (ПС) *для профессиональных компетенций
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики. ИОПК-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности. ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности.	**Знает:** принципы комплексной защиты, содержание политики информационной безопасности, взаимосвязь организационных, физических и технических мер. **Умеет:** разрабатывать политику безопасности, распределять ответственность, планировать внедрение и сопровождение комплекса защитных мер. **Владеет:** навыками составления политики безопасности, матрицы ответственности и плана реализации и контроля защитных мер.	—
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИОПК-12.1. Знает порядок проектирования подсистем, средств обеспечения защиты информации. ИОПК-12.2. Формулирует требования и характеристики подсистем и средств обеспечения защиты информации для их последующего проектирования. ИОПК-12.3. Осуществляет подготовку исходных данных для технико-экономического обоснования проектных решений.	**Знает:** этапы проектирования, состав исходных данных, требования к подсистемам безопасности и способы технико-экономического обоснования решений. **Умеет:** проводить обследование объекта, формировать модель угроз, требования и техническое задание, сравнивать проектные варианты. **Владеет:** навыками подготовки проектных исходных данных, схем архитектуры, спецификаций и расчетов затрат на комплексную систему безопасности.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» образовательной программы (Б1.О.03 Общепрофессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **6 з.е. (216 час.)** их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**216**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**100/66**
занятия лекционного типа (лекции)	40/24
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	44/32
лабораторные работы	16/10
Самостоятельная работа всего, в т.ч.:	**89/141**
Самоподготовка по темам (разделам) дисциплины	89/141
Выполнение курсового проекта	36 / 36
Контроль (часы на экзамен, зачет)	**27/9**
Промежуточная аттестация	**Экзамен; защита КП**

Примечание: 216/216 объем часов соответственно для очной, очно-заочной форм обучения

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 1. ОБСЛЕДОВАНИЕ ОБЪЕКТА И ИСХОДНЫЕ ДАННЫЕ ДЛЯ ПРОЕКТИРОВАНИЯ** Содержание лекции: Понятие комплексной системы безопасности. Границы объекта, активы, процессы и потоки данных. Обследование помещений и информационной инфраструктуры. Категории информации и исходные ограничения. Оформление результатов обследования.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №1. Исследование потоков данных и границ учебного стенда.		2/1			Отчет по лабораторной работе
	Практическая работа №1. Обследование учебного объекта и составление перечня активов.			4/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				6/10	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 2. МОДЕЛЬ УГРОЗ И ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ** Содержание лекции: Источники угроз и модель нарушителя. Уязвимости, последствия и сценарии реализации угроз. Качественная оценка вероятности и ущерба. Приоритеты обработки рисков. Связь угроз с требованиями к защите.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №2. Проверка сценариев угроз на модели объекта.		2/1			Отчет по лабораторной работе
	Практическая работа №2. Разработка модели угроз и реестра рисков.			4/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				6/11	Самостоятельное изучение учебных материалов

ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 3. ПОЛИТИКА БЕЗОПАСНОСТИ И ТРЕБОВАНИЯ К КОМПЛЕКСНОЙ СИСТЕМЕ** Содержание лекции: Цели и принципы политики безопасности. Роли, полномочия и ответственность. Правила доступа, управления изменениями и реагирования. Функциональные и эксплуатационные требования. Состав технического задания и критерии приемки.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №3. Проверка ролевой модели доступа.		2/1			Отчет по лабораторной работе
	Практическая работа №3. Разработка политики безопасности и технического задания.			6/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				6/11	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 4. АРХИТЕКТУРА КОМПЛЕКСНОЙ СИСТЕМЫ И ИНТЕГРАЦИЯ ПОДСИСТЕМ** Содержание лекции: Многоуровневая защита и зоны безопасности. Подсистемы физической, технической и информационной защиты. Интерфейсы, совместимость и обмен событиями. Централизованное управление. Резервирование и предотвращение общих точек отказа.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №4. Исследование взаимодействия подсистем защиты.		2/1			Отчет по лабораторной работе
	Практическая работа №4. Разработка архитектуры комплексной системы безопасности.			6/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				7/12	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 5. ПРОЕКТИРОВАНИЕ ФИЗИЧЕСКОЙ И ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ** Содержание лекции: Зонирование территории и помещений. Контроль и управление физическим доступом, охранная сигнализация и видеонаблюдение. Защита от утечки по техническим каналам. Электропитание и климатические условия. Согласование физических мер с режимом объекта.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №5. Моделирование событий физического доступа.		2/1			Отчет по лабораторной работе
	Практическая работа №5. Проектирование физической и инженерно-технической защиты объекта.			6/4		Отчет по практической работе

	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				7/12	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 6. ПРОЕКТИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ** Содержание лекции: Сегментация сети и защищенное взаимодействие. Управление учетными записями и правами. Защита рабочих станций, серверов и данных. Резервное копирование. Журналирование и мониторинг. Выбор средств с учетом требований, совместимости и сертифицированной конфигурации.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №6. Проверка сегментации и резервного восстановления.		2/1			Отчет по лабораторной работе
	Практическая работа №6. Проектирование защиты информационной инфраструктуры.			6/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				7/12	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 7. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ И ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ** Содержание лекции: Сравнение вариантов проекта по затратам, эффективности и ограничениям. Единовременные и эксплуатационные расходы. Подготовка спецификаций, схем, ведомостей и пояснительной записки. Прослеживаемость требований и проектных решений.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос
	Лабораторная работа №7. Расчет затрат и анализ чувствительности проектного решения.		2/2			Отчет по лабораторной работе
	Практическая работа №7. Сравнение вариантов проекта и подготовка спецификации.			6/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				7/12	Самостоятельное изучение учебных материалов
ОПК-10 ИОПК-10.1 ИОПК-10.2 ИОПК-10.3 ОПК-12 ИОПК-12.1 ИОПК-12.2 ИОПК-12.3	**ТЕМА 8. ВНЕДРЕНИЕ, ИСПЫТАНИЯ И СОПРОВОЖДЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ** Содержание лекции: План внедрения и управление изменениями. Предварительные и приемочные испытания. Проверка взаимодействия подсистем и восстановления после отказов. Регламенты эксплуатации, мониторинг показателей и пересмотр рисков. Подготовка защиты курсовой работы.	5/3				Лекция-визуализация (в т.ч. в ЭИОС) Тематический опрос

	Лабораторная работа №8. Комплексная проверка защитных функций учебного стенда.		2/2			Отчет по лабораторной работе
	Практическая работа №8. Разработка плана внедрения и программы приемочных испытаний.			6/4		Отчет по практической работе
	Самостоятельная работа. Изучение учебных материалов и подготовка к занятиям.				7/13	Самостоятельное изучение учебных материалов
	Курсовая работа. Проект комплексной системы безопасности учебного объекта.				36/48	Пояснительная записка и защита курсовой работы
	ИТОГО	**40/24**	**16/10**	**44/32**	**89/141**	

Примечание: 216/216 объем часов соответственно для очной, очно-заочной форм обучения

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

– качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;

– качество оформления отчета по работе;

– качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Курсовая работа выполняется по индивидуальному заданию. Рекомендуется последовательно подготовить результаты обследования, модель угроз, политику и требования, архитектуру и спецификацию, расчет затрат и программу испытаний. Промежуточные результаты обсуждаются на консультациях; готовая работа представляется и защищается отдельно от экзамена.

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по очно-заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

4.6. Методические указания для выполнения курсового проекта / работы

Выполнение курсового проекта/ работы способствует лучшему освоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся готовности к самостоятельной профессиональной деятельности, является этапом к выполнению выпускной квалификационной работы.

Примерная тематика курсовых работ (проектов)

1. Проектирование комплексной системы безопасности офисного здания.
2. Проектирование комплексной системы безопасности банковского учреждения.
3. Проектирование комплексной системы безопасности объекта образования.
4. Проектирование комплексной системы безопасности промышленного предприятия.
5. Проектирование комплексной системы безопасности складского комплекса.
6. Проектирование подсистемы контроля и управления доступом для многофункционального центра.
7. Проектирование подсистемы видеонаблюдения для торгового центра.
8. Проектирование интегрированной системы безопасности объекта критической информационной инфраструктуры.
9. Проектирование комплексной системы безопасности объекта транспортной инфраструктуры.
10. Проектирование комплексной системы безопасности жилого комплекса

- Цели и задачи курсового проектирования
- Выбор темы курсового проектирования
- Организация, выполнение и руководство курсовым проектированием
- Структура и содержание курсового проекта / работы.

Методические указания по выполнению основных разделов

- Требования к оформлению курсового проекта / работы
- Порядок сдачи и защиты курсового проекта / работы

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Коваленко, В. В. Проектирование информационных систем : учеб. пособие для студентов (бакалавров и специалистов) вузов и магистров по направлению 09.03.03 "Приклад. информатика" (профиль "Приклад. информатика в экономике") / В. В. Коваленко. – 2-е изд., перераб. и доп. – Документ read. – Москва : ФОРУМ [и др.], 2023. – 357 с. : ил., табл. – (Высшее образование. Бакалавриат). – Прил. – URL: https://znanium.ru/read?id=415461 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-00091-637-7. - 978-5-16-107012-3. – Текст : электронный.

2. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00.

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ read. - Москва : ФОРУМ [и др.], 2022. - 592 с. : ил. - (Высшее образование - Бакалавриат) (Высшее образование - Бакалавриат). - Предм. указ. - URL: https://znanium.ru/read?id=389857 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8199-0730-6. - 978-5-16-106148-0. - Текст : электронный. - Текст : электронный.

4. Шейдаков, Н. Е. Физические основы защиты информации : учеб. пособие для студентов вузов по направлению подгот. "Информ. безопасность" / Н. Е. Шейдаков, О. В. Серпенинов, Е. Н. Тищенко ; Ростов. гос. эконом. ун-т (РИНХ). – Документ read. – Москва : Риор [и др.], 2022. – 204 с. – (Высшее образование). – URL: https://znanium.com/read?id=389741 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-369-01603-9. - 978-5-16-105331-7. – Текст : электронный.

Дополнительная литература

5. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учеб. пособие / Т. В. Гвоздева, Б. А. Баллод. – Изд. 2-е, стер. – Документ Reader. – Санкт-Петербург [и др.] : Лань, 2021. – 250 с. – (Учебники для вузов. Специальная литература). – Прил. – URL: https://reader.lanbook.com/book/169810 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-8114-7963-4. – Текст : электронный.

6. Зайцев, А. П. Технические средства и методы защиты информации : учеб. для вузов по группе специальностей "Информ. безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов ; под ред. А. П. Зайцева и А. А. Шелупанова. - 7-е изд. - Москва : Горячая линия -Телеком, 2020. - 442 с. : ил. - Прил. - ISBN 978-5-9912-0233-6 : 577-72. - Текст : непосредственный.

7. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. – 3-е изд. – Документ read. – Москва : РИОР [и др.], 2024. – 400 с. – (Высшее образование). – URL:

https://znanium.ru/read?id=443251 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-369-01759-3. - 978-5-16-106478-8. – Текст : электронный.

8. Коноплева, И. А. Управление безопасностью и безопасность бизнеса : учеб. пособие для вузов по специальности "Приклад. информатика (по обл.)" / И. А. Коноплева, И. А. Богданов. – Документ read. – Москва : ИНФРА-М, 2020. – 447 с. : табл. – (Высшее образование). – Глоссарий. – URL: https://znanium.com/read?id=354808 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-16-003230-6. – Текст : электронный.

9. Малюк, А. А. Теория защиты информации / А. А. Малюк. – Москва : Горячая линия - Телеком, 2013. – 184 с. : табл. – ISBN 978-5-9912-0246-6 : 448-10. – Текст : непосредственный.

10. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности : учеб. пособие для вузов по направлению "Информац. системы и технологии" / Ю. Ф. Мартемьянов, Яковлев, Ал. В., Яковлев, Ан. В. – 2-е изд., стер. – Москва : Горячая линия -Телеком, 2020. – 332 с. : ил. – ISBN 978-5-9912-0677-8 : 455-51. – Текст : непосредственный.

11. Партыка, Т. Л. Информационная безопасность : учеб. пособие для сред. проф. образования по специальностям информатики и вычисл. техники / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – Документ read. – Москва : ФОРУМ [и др.], 2021. – 432 с. : ил. – (Среднее профессиональное образование). – Глоссарий. – URL: https://znanium.ru/read?id=364624 (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-16-101302-1. – Текст : электронный.

12. Янка, Т. Безопасность WEB-приложений. Исчерпывающий гид для начинающих разработчиков / Т. Янка ; [пер. с англ. М. А. Райтмана]. - Москва : Эксмо, 2023. - 462 с. : ил. - (КиберБез. Лучшие книги о безопасности в сетях). - ISBN 978-5-04-171803-9 : 544-00. - Текст : непосредственный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU : Электронное периодическое издание : сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 09.11.2023). – Текст: электронный.

2. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 09.11.2023). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

3. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 09.11.2023). - Текст : электронный.

4. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 09.11.2023). - Текст : электронный.

5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Текстовый и табличный редакторы учебной аудитории	в соответствии с условиями использования установленного программного обеспечения
3	Oracle VM VirtualBox (для изолированного учебного стенда)	свободно распространяемое программное обеспечение
4	СДО MOODLE	через электронную информационно-образовательную среду университета

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Экзамен / Защита КП	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество	Баллы за единицу	Максимум баллов
Активность и тематический контроль на лекциях	8	1	8
Лабораторные работы	8	3	24
Практические работы	8	6	48
Самостоятельная работа / рубежный опрос	4	5	20
ИТОГО			100 баллов

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа №1. Обследование учебного объекта и составление перечня активов.

Задание 1. Описать учебную организацию, ее процессы, помещения и информационную инфраструктуру.

Задание 2. Составить перечень активов, их владельцев и требований к конфиденциальности, целостности и доступности.

Задание 3. Построить схему потоков данных и отметить границы объекта защиты.

Задание 4. Зафиксировать условия эксплуатации, имеющиеся средства и ресурсные ограничения.

Задание 5. Оформить акт обследования и перечень исходных данных для проектирования.

Практическая работа №2. Разработка модели угроз и реестра рисков.

Задание 1. Определить внешних и внутренних нарушителей и их возможности.

Задание 2. Составить сценарии угроз для активов, выделенных в работе №1.

Задание 3. Оценить вероятность и ущерб по заданной качественной шкале и ранжировать риски.

Задание 4. Определить способы обработки рисков и требования к защитным мерам.

Задание 5. Оформить реестр рисков с указанием оснований оценки и остаточного риска.

Практическая работа №3. Разработка политики безопасности и технического задания.

Задание 1. Определить цели политики безопасности и область ее действия.

Задание 2. Назначить роли владельцев ресурсов, администраторов, пользователей и ответственных за контроль.

Задание 3. Разработать правила доступа, управления изменениями и реагирования на инциденты.

Задание 4. Сформулировать измеримые требования к комплексной системе и условия приемки.

Задание 5. Оформить политику безопасности и проект технического задания.

Практическая работа №4. Разработка архитектуры комплексной системы безопасности.

Задание 1. Выделить зоны доверия и основные подсистемы безопасности.

Задание 2. Построить структурную схему системы и определить интерфейсы взаимодействия.

Задание 3. Распределить защитные функции между подсистемами без необоснованного дублирования.

Задание 4. Предусмотреть резервирование, управление и сбор событий безопасности.

Задание 5. Составить матрицу соответствия «угроза — требование — подсистема — проверка».

Практическая работа №5. Проектирование физической и инженерно-технической защиты объекта.

Задание 1. Нанести на план учебного объекта защищаемые зоны, точки прохода и размещение оборудования.

Задание 2. Определить функции контроля доступа, сигнализации и видеонаблюдения.

Задание 3. Выбрать меры защиты от выявленных технических каналов утечки.

Задание 4. Предусмотреть требования к электропитанию, размещению и обслуживанию оборудования.

Задание 5. Подготовить схему размещения и обоснование согласованности физических и информационных мер.

Практическая работа №6. Проектирование защиты информационной инфраструктуры.

Задание 1. Разработать схему сегментации сети и разрешенных межсегментных взаимодействий.

Задание 2. Составить матрицу ролей и доступа к информационным ресурсам.

Задание 3. Определить меры защиты конечных узлов, серверов и каналов связи.

Задание 4. Разработать требования к резервному копированию, журналированию и мониторингу.

Задание 5. Оформить функциональную схему и требования к совместимости выбранных средств.

Практическая работа №7. Сравнение вариантов проекта и подготовка спецификации.

Задание 1. Сформировать два реализуемых варианта комплексной системы для одного объекта.

Задание 2. Подготовить спецификации оборудования, программных средств и работ.

Задание 3. Рассчитать капитальные и эксплуатационные затраты по заданным исходным ценам.

Задание 4. Сравнить варианты по покрытию угроз, затратам, надежности и ограничениям.

Задание 5. Обосновать выбор и оформить расчет, спецификацию и перечень проектных документов.

Практическая работа №8. Разработка плана внедрения и программы приемочных испытаний.

Задание 1. Разработать этапы внедрения, роли исполнителей и порядок согласования изменений.

Задание 2. Сформировать перечень приемочных проверок по требованиям технического задания.

Задание 3. Определить исходные условия, тестовые воздействия и ожидаемые результаты.

Задание 4. Предусмотреть проверку отказов и восстановление работоспособности.

Задание 5. Оформить план внедрения, программу испытаний и форму протокола приемки.

8.2.2. Типовые задания для лабораторных работ

Лабораторная работа №1. Исследование потоков данных и границ учебного стенда.

Цель работы: исследовать исходные данные и проверить границы объекта защиты.

Задание 1. Подготовить схему и таблицу узлов учебного стенда по заданным исходным данным.

Задание 2. Зафиксировать штатные потоки данных и разрешенные взаимодействия.

Задание 3. Проверить доступность выбранных локальных ресурсов штатными средствами системы.

Задание 4. Сопоставить наблюдаемые взаимодействия с исходной схемой и выявить расхождения.

Задание 5. Оформить протокол исследования и уточнить границы защиты.

Лабораторная работа №2. Проверка сценариев угроз на модели объекта.

Цель работы: проверить реализацию выбранных сценариев и действие компенсирующих мер.

Задание 1. Выбрать два сценария угроз из разработанной модели.

Задание 2. Задать исходные условия и ожидаемые последствия в изолированной учебной модели.

Задание 3. Воспроизвести ошибочное разрешение доступа либо изменение тестового файла.

Задание 4. Сопоставить последствия до и после введения выбранной меры защиты.

Задание 5. Оформить результаты и ограничения проведенной проверки.

Лабораторная работа №3. Проверка ролевой модели доступа.

Цель работы: проверить соответствие фактического доступа заданной ролевой модели.

Задание 1. Создать тестовые ресурсы и учетные записи либо использовать подготовленный стенд.

Задание 2. Настроить права доступа по заданной матрице ролей.

Задание 3. Проверить разрешенные и запрещенные операции для каждой роли.

Задание 4. Зафиксировать отклонения и скорректировать настройки.

Задание 5. Оформить протокол соответствия фактических прав проектной матрице.

Лабораторная работа №4. Исследование взаимодействия подсистем защиты.

Цель работы: оценить согласованность взаимодействия подсистем и регистрацию событий.

Задание 1. Определить события и интерфейсы обмена между двумя учебными подсистемами.

Задание 2. Подготовить набор штатных и ошибочных событий.

Задание 3. Проверить передачу событий и согласованность времени в журналах либо их модели.

Задание 4. Воспроизвести потерю связи и оценить предусмотренную реакцию.

Задание 5. Оформить таблицу взаимодействий и перечень выявленных ограничений.

Лабораторная работа №5. Моделирование событий физического доступа.

Цель работы: исследовать модель физического доступа и реакции на нарушения правил.

Задание 1. Построить модель точек прохода и уровней допуска сотрудников.

Задание 2. Задать расписания доступа и события отказа идентификатора.

Задание 3. Воспроизвести разрешенный проход, отказ в доступе и попытку входа вне расписания.

Задание 4. Проверить фиксацию событий и передачу тревожного сообщения в модели.

Задание 5. Составить протокол и рекомендации по корректировке правил доступа.

Лабораторная работа №6. Проверка сегментации и резервного восстановления.

Цель работы: проверить изоляцию взаимодействий и восстановление тестовых данных.

Задание 1. Подготовить изолированную схему учебных сегментов или модель правил фильтрации.

Задание 2. Проверить разрешенные и запрещенные соединения.

Задание 3. Создать резервную копию тестовых данных и зафиксировать контрольные значения.

Задание 4. Восстановить данные после учебного сбоя и проверить их целостность.

Задание 5. Оформить протокол доступности, изоляции и восстановления.

Лабораторная работа №7. Расчет затрат и анализ чувствительности проектного решения.

Цель работы: получить навыки расчета затрат и проверки устойчивости проектного выбора.

Задание 1. Внести исходные стоимости и сроки службы компонентов в электронную таблицу.

Задание 2. Рассчитать суммарные затраты двух вариантов за заданный период.

Задание 3. Изменить стоимость сопровождения и число рабочих мест в заданных пределах.

Задание 4. Оценить изменение итоговых затрат и устойчивость выбранного варианта.

Задание 5. Оформить расчетную таблицу, исходные допущения и выводы.

Лабораторная работа №8. Комплексная проверка защитных функций учебного стенда.

Цель работы: проверить совокупность защитных функций по программе испытаний.

Задание 1. Зафиксировать исходную конфигурацию стенда и программу проверок.

Задание 2. Выполнить проверки доступа, регистрации событий и резервного восстановления.

Задание 3. Воспроизвести отказ одной учебной подсистемы и проверить компенсирующие меры.

Задание 4. Сопоставить результаты с критериями приемки и устранить обнаруженные отклонения.

Задание 5. Оформить итоговый протокол с выводом о выполнении проверенных требований.

8.2. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *экзамен / защита курсового проекта (курсовой работы) (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Защита курсового проекта/ работы. *Результаты защиты курсового проекта/ работы выставляются по пятибалльной системе оценивания ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно") с обязательным проставлением количества баллов, набранных в соответствии с балльно-рейтинговой системой (по стобалльной шкале).*

Типовые темы курсовых проектов

Курсовой проект предполагает разработку проектных решений комплексной системы

безопасности для конкретного типа объекта защиты. Примерные темы курсовых проектов:

1. Проектирование комплексной системы безопасности офисного здания.
2. Проектирование комплексной системы безопасности банковского учреждения.
3. Проектирование комплексной системы безопасности объекта образования.
4. Проектирование комплексной системы безопасности промышленного предприятия.
5. Проектирование комплексной системы безопасности складского комплекса.
6. Проектирование подсистемы контроля и управления доступом для

многофункционального центра.

7. Проектирование подсистемы видеонаблюдения для торгового центра.
8. Проектирование интегрированной системы безопасности объекта критической

информационной инфраструктуры.

9.Проектирование комплексной системы безопасности объекта транспортной инфраструктуры.

10. Проектирование комплексной системы безопасности жилого комплекса.

Перечень вопросов и заданий для подготовки к экзамену

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

1. Понятие комплексной системы безопасности и взаимосвязь ее подсистем.
2. Цели и область действия политики информационной безопасности.
3. Принципы многоуровневой защиты и минимальных привилегий.
4. Распределение ролей, полномочий и ответственности за безопасность.
5. Управление физическим доступом и доступом к информационным ресурсам.

6. Согласование организационных и технических мер защиты.
7. Планирование внедрения комплекса защитных мер.
8. Управление изменениями конфигурации системы безопасности.
9. Организация регистрации и анализа событий безопасности.
10. Взаимодействие подсистем контроля доступа, сигнализации и мониторинга.
11. Организация резервного копирования и восстановления.
12. Планирование действий при отказе защитной подсистемы.
13. Показатели выполнения и эффективности защитных мер.
14. Порядок пересмотра политики безопасности и реестра рисков.
15. Регламенты эксплуатации и обслуживания комплекса.
16. Критерии приемки и документирование результатов испытаний.
17. Остаточный риск и порядок согласования его принятия.
18. Обоснование выбора мер с учетом условий эксплуатации.
19. Требования к совместимости подсистем и средств защиты.
20. Прослеживаемость угроз, требований, мер и контрольных процедур.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

1. Этапы проектирования комплексной системы безопасности.
2. Обследование объекта и состав исходных данных.
3. Инвентаризация и классификация активов.
4. Построение схем потоков данных и границ доверия.
5. Разработка модели нарушителя и модели угроз.
6. Качественная оценка вероятности, ущерба и приоритетов риска.
7. Функциональные и эксплуатационные требования к системе.
8. Состав технического задания на комплексную систему.
9. Зонирование территории, помещений и информационной инфраструктуры.
10. Выбор архитектуры и интерфейсов взаимодействия подсистем.
11. Подготовка исходных данных для выбора физических мер защиты.
12. Подготовка исходных данных для защиты от технических каналов утечки.
13. Подготовка исходных данных для сегментации сети и управления доступом.
14. Выбор показателей надежности и восстановления.
15. Состав спецификации оборудования, программных средств и работ.
16. Единовременные и эксплуатационные затраты проектного решения.
17. Методы сравнения альтернативных вариантов проекта.
18. Анализ чувствительности затрат к изменению исходных данных.
19. Состав проектной и эксплуатационной документации.
20. Порядок обоснования решений и защиты курсовой работы.