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

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(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 2024

Угрозы информационной безопасности автоматизированных систем
Рабочая программа дисциплины

Составитель(и):
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 14.03.2024 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины –формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем (АС), выявления угроз безопасности информации.

Задачи дисциплины:

– рассмотрение существа проблемы безопасности информации в автоматизированных системах, основных способов обеспечения доступности, конфиденциальности и целостности информации при её передаче и обработке.

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-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1 Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования	Знать: • основные виды угроз безопасности информации при её хранении и обработки в АС и её передачи. • угрозы и методы нарушения безопасности АС; • формальные модели, лежащие в основе систем защиты АС; • стандарты по оценке защищённости АС и их теоретические основы
	ПК-2.2 Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации	Уметь: • проводить анализ угроз безопасности АС; • разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы
	ПК-2.3 Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах	Владеть: • навыками работы с АС распределённых вычислений и обработки информации; • навыками работы с нормативными документами ФСТЭК России
ПК-8 Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах	ПК-8.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации	Знать: • методы и средства реализации, защищённых АС; • методы и средства верификации и анализа надёжности, защищённых АС • Базовую модель угроз ФСТЭК России

	ПК-8.2 Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем	Уметь: • анализировать угрозы безопасности информации АС; • реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищённости АС.
	ПК-8.3 Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы	Владеть: • приёмами использования критериев оценки защищённости АС; • приёмами построения формальных моделей систем защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Угрозы информационной безопасности автоматизированных систем» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих модулей и дисциплин: «Правовое и организационное обеспечение информационной безопасности», «Информационные процессы и системы».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Технические средства защиты информации от утечки по техническим каналам», «Безопасность критически важных информационных систем», «Защита информации от вредоносного программного обеспечения», «Безопасность систем баз данных», «Безопасность вычислительных сетей».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3_ з.е., 108 академических часа.

Структура дисциплины для очной формы обучения

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

Семестр	Тип учебных занятий	Количество часов
5	Лекции	**28**
5	Практические работы	**36**
5	Промежуточная аттестация	**18**
Всего:		**64**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _26_ академических часов.

3. Содержание дисциплины

Тема 1. Основные угрозы информационной безопасности автоматизированных систем

Актуальность проблемы защиты АС в современных условиях. Факторы, её определяющие. Защита АС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими.

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России и её связь угрозами АС. Основные термины и определения.

Классификация угроз информационной безопасности автоматизированных систем. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в АС. Источниками угроз НСД. Виды нарушителей безопасности информации. Общая характеристика уязвимостей АС.

Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования.

Общая характеристика уязвимостей прикладного программного обеспечения.

Общая характеристика угроз непосредственного доступа в операционную среду АС.

Общая характеристика угроз безопасности информации АС, реализуемых с использованием протоколов межсетевого взаимодействия.

Общая характеристика угроз программно-математических воздействий.

Общая характеристика нетрадиционных информационных каналов.

Характеристика стеганографических методов преобразования информации.

Общая характеристика результатов несанкционированного или случайного доступа.

Тема 2 Модели угроз безопасности информации в автоматизированных системах.

Типовые модели угроз безопасности АС на основе базовой модели угроз ФСТЭК России.

Классификация АС. Модели угроз разных типов АС.

Тема 3. Оценка угроз безопасности информации автоматизированных систем

Термины и определения. Порядок оценки угроз безопасности информации. Определение негативных последствий от реализации (возникновения) угроз безопасности информации АС. Определение возможных объектов воздействия угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности. Экспертная оценка угроз безопасности информации АС. Структура модели угроз безопасности информации АС. Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации. Возможные цели реализации угроз безопасности информации нарушителями. Уровни возможностей нарушителей по реализации угроз безопасности информации.

Тема 4. Банк данных угроз безопасности информации ФСТЭК России

Классификация уязвимостей по ГОСТ Р 56546-2015. Виды уязвимостей в Банке данных. Основные угрозы безопасности информации. Порядок включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России

Тема 5. Обеспечение безопасности автоматизированных систем

Организационная структура системы обеспечения безопасности АС. Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС. Требования к технологии управления безопасностью. Мероприятия при реализации технологии управления безопасностью. Институт ответственных за обеспечение информационной безопасности. Влияние на безопасность ИТ разных субъектов организации ИБ. Цели регламентации действий

пользователей и обслуживающего персонала АС. Составляющие эффективного функционирования системы безопасности ИТ. Политика безопасности организации в области ИТ, её цель, условия осуществления и проблемы. Уровни зрелости (в сфере обеспечения ИБ). Виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности АС. Организационно-распорядительные документы по обеспечению безопасности АС. Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.

Явная и неявная компрометация ключей. Признаки и действия при компрометации ключей. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей АС. Регламентация порядка изменения конфигурации аппаратно-программных средств АС.

Тема 6. Недекларированные возможности

Основные положения РД ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

Классификация недекларированных возможностей. Выявление уязвимостей и недекларированных возможностей в ПО. Защита от уязвимостей и недекларированных возможностей.

Тема 7. Защита информации в автоматизированных системах от угроз безопасности

Основные механизмы защиты автоматизированных систем от НСД. Сущность и назначение идентификации и аутентификации пользователей. Виды и способы аутентификации. Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа. Сущность избирательного и полномочного разграничения доступа. Замкнутая программная среда. Регистрация и оперативное оповещение о событиях безопасности.

Защита периметра корпоративной сети.

Аппаратно-программные средства защиты информации от НСД. Рекомендации по выбору СЗИ НСД. Виды биометрической идентификации, преимущества и недостатки.

Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды. Демилитаризованная зона. Анализ содержимого почтового и вебтрафика.

Виртуальные частные сети.

Концепция построения виртуальных частных сетей – VPN. Основные понятия и функции сети VPN. Защита информации в процессе её передачи по туннелю VPN. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN.

Применение штатных и дополнительных СЗИ НСД. Стратегия безопасности компании Microsoft. Защита от вмешательства в процесс нормального функционирования АС. Встроенные механизмы разграничения доступа на примере ОС Windows. Уровни доверия механизм целостности. Оперативное оповещение о зарегистрированных попытках НСД. Службы ACS. Система защиты информации от НСД Secret Net 6. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Основные угрозы информационной безопасности авто-	Лекция 1.	Традиционная с использованием презентаций, Опрос

	матизированных систем	Самостоятельная работа	Изучение материалов лекций
2	Модели угроз безопасности информации в автоматизированных системах.	Лекция 2. Самостоятельная работа	Традиционная с использованием презентаций, Опрос Изучение материалов лекций
3	Оценка угроз безопасности информации автоматизированных систем	Лекция 3 Самостоятельная работа	Традиционная с использованием презентаций, Опрос Изучение материалов лекций
4	Банк данных угроз безопасности информации ФСТЭК России	Лекция 4. Самостоятельная работа	Традиционная с использованием презентаций, Опрос Выполнение задания Изучение материалов лекций
5	Обеспечение безопасности автоматизированных систем	Лекция 5. Самостоятельная работа	Традиционная с использованием презентаций, Опрос Изучение материалов лекций
6	Недекларированные возможности	Лекция 6 Самостоятельная работа	Традиционная с использованием презентаций, Опрос Изучение материалов лекций
7	Защита информации в автоматизированных системах от угроз безопасности	Лекция 7 Самостоятельная работа	Традиционная с использованием презентаций, Опрос Изучение материалов лекций
8	Практическая работа № 1. Разработка организационных и организационно-технических мероприятий по защите автоматизированной системы	Практическая работа	Выполнение и защита практической работы
9	Практическая работа № 2. Создание простого VPN канала	Практическая работа	Выполнение и защита практической работы
10	Практическая работа № 3. Защита автоматизированной системы путём создания списков контроля доступа	Практическая работа	Выполнение и защита практической работы

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	*3 балла*	*15 баллов*
- практическая работа 1-3	*15 баллов*	*45 баллов*
Промежуточная аттестация –экзамен (экзамен по билетам)		40 баллов
Итого за семестр		100 баллов

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

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

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	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 теку-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		щей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. 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.	Критерии классификации и классификация нарушителей.	ПК-2, ПК-8
2.	Основные понятия в ИБ АС.	ПК-2, ПК-8
3.	Цель защиты АС и циркулирующей в ней информации.	ПК-2, ПК-8
4.	Перечислите виды угроз безопасности информации АС	ПК-2, ПК-8
5.	Перечислите этапы анализа рисков и управления ими.	ПК-2, ПК-8
6.	Перечислите модели угроз безопасности информации АС	ПК-2, ПК-8
7.	Назовите порядок оценки угроз безопасности информации.	ПК-2, ПК-8
8.	Сущность экспертной оценки угроз безопасности информации АС	ПК-2, ПК-8
9.	Классификация уязвимостей по ГОСТ Р 56546-2015	ПК-2, ПК-8
10.	Перечислите основные виды уязвимостей в Банке данных ФСТЭК России.	ПК-2, ПК-8
11.	Недекларированные возможности.	ПК-2, ПК-8
12.	Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей	ПК-2, ПК-8
13.	Организационная структура системы обеспечения безопасности АС.	ПК-2, ПК-8

14.	Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС.	ПК-2, ПК-8
15.	Влияние на безопасность ИТ разных субъектов организации ИБ.	ПК-2, ПК-8
16.	Порядок работы с носителями ключевой информации.	ПК-2, ПК-8
17.	Явная и неявная компрометация ключей.	ПК-2, ПК-8
18.	Признаки и действия при компрометации ключей.	ПК-2, ПК-8
19.	Регламентация правил парольной и антивирусной защиты.	ПК-2, ПК-8
20.	Что такое демилитаризованная зона?	ПК-2, ПК-8
21.	Какие сервисы помещают в ДМЗ?	ПК-2, ПК-8
22.	Основные виды VPN?	ПК-2, ПК-8
23.	Основные варианты архитектуры VPN	ПК-2, ПК-8
24.	Основные механизмы защиты автоматизированных систем от НСД.	ПК-2, ПК-8
25.	Виды и способы аутентификации.	ПК-2, ПК-8
26.	Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа.	ПК-2, ПК-8

Промежуточная аттестация (примерные вопросы к экзамену)

№	Вопрос	Реализуемая компетенция
1.	Защита АС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими.	ПК-2, ПК-8
2.	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России и её связь угрозами АС.	ПК-2, ПК-8
3.	Классификация угроз информационной безопасности автоматизированных систем.	ПК-2, ПК-8
4.	Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования.	ПК-2, ПК-8
5.	Общая характеристика уязвимостей прикладного программного обеспечения.	ПК-2, ПК-8
6.	Общая характеристика угроз непосредственного доступа в операционную среду АС.	ПК-2, ПК-8
7.	Общая характеристика угроз безопасности информации АС, реализуемых с использованием протоколов межсетевого взаимодействия.	ПК-2, ПК-8
8.	Общая характеристика угроз программно-математических воздействий.	ПК-2, ПК-8
9.	Общая характеристика нетрадиционных информационных каналов.	ПК-2, ПК-8
10.	Характеристика стеганографических методов преобразования информации и результатов несанкционированного или случайного доступа.	ПК-2, ПК-8
11.	Типовые модели угроз безопасности АС на основе базовой модели угроз ФСТЭК России. Классификация АС. Модели угроз разных типов АС.	ПК-2, ПК-8
12.	Порядок оценки угроз безопасности информации. Определение негативных последствий от реализации (возникновения) угроз безопасности информации АС.	ПК-2, ПК-8
13.	Структура модели угроз безопасности информации АС. Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации	ПК-2, ПК-8
14.	Возможные цели реализации угроз безопасности информации нарушителями. Уровни возможностей нарушителей по реализации угроз безопасности информации.	ПК-2, ПК-8
15.	Классификация уязвимостей по ГОСТ Р 56546-2015. Виды уязвимостей в Банке данных.	ПК-2, ПК-8

16.	Порядок включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз	ПК-2, ПК-8
17.	Организационная структура системы обеспечения безопасности АС. Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС. Требования к технологии управления безопасностью.	ПК-2, ПК-8
18.	Влияние на безопасность ИТ разных субъектов организации ИБ	ПК-2, ПК-8
19.	Виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты.	ПК-2, ПК-8
20.	Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора.	ПК-2, ПК-8
21.	Основные положения РД ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».	ПК-2, ПК-8
22.	Классификация недекларированных возможностей. Выявление уязвимостей и недекларированных возможностей в ПО. Защита от уязвимостей и недекларированных возможностей.	ПК-2, ПК-8
23.	Сущность и назначение идентификации и аутентификации пользователей. Виды и способы аутентификации.	ПК-2, ПК-8
24.	Основные механизмы защиты автоматизированных систем от НСД.	ПК-2, ПК-8
25.	Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа.	ПК-2, ПК-8
26.	Сущность избирательного и полномочного разграничения доступа.	ПК-2, ПК-8
27.	Замкнутая программная среда.	ПК-2, ПК-8
28.	Криптографические методы защиты информации. Криптография с симметричными и открытыми ключами	ПК-2, ПК-8
29.	Электронная цифровая подпись. Реализация ЭЦП.	ПК-2, ПК-8
30.	Система обнаружения и предотвращения атак.	ПК-2, ПК-8
31.	Защита периметра компьютерных сетей и управление механизмами защиты.	ПК-2, ПК-8
32.	Виды биометрической идентификации, преимущества и недостатки	ПК-2, ПК-8
33.	Аппаратно-программные средства защиты информации от НСД.	ПК-2, ПК-8
34.	Применение штатных и дополнительных СЗИ НСД.	ПК-2, ПК-8
35.	Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра.	ПК-2, ПК-8
36.	Межсетевые экраны их виды. Демилитаризованная зона.	ПК-2, ПК-8
37.	Концепция построения виртуальных частных сетей – VPN.	ПК-2, ПК-8
38.	VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN	ПК-2, ПК-8
39.	Стратегия безопасности компании Microsoft.	ПК-2, ПК-8
40.	Защита от вмешательства в процесс нормального функционирования АС.	ПК-2, ПК-8
41.	Встроенные механизмы разграничения доступа на примере ОС Windows.	ПК-2, ПК-8
42.	Уровни доверия механизм целостности. Службы ACS.	ПК-2, ПК-8
43.	Оперативное оповещение о зарегистрированных попытках НСД.	ПК-2, ПК-8
44.	Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.	ПК-2, ПК-8

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. *Базовая модель угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/files/492/---15--2008-/887/---15--2008-.pdf, свободный. – Загл. с экрана
2. Методика оценки угроз безопасности информации. [Электронный ресурс] / Методический документ. Утверждён ФСТЭК России 5 февраля 2021 г. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g
3. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g, свободный. – Загл. с экрана.

Дополнительные

1. Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России. [Электронный ресурс] / Методический документ. Утверждён ФСТЭК России 26 июня 2018 г. – Режим доступа: https://bdu.fstec.ru/regulations
2. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114 [Электронный ресурс] : Режим доступа : https://fstec.ru/files/489/---4--1999--N-114/880/---4--1999--N-114.pdf свободный. – Загл. с экрана.
3. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. [Электронный ресурс] – Режим доступа: https://protect.gost.ru/v.aspx?control=7&id=201376
4. Банк данных угроз безопасности информации. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана.

Литература

Основная

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022. – Режим доступа: по подписке.
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.

Дополнительная

1. *Олифер, В. Г.* Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань :

электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346. — Режим доступа: для авториз. пользователей.
2. *Воробьев, С. П.* Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292247. — Режим доступа: для авториз. пользователей.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный бюллетень Jet Info [Электронный ресурс]. – Электрон. дан. – [М., 2014]. – Режим доступа свобод.: http://www.jetinfo.ru/ .
2. Сайт НИЦ «Охрана» Росгвардии.– Режим доступа свобод.: http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html
3. Glossary Commander. Служба тематических толковых словарей [Электронный ресурс]. – Электрон. дан. - [М., 2008]. - Режим доступа свобод.: http://glossary.ru/ .
4. Сайт справочно-правовой системы по федеральному и региональным законодательствам России - Режим доступа свобод.: http://pravo.ru/
5. Информационный портал в области защиты информации Режим доступа свобод.: http://www.securitylab.ru
6. Портал ФСТЭК http://www.fstec.ru
7. ELibrary.ru Научная электронная библиотека www.elibrary.ru
8. Электронная библиотека Grebennikon.ruwww.grebennikon.ru

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

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. MicrosoftOffice
3. KasperskyEndpointSecurity

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.8

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.

Практическое работа 1 (8 ч.) – Разработка организационных и организационно-технических мероприятий по защите автоматизированной системы – проверка сформированности компетенций – ПК-2; ПК-8
Задания:
1. Разработать для предложенной фирмы виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты.
2. Составить матрицу разделения доступа к ресурсам для предложенной фирмы.
3. Выполнить мандатное разграничение доступа к ресурсам.
4. Ответить на устные вопросы при защите.

Указания по выполнению заданий:
1. Изучить теоретические материалы.
2. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Практическая работа № 2 (8 ч.). Создание простого VPN канала – проверка сформированности компетенций – ПК-2; ПК-8
Практическая работа № 7 из учебного пособия:

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.

Практическая работа № 3 (20 ч.). Защита автоматизированной системы путём создания списков контроля доступа – проверка сформированности компетенций – ПК-2; ПК-8
На основе разработанной модели разграничения доступа, используя практическую работу № 6 из учебного пособия:
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.

Крайне желательно практические работы № 2 и 3 выполнять после завершения практических работ № 1-6 дисциплины «Сети и системы передачи информации».

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office и выше и передаётся преподавателю посредством оговорённой формы связи.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Угрозы информационной безопасности автоматизированных систем» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель формирование базовых знаний в области обеспечения информационной безопасности АС, выявления угроз безопасности информации.

Задачи: рассмотрение существа проблемы безопасности информации в автоматизированных системах, основных способов обеспечения доступности, конфиденциальности и целостности информации при её передаче и обработке.

Дисциплина направлена на формирование следующих компетенций:

- ПК-2– Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
- ПК-8 – Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах

В результате освоения дисциплины обучающийся должен:

Знать: основные виды угроз безопасности информации при её хранении и обработки в АС и её передачи; угрозы и методы нарушения безопасности АС; формальные модели, лежащие в основе систем защиты АС; стандарты по оценке защищённости АС и их теоретические основы; методы и средства реализации, верификации и анализа надёжности защищённых АС; Базовую модель угроз ФСТЭК России.

Уметь: проводить анализ угроз безопасности АС; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; анализировать угрозы безопасности информации АС; реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищённости АС.

Владеть: навыками работы с АС распределённых вычислений и обработки информации; навыками работы с нормативными документами ФСТЭК России; приёмами использования критериев оценки защищённости АС, построения формальных моделей систем защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.