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 комплексной защиты информации

ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
Рабочая программа дисциплины

Составитель:
Кандидат военных наук, доцент. кафедры КЗИ Д.Н. Баранников

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование основных знаний и умений в области технологий проектирования защищенных автоматизированных систем и соответствующими общепрофессиональными компетенциями в соответствии с ООП.
Задачи дисциплины:
– формирование знаний в области технических средств контроля мер защиты информации в автоматизированных системах (АС);
– уяснение основных понятий и определений, позволяющих осуществлять выбор и технических средств защиты;
– Рассмотреть особенности контроля эффективности мер защиты с помощью технических средств, а также методов, используемых при проведении контроля.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	Знать: • оценки работоспособности применяемых средств защиты информации в АС с использованием штатных средств и методик.
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	Уметь: • оценить эффективности применяемых средств защиты информации в АС с использованием штатных средств и методик
	ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации	Владеть: • навыками определения уровня защищённости и доверия средств защиты информации АС.
ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК-4.1 Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Знать: • методы и способы обеспечения отказоустойчивости АС; • содержание и порядок деятельности персонала по эксплуатации защищенных АС и подсистем безопасности АС
	ПК-4.2 Умеет применять типовые программные средства резер-	Уметь: • применять типовые программные средства ре-

	вирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах	зервирования и восстановления информации, средства обеспечения отказоустойчивости в АС
	ПК-4.3 Владеет навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций	Владеть: • навыками обнаружения, устранения неисправностей в работе системы защиты информации АС; • резервирования программного обеспечения, технических средств, каналов передачи данных АС управления на случай возникновения нештатных ситуаций

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технические средства контроля эффективности мер защиты информации в автоматизированных системах» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Операционные системы».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексная защита объектов информатизации», «Безопасность вычислительных сетей», «Безопасность систем баз данных».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _2_ з.е., 72 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
5	Лекции	**16**
5	Практические работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _32_ академических часа.

3. Содержание дисциплины

Тема 1. Методы и средства технической разведки

Деятельность государств по добыванию с помощью технических средств добывать сведения. Устройства и технологии, позволяющие получать сведения технического характера. Принципы организации и ведения технической разведки. Классификация технической разведки. Способы перехвата.

Тема 2. Первоочередные мероприятия по обеспечению информационной безопасности и контроль эффективности системы защиты, и рассмотрение требований к защите информации.

Определение объектов защиты. Классификация объектов защиты. Система мер, рекомендуемая для большинства компаний. Организационные меры. Установка градации сотрудников и их уровней доступа к информации. Обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты. Обеспечение защиты информации при управлении доступом. Предотвращение утечек информации. Управление инцидентами информационной безопасности. Требования к защите информации.

Тема 3. Методы контроля эффективности мер защиты информации в автоматизированных система

Проверка соответствия. Оценка возможностей. Анализ разрешенных и запрещенных связей. Проведение оценки соответствия. Требования к средствам контроля защищенности информации. Автоматизированный контроль. Система контроля. Документирование результатов контроля.

Тема 4. Средства оперативного контроля и регистрации событий безопасности

Средства разграничения и контроля целостности. Средства объективного контроля. оперативного ознакомления администратора безопасности. Подключение к файловому серверу. Запуск и завершение программы. Измерение. Регистрация. Получение первичной информации.

Тема 5. Средства контроля эффективности мер защиты от утечки по техническим каналам

Технические мероприятия. Активные технические средства защиты информации. Пассивные технические средства защиты информации. Контроль и ограничение доступа к ИС и в выделенные помещения с помощью технических средств и систем. Экранирование ОТСС и их соединительных линий. Установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны. Установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны. Установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещений помехоподавляющих фильтров.

Тема 6. Проектирование системы защиты от НСД

Классификация мер и средств защиты. Меры по идентификации и аутентификации. Общие сведения о проектировании СЗИ. Стадии проектирования и основные подходы к встраиванию СЗИ. Принципы и методы построения защищённых АС. Место и роль спецификации при проектировании СЗИ. Разработка технического проекта. Разработка рабочей документации. Подготовка и оформление технической документации. Разработка порядка сопровождения. Разработка порядка и этапов внедрения СЗИ.

Тема 7. Автоматизированная система оценки защищенности технических средств от утечки информации по каналу ПЭМИН "Сигурд"

Назначение и состав. Программная оболочка. Достоинства и недостатки. Основные технические характеристики. Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки. Схема измерений ПЭМИН. Принцип проведения исследований. Отличительные особенности от других систем. Действия персонала при проведении исследований. Оценка результатов.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Общая характеристика процесса проектирования защищенных автоматизированных систем	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Подготовка к занятиям с использованием ЭБС
2	Исходные данные для проектирования.	Лекция 2. Практическое занятие 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
3	Организационные процессы создания автоматизированных систем	Лекция 3. Практическое занятие 2. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
4	Модели жизненного цикла автоматизированных систем	Лекция 4. Практическое занятие 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
5	Особенности проектирования комплексной системы информационной безопасности	Лекция 5. Практическое занятие 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
6	Проектирование системы защиты от НСД	Лекция 6. Практическое занятие 5.	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО

		Самостоятельная работа	Опрос, тест Подготовка к занятиям с использованием ЭБС
7	Аттестация автоматизированной системы по требованиям безопасности	Лекция 7. Практическое занятие 6. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использованием ЭБС

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

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

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

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
– опрос (темы 1-3)	*4 балла*	*12 баллов*
– тест (темы 4-7)	*3 балла*	*12 баллов*
– практическое занятие (темы 1-6)	*6 баллов*	*36 баллов*
Промежуточная аттестация – зачёт (зачет по билетам)		*40 баллов*
Итого за семестр		100 баллов

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

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E

20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Виды несанкционированного доступа в информационную систему. Способы противодействия	ПК-6; ПК-4
2.	Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т. п.).	ПК-6; ПК-4
3.	Примеры реализации угроз информационной безопасности	ПК-6; ПК-4
4.	Причины, виды и каналы утечки информации.	ПК-6; ПК-4
5.	Разработка и реализация политики безопасности для защиты информации.	ПК-6; ПК-4
6.	Основные типы политики безопасности для управления доступом к данным: дискреционная и мандатная политика безопасности.	ПК-6; ПК-4
7.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	ПК-6; ПК-4
8.	Подтверждение подлинности объектов и субъектов информационной системы.	ПК-6; ПК-4
9.	Парольные схемы аутентификации.	ПК-6; ПК-4
10.	Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита	ПК-6; ПК-4
11.	Разрабатываемые организационно-распорядительные документы должны определять	ПК-6; ПК-4
12.	Предварительные испытания и опытная эксплуатация	ПК-6; ПК-4
13.	Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы.	ПК-6; ПК-4
14.	Вирусы, троянские программы. Антивирусное программное обеспечение	ПК-6; ПК-4
15.	Требования к качеству готового продукта. Оснащенность технологического процесса необходимыми средствами контроля параметров.	ПК-6; ПК-4
16.	Роль стандартов информационной безопасности. Основное содержание стандартов.	ПК-6; ПК-4
17.	Классы защищенности компьютерных систем	ПК-6; ПК-4
18.	Каналы несанкционированного доступа. Типовые причины возникновения.	ПК-6; ПК-4
19.	Показатели защищенности средств вычислительной техники от несанкционированного доступа.	ПК-6; ПК-4
20.	Место информационной безопасности в национальной безопасности	ПК-6; ПК-4

	страны.	
21.	Информация как предмет защиты. Критерии секретной и конфиденциальной информации	ПК-6; ПК-4
22.	Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах	ПК-6; ПК-4
23.	Процедурный уровень информационной безопасности. Классы мер процедурного уровня	ПК-6; ПК-4
24.	Классификация защищаемой информации по принадлежности, содержанию и степени секретности	ПК-6; ПК-4
25.	Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну	ПК-6; ПК-4
26.	Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники	ПК-6; ПК-4
27.	Организация защиты конфиденциальной информации от утечки по техническим каналам	ПК-6; ПК-4
28.	Методы защиты информации: скрытие, ранжирование, дезинформация, дробление	ПК-6; ПК-4

Промежуточная аттестация (примерные вопросы к экзамену) – проверка сформированности компетенций – ПК-6; ПК-4

№	Вопрос	Реализуемая компетенция
1.	Какие основные криптографические протоколы используются в сетях	ПК-6; ПК-4
2.	Российские и международные стандарты на формирование цифровой подписи существуют	ПК-6; ПК-4
3.	Что такое инфраструктура открытых ключей	ПК-6; ПК-4
4.	Какие используются ассиметричные алгоритмы шифрования	ПК-6; ПК-4
5.	Какие используются симметричные алгоритмы шифрования	ПК-6; ПК-4
6.	Что такое средства стеганографической защиты информации	ПК-6; ПК-4
7.	Что такое механизм контроля и разграничения доступа	ПК-6; ПК-4
8.	Какие программные реализации программно-аппаратных средств защиты информации	ПК-6; ПК-4
9.	Основные направления, методы и средства технического противодействия закладным устройствам.	ПК-6; ПК-4
10.	Понятие о демаскирующих признаках объекта. Демаскирующие признаки сигналов	ПК-6; ПК-4
11.	Методы локализации закладных устройств. Метод энергетического зондирования. Метод акустической и радиолокационной	ПК-6; ПК-4

	триангуляции	
12.	Атрибуты и признаки потенциально опасного сигнала закладных устройств.	ПК-6; ПК-4
13.	Государственная система (иерархия) в области технических средств защиты информации. Основные руководящие, нормативные и методические документы	ПК-6; ПК-4
14.	Технический контроль эффективности мер по защите информации. Общая методика проведения технического контроля (ПЭМИН, акустических и виброакустических каналов утечки).	ПК-6; ПК-4
15.	Методы защиты программ от исследования	ПК-6; ПК-4
16.	Подходы к задаче защиты от копирования программ	ПК-6; ПК-4
17.	Типовое содержание работ в части создания защищенной автоматизированной системы	ПК-6; ПК-4
18.	Микроядерная архитектура с точки зрения создания защищенных операционных систем	ПК-6; ПК-4
19.	Средства обеспечения целостности и конфиденциальности при передаче информации по каналам связи	ПК-6; ПК-4
20.	Симметричные и асимметричные алгоритмы шифрования информации	ПК-6; ПК-4
21.	Функции удостоверяющего центра	ПК-6; ПК-4
22.	Основные схемы резервного копирования.	ПК-6; ПК-4
23.	Защита данных от разрушающих программных воздействий.	ПК-6; ПК-4
24.	Перечень организаций, участвующих в работах по созданию защищенных автоматизированных систем	ПК-6; ПК-4
25.	Юридические аспекты несанкционированного копирования программ	ПК-6; ПК-4
26.	Реализация механизмов безопасности на аппаратном уровне.	ПК-6; ПК-4
27.	Аутентификация пользователей при локальном и удаленном доступе к КС.	ПК-6; ПК-4
28.	Принцип работы систем обнаружения вторжений	ПК-6; ПК-4
29.	Взаимная проверка подлинности пользователей.	ПК-6; ПК-4
30.	Этапы разработки модели угроз.	ПК-6; ПК-4

Примерные тестовые задания

- проверка сформированности компетенций – ПК-6; ПК-4

1. Перечень сведений, доступ к которым не может быть ограничен определен:
а) Федеральным законом от 27 июля 2006 г. N 149-ФЗ;
б) Указом Президента РФ от 6 марта 1997 г. No 188;
в) Указом Президента РФ от 30 ноября 1995 г. N 1203.
2. Что такое доктрина информационной безопасности РФ
а) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации;
б) совокупность нормативных актов, обязательных для выполнения всеми хозяйствующими субъектами.
в) совокупность документов, регламентирующих организационно-технические мероприятия по обеспечению информационной безопасности Российской Федерации.
3. В российской практике проектирование ведётся ...
a. Поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-68.
b. в соответствии со стадиями, регламентированными ГОСТ 2.103-98.
c. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-78.
d. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-98.
4. Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к:
а) предупреждению угроз;
б) выявлению угроз;
в) локализации угроз;
г) ликвидации последствий угроз.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература
Основная

1. *Олифер В.Г.* Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М. [и др.] : Питер, 2008. – 957 с.
2. *Митюшин Д.А.* Использование программного комплекса Cisco Packet Tracer v.7.3 в изучении сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 с.
3. Голиков А. М. Основы проектирования защищенных телекоммуникационных систем: учебное пособие, Томск: ТУСУР, 2016. –396 с., http://biblioclub.ru

Дополнительная

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. http://rkn.gov.ru/Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

2. Nginx.org – [Электронный ресурс] : Режим доступа : https://nginx.org/ru, свободный. – Загл. с экрана
3. Wireshark Developer's Guide [Электронный ресурс]: Режим доступа: https://www.wireshark.org/docs/wsdg_html_chunked/, свободный. – Загл. с экрана

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
5. Cisco Packet Tracer v.7.2

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

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

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

При необходимости предусматривается увеличение времени для подготовки ответа.

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

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

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

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

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

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

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

9. Методические материалы

9.1 Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.
Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.
Тематика практических занятий соответствует программе дисциплины.

Практическая работа № 1 (4 ч) ***Определение целей защиты информации на предприятии регионального уровня. Рассмотрение особенностей объекта защиты информации – ПК-6; ПК-4***
Задания:

1. Осуществить принятие решения о необходимости защиты информации, содержащейся в информационной системе.
2. Определить угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе.
3. Определить требования к системе защиты информации информационной системы.

Практическая работа № 2 (4 ч) ***Определение каналов утечки информации и выработка мер защиты – ПК-6; ПК-4***
Задания:

1. Рассмотрение схемы технического канала утечки информации.
2. Анализ активного метода защиты информации от утечки.
3. Анализ пассивного метода от утечки инормации.

Практические работы № 3 (4 ч) ***Порядок проведения контроля эффективности мер защиты инструментальным методом – ПК-6; ПК-4***
Задания:

1. Подготовка исходных данных.
2. Оценить эффективность мер защиты информации инструментальным методом.
3. Сделать выводы

Практическая работа № 4 (4 ч) ***Порядок проведения контроля эффективности мер защиты инструментально-расчетным методом – ПК-6; ПК-4***
Задания:

1. Подготовка исходных данных.
2. Оценить эффективность мер защиты информации инструментально-расчетным методом.
3. Сделать выводы

Практическая работа № 5 (4 ч) ***Проведение контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИН – ПК-6; ПК-4***
Задания:

1. Изучение инструкции по эксплуатации.

2. Изучение схемы для определения побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации.

Практическая работа № 6 (4 ч) ***Аттестация автоматизированной системы по требованиям безопасности – ПК-6; ПК-4***

Задания:

1. изучить план-схему местности, границы контролируемой зоны объекта и места возможного ведения разведки ПЭМИН.
2. определить реальные размеры зоны R2 технических средств, установленных на объекте, по соответствующим методикам из сборника методик инструментального контроля.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Технические средства контроля эффективности мер защиты информации в автоматизированных системах» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – формирование основных знаний и умений в области технологий проектирования защищенных автоматизированных систем и соответствующими общепрофессиональными компетенциями в соответствии с ООП.
Задачи дисциплины:
– формирование знаний в области технических средств контроля мер защиты информации в автоматизированных системах;
– уяснение основных понятий и определений, позволяющих осуществлять выбор и технических средств защиты;
– Рассмотреть особенности контроля эффективности мер защиты с помощью технических средств, а также методов, используемых при проведении контроля.

Дисциплина направлена на формирование следующих компетенций:
- ПК-6 – Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
- ПК-4 – Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций

В результате освоения дисциплины обучающийся должен:
Знать: критерии оценки защищённости АС, основные угрозы безопасности информации АС; модели нарушителя в АС, методы оценки работоспособности применяемых средств защиты информации в АС с использованием штатных средств и методик; методы и способы обеспечения отказоустойчивости АС; содержание и порядок деятельности персонала по эксплуатации защищённых АС и подсистем безопасности АС
Уметь: контролировать уровень защищённости в АС; регистрировать и анализировать события, связанные с защитой информации в АС; оценить эффективности применяемых средств защиты информации в АС с использованием штатных средств и методик; применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в АС
Владеть: навыками проведения аудита защищённости информации в АС, навыками определения уровня защищённости и доверия средств защиты информации АС; навыками обнаружения, устранения неисправностей в работе системы защиты информации АС; резервирования программного обеспечения, технических средств, каналов передачи данных АС управления на случай возникновения нештатных ситуаций

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.
Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.