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

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 23.03.2023

Оглавление

1. Пояснительная записка

1.1. Цель и задачи дисциплины
Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.
Задачи: изучение основ построения подсистем информационной безопасности, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Уметь: анализировать ограничения вычислительных ресурсов, выбирать оптимальный набор программно-аппаратных ПАСЗИ
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Владеть: навыками использования положений стандартов при разработке, настройке и эксплуатации ПАСЗИ
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	ОПК-10.1 Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации
	ОПК-10.2 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	Уметь: осуществлять настройку политики ученых записей, выполнять администрирование учетных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости

		подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестра.
	ОПК-10.3 Владеет принципами формирования политики информационной безопасности объекта информатизации	Владеть: навыками администрирования подсистем безопасности, настройки системы, политик безопасности, управления учетными записями.
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта	Знать:линейку программно-аппаратных средств защиты информации; подходы к тестированию программно-аппаратных средств защиты информации Владетьнавыками проектирования, настройки и эксплуатации средств защиты информации с учетом технико-экономических показателей.
	ОПК-12.2 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	Уметь:осуществлять выбор программно-аппаратных средств защиты информации адекватных решаемым задачам; составлять методики испытаний средств защиты информации; подходы по оценке показателей качества, критерии оценки программно-аппаратных средств защиты информации
	ОПК-12.3 Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	Владетьнавыками проектирования, настройки и эксплуатации средств защиты информации с учетом технико-экономических показателей.

1.3. Место дисциплины в структуре образовательной программы

«Программно-аппаратные средства защиты информации» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: "Безопасность операционных систем", "Защита информации от вредоносного программного обеспечения".

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: "Оценка безопасности программного обеспечения автоматизированных систем", "Безопасность программного обеспечения автоматизированных систем".

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часов

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	Лабораторные работы	**20**
6	Лекции	**16**
6	Лабораторные работы	**20**
	Всего:	**72**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _72_ академических часов.

3. Содержание дисциплины

5 семестр

№	Наименование раздела дисциплины	Содержание
1	**Общие представления о программно-аппаратных средствах защиты информации**	Общее понятие программно-аппаратных средств защиты информации. Типы программно-аппаратных средств защиты информации. Средства криптографической защиты информации. Генераторы псевдослучайных чисел. Аппаратные модули доверенной загрузки. Средства контроля внешних носителей. Межсетевое экранирование.
2	**Средства идентификации и аутентификации**	Понятия идентификации и аутентификации. Локальная аутентификация. Свойства хэш-функций. Алгоритм NTLM. Концепция PluggableAuthenticationModule. Сетевой протокол аутентификации Kerberos. Атаки на подсистему аутентификации.
3	**Разграничение доступа**	Дискреционное и мандатное разграничение доступа. Субъекты и объекты доступа. Структуры файловых систем NTFS и UFS, метаданные. Списки контроля доступа.

		SecurityReferenceMonitor, авторизация.
4	**Регистрация событий безопасности**	Регистрация событий безопасности. Категории регистрируемых событий. Регистрация доступ к объектам файловой системы. Управление регистрационными журналами.
5	**Контроль целостности**	Процедура контроля целостности. Алгоритмы расчета контрольных сумм (CRC, MD5, SHA-1). Средства гарантийного удаления информации.

6 семестр

№	Наименование раздела дисциплины	Содержание
1	**Предмет и задачи программно-аппаратной защиты информации**	Предмет защиты. Свойства информации и её ценность. Объект защиты информации. Виды информации. Утечка информации и её виды. Сетевое и межсетевое взаимодействие. Политика безопасности.
2	**Вредоносные программы и удалённые сетевые атаки**	Вредоносные программы. Компьютерные вирусы. Троянские кони. Сетевые черви. Потайные ходы и руткиты. вредоносные программы для мобильных устройств. Прочие вредоносные программы. Наименование вирусов. Элементы защиты от вредоносного программного обеспечения. Технология Black и Whitelisting. Удалённые сетевые атаки. Сетевые атаки. Обобщённый сценарий атаки. Атаки «отказ в обслуживании». Атаки на протоколы IP, ICMP, UDP, TCP. Генераторы атак. Атака К. Митника. Классификации удалённых атак.
3	**Межсетевые экраны**	Развитие технологий межсетевого экранирования. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояний. Межсетевые экраны уровня ядра. Персональные межсетевые экраны. Распределённые межсетевые экраны. Межсетевые экраны Web-приложений. Новое поколение межсетевых экранов. Обход межсетевых экранов. Постепенный подход. Туннелирование. Требования и показатели защищённости межсетевых экранов. Тестирование межсетевых экранов. Примеры межсетевых экранов.
4	**Виртуальные частные сети**	Виртуализация и облачные технологии. Туннелирование. Протоколы VPN канального уровня. Протокол IPSec. Ассоциация обеспечения безопасности. Туннельный и

		транспортный режимы протокола IPSec. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Пример применения протокола IKE. Совместное использование протоколов ESP и AH. Основные типы защищённых связей. Протоколы VPN транспортного уровня. Цифровые сертификаты. Примеры отечественного построения VPN. Криптошлюзы. Инфраструктура PKI
5	**Системы обнаружения и предотвращения вторжений**	Модели систем обнаружения вторжений. Модель Д. Деннинг. Модель CIDF. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Система обнаружения вторжений Snort. Декодер пакетов. Препроцессоры. Препроцессоры сборки пакетов. Препроцессоры нормализации протоколов. Препроцессоры обнаружения аномалий. Процессор обнаружения. Модули вывода. Правила Snort. Примеры правил. Обнаружение аномалий. Методы DataMining. Методы технологии мобильных агентов. Методы построения иммунных систем. Применение генетических алгоритмов. Применение нейронных сетей. Языки описания атак. Другие методы обнаружения вторжений. Системы анализа защищённости. Системы анализа целостности. Вспомогательные средства обнаружения. Методы обхода систем обнаружения вторжений. Методы обхода сетевых систем обнаружения вторжений. Методы обхода хостовых систем обнаружения вторжений. Динамические методы обхода. Тестирование систем обнаружения вторжений. Тестирование коммерческих систем. Тестирование исследовательских прототипов. Методы формирования тестовых наборов. Матрица несоответствий. Системы предупреждения вторжений

4. Образовательные технологии

5 семестр

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Общие представления о программно-аппаратных средствах защиты	Лекция 1.1 Лекция 1.2 Самостоятельная работа	Традиционная с использованием презентаций Тестирование Изучение материалов лекций

	информации		
2	Средства идентификации и аутентификации	Лекция 2.1 Лекция 2.2 Лекция 2.3 Лабораторная работа 1. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
3	Разграничение доступа 3.1. Дискреционное разграничение доступа 3.2. Полномочное разграничение доступа	Лекция 3.1 Лекция 3.2 Лекция 3.3 Лабораторная работа2. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
4	Регистрация событий безопасности	Лекция 4.1 Лекция 4.2 Лекция 4.3 Лабораторная работа3. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
5	Контроль целостности	Лекция 5.1 Лекция 5.2 Лекция 5.3 Лабораторная работа4. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций

6 семестр

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Предмет и задачи программно-аппаратной защиты информации	Лекция 1 Самостоятельная работа	Традиционная лекция с использованием презентаций Тестирование Подготовка к занятиям с использованием ЭБС
2	Удалённые сетевые атаки	Лекция 2 Лабораторная работа 1.	Традиционная лекция с использованием презентаций Тестирование Занятия с использованием специализированного ПО

		Самостоятельная работа	Подготовка к занятиям с использованием ЭБС
3	Межсетевые экраны и аппаратные криптографические шлюзы	Лекция 3.1. Лекция 3.2. Лабораторная работа 2. Самостоятельная работа	Традиционная лекция с использованием презентаций Тестирование Занятия с использованием специализированного ПО и оборудования Подготовка к занятиям с использованием ЭБС
4	Виртуализация и облачные технологии. Виртуальные частные сети	Лекция 4.1 Лекция 4.2 Лабораторная работа 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Тестирование Занятия с использованием специализированного ПО и оборудования Подготовка к занятиям
5	Системы обнаружения и предотвращения вторжений	Лекция 5.1. Лекция 5.2. Лабораторная работа 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Тестирование Занятия с использованием специализированного ПО и оборудования Подготовка к занятиям с использованием ЭБС

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5 семестр

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль (5 семестр): *– тестирование (темы 1-5)* *– лабораторные работы (темы 2-3)* *– лабораторные работы(темы 4-5)*	 *4 балла* *10 баллов* *10 баллов*	 *20 баллов* *20 баллов* *20 баллов*
Промежуточная аттестация - зачет *(Зачет по билетам)*		*40 баллов*
Итого за семестр		*100 баллов*

6 семестр

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль (6 семестр): *– тестирование (темы 1-5)*	 *4 балла*	 *20 баллов*

– лабораторные работы(темы 2-3) *– лабораторные работы(темы 4-5)*	*10 баллов* *10 баллов*	*20 баллов* *20 баллов*
Промежуточная аттестация – экзамен *(экзаменпо билетам)*		*40 баллов*
Итого за семестр		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 5	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-12.1; ОПК-12.2; ОПК-12.3; УК-2.1; УК-2.2; УК-2.3	Опрос
2.	Лабораторные занятия 1 – 4 (5 семестр)	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-12.1; ОПК-12.2; ОПК-12.3; УК-2.1; УК-2.2; УК-2.3	Отчет по лабораторным работам
3	Лабораторные занятия 1 – 4 (6 семестр)	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-12.1; ОПК-12.2; ОПК-12.3; УК-2.1; УК-2.2; УК-2.3	Отчет по лабораторным работам

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

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

5.2.Критерии выставления оценки по дисциплине

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

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов 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

Примерные контрольные вопросы для зачета - проверка сформированности компетенций ОПК-10, УК-2

Контрольные вопросы	Проверяемые компетенции
1. Базовые сервисы безопасности.	ОПК-10.1, ОПК-10.2
2. Назначение и принцип работы утилиты «Ревизор 1».	ОПК-10.1
3. Назначение и принцип работы утилиты «Ревизор 2».	ОПК-10.1; УК-2.1; УК-2.2
4. Назначение и принцип работы утилиты ФИКС.	ОПК-10.1; УК-2.1
5. Идентификация и аутентификация и управление учетными записями пользователей в СУБД Oracle.	ОПК-10.1, ОПК-10.2

6. Разграничение доступа в СУБД Oracle.	ОПК-10.1, ОПК-10.2
7. Мандатное разграничение доступа в OracleLabelSecurity.	ОПК-10.1, ОПК-10.2
8. Схема аутентификации Нидхема-Шредера.	ОПК-10.1, ОПК-10.2
9. Протокол аутентификации Kerberos.	ОПК-10.1, ОПК-10.2
10. Назначение и принципы работы Oracle Database Vault.	ОПК-10.1; УК-2.1; УК-2.2; УК-2.3
11. Линейка продуктов ОКБ САПР.	ОПК-10.3
12. Назначение и функциональные возможности АМДЗ Аккорд.	ОПК-10.3; УК-2.1; УК-2.2;
13. Типы СКЗИ и их функциональное назначение.	ОПК-10.2, ОПК-10.3
14. Линейка продуктов на рынке СЗИ.	ОПК-10.3; УК-2.1; УК-2.2
15. Архитектура и состав СЗИ SecretNet.	ОПК-10.3
16. Разграничение доступа к устройствам в SecretNet.	ОПК-10.1, ОПК-10.2; УК-2.1; УК-2.2; УК-2.3
17. Полномочное управление доступом в SecretNet.	ОПК-10.1, ОПК-10.2
18. Контроль целостности в SecretNet.	ОПК-10.1, ОПК-10.2
19. Концепция замкнутой программной среды, реализация в SecretNet.	ОПК-10.1, ОПК-10.2
20. Средства анализа и поиска уязвимостей XSpider и MaxPatrol.	ОПК-10.2, ОПК-10.3; УК-2.1; УК-2.2; УК-2.3
21. Архитектура и состав SafeNet.	ОПК-10.2, ОПК-10.3
22. Состав и назначение PCI Соболь.	ОПК-10.3
23. Понятие «кольца защиты» ОС.	ОПК-10.2; УК-2.1; УК-2.2; УК-2.3
24. Аппаратные технологии поддержки виртуализации.	ОПК-10.2, ОПК-10.3
25. Принципы доменной защиты.	ОПК-10.2, ОПК-10.3
26. Понятие и особенность ролевой политики безопасности.	ОПК-10.2, ОПК-10.3; УК-2.2; УК-2.3
27. Транзакционная память и защита информации в Супер-ЭВМ.	ОПК-10.2, ОПК-10.3 УК-2.1; УК-2.2

Примерные задания для тестирования- проверка сформированности компетенцийОПК-10, УК-2

1. Целью защиты информации являются:

а) предотвращение утечки, искажения, утраты, блокирования или незаконного тиражирования информации.

б) внедрение сторонних программных агентов.

в) предотвращение чтения журналов регистрации.

2. Доверенная загрузка — это:

а) сетевое устройство, подключаемое к материнской плате компьютера.

б)загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя .

в) загрузка операционной системы с внешних незарегистрированных носителей без контроля целостности образа операционной системы.

Примерные вопросы к экзамену - проверка сформированности компетенций ОПК-12

Контрольные вопросы	**Проверяемые компетенции**
1. Предмет и объект защиты программно-аппаратной защиты. Свойства, виды информации и её ценность.	ОПК-12.1
2. Утечка информации и её виды. Каналы утечки.	ОПК-12.1
3. Сетевое и межсетевое взаимодействие.	ОПК-12.2
4. Политика безопасности.	ОПК-12.2
5. Вредоносные программы. Компьютерные вирусы.	ОПК-12.2
6. Троянские кони и сетевые черви.	ОПК-12.2
7. Вредоносные программы. Потайные ходы и руткиты.	ОПК-12.1, ОПК-12.2
8. вредоносные программы для мобильных устройств. Прочие вредоносные программы.	ОПК-12.1, ОПК-12.2
9. Наименование вирусов. Элементы защиты от вредоносного программного обеспечения.	ОПК-12.1, ОПК-12.2
10. Технология Black и Whitelisting.	ОПК-12.1, ОПК-12.3
11. Сетевые атаки. Обобщённый сценарий атаки.	ОПК-12.1, ОПК-12.3
12. Атаки «отказ в обслуживании».	ОПК-12.1, ОПК-12.3
13. Атаки на протоколы IP, ICMP, UDP, TCP. Генераторы атак. Атака К. Митника.	ОПК-12.1, ОПК-12.3
14. Классификации удалённых атак.	ОПК-12.1
15. Технологии межсетевого экранирования.	ОПК-12.1
16. Методы обхода межсетевых экранов.	ОПК-12.2
17. Требования и показатели защищённости межсетевых экранов.	ОПК-12.1, ОПК-12.2
18. Тестирование межсетевых экранов.	ОПК-12.3
19. Сущность виртуализации и облачных технологий.	ОПК-12.1
20. Туннелирование. Протоколы VPN канального уровня.	ОПК-12.2
21. Протокол IPSec.	ОПК-12.2
22. Протокол обмена интернет-ключами. Пример применения протокола IKE.	ОПК-12.2
23. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH.	ОПК-12.2
24. Основные типы защищённых связей. Протоколы VPN транспортного уровня.	ОПК-12.2
25. Криптошлюзы.	ОПК-12.2
26. Инфраструктура PKI	ОПК-12.3, ОПК-12.2
27. Модели систем обнаружения вторжений.	ОПК-12.3
28. Классификация систем обнаружения вторжений.	ОПК-12.3
29. Обнаружение сигнатур и обнаружение аномалий.	ОПК-12.3

30. Система обнаружения вторжений Snort.	ОПК-12.3, ОПК-12.2
31. Методы DataMining. Методы технологии мобильных агентов и построения иммунных систем.	ОПК-12.1, ОПК-12.2
32. Методы DataMining. Применение генетических алгоритмов и нейронных сетей.	ОПК-12.1, ОПК-12.2
33. Методы обнаружения вторжений на основе анализа защищённости, анализа целостности. Вспомогательные средства обнаружения.	ОПК-12.1, ОПК-12.2
34. Методы обхода систем обнаружения вторжений.	ОПК-12.3
35. Тестирование систем обнаружения вторжений.	ОПК-12.3
36. Системы предупреждения вторжений	ОПК-12.1

Примерные задания для тестирования-проверка сформированности компетенций ОПК-12

1. Протокол IPSec работает на коком уровне модели OSI:
а) на сетевом уровне.
б) на канальном уровне.
в) на физическом уровне.

2. Руткит — это:
а) компьютерный вирус.
б) набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих: маскировку объектов (процессов, файлов, каталогов, драйверов);управление (событиями, происходящими в системе);сбор данных (параметров системы).
в) рекламное программное обеспечение

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., посл. от 01.05.2019). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» (с изм. и доп., посл. от 31.12.2017). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральныйзакон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» (с изм. и доп., посл. от 23.06.2016). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральныйзакон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» (с изм. и доп., посл. от 28.11.2018). [Электронный ресурс] : Режим

доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература
основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368
2. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
3. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
4. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Официальный сайт ФСТЭК РФ [Электронный ресурс] : Режим доступа: http://www.fstec.ru/, свободный. – Загл. с экрана.
2. Сайт компании ОКБ САПР [Электронный ресурс] : Режим доступа: http://www.okbsapr.ru/, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ruwww.grebennikon.ru
Cambridge University Press
ProQuest Dissertation& Theses Global
SAGE Journals
TaylorandFrancis
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. MicrosoftOffice
3. Kaspersky Endpoint Security

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

2) для лабораторных 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. MicrosoftSharePoint 2010
6. SecretNetStudio 8.4
7. Dallas Lock 8.0
8. Vmware Player 15.5 + Гостевая ОС CentOS 7
9. Open VPN
10. Wireshark 3.0
11. Snort
12. НаборМЭ:
    - Avast firewall
    - Avira firewall
    - Comodo firewall
    - DrWeb Security suite
    - Zone Alarm firewall
    - OutPost firewall
    - McAffeTotalSecurity
    - Avg-internet-security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

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 EmBrailleViewPlus;

- 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 лабораторных занятий
- проверка сформированности компетенций ОПК-10,ОПК-12, УК-2

Темы учебной дисциплины предусматривают проведение лабораторных работ, которые служат как целям текущего и промежуточного контроля за подготовкой 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.

Целью лабораторных работ является закрепление теоретического материала и приобретение практических навыковиспользования методов применения пакетов компьютерной математики в профессиональной деятельности, применять навыки для принятия наиболее эффективных решений в условиях быстро меняющейся реальности, для быстрой адаптации к изменяющимся условиям деятельности.
Тематика лабораторных работ соответствует программе курса.

5 семестр

Лабораторная работа 1(10 ч.). Основные сервисы безопасности- проверка сформированности компетенций ОПК-10,ОПК-12, УК-2

Цель работы: получение практических навыков о сервисах безопасности современных продуктов.
Указания по выполнению задания: обратить внимание на базовые механизмы реализации защиты.
Выполнение задания:
В ходе практической работы студенты знакомятся с основными подходами в области реализации сервисов безопасности операционной систем на примере CentOS 7.
Контрольные вопросы:
1. Понятие сервис безопасности.
2. Архитектура реализации сервисов безопасности.
3. Функциональность сервисов безопасности.

Лабораторная работа 2(10 ч.). Средства аутентификации и идентификации ПАСЗИ защиты от НСД- проверка сформированности компетенций ОПК-10,ОПК-12, УК-2
Цель работы: получение практических навыков в разработке и эксплуатации средств аутентификации и идентификации .
Указания по выполнению задания: обратить внимание на прикладные области применения средств защиты программного обеспечения.
Выполнение задания:

В ходе практической работы студенты знакомятся с штатными средствами аутентификации и идентификации.
Контрольные вопросы:
1.Функциихеширования паролей.
2. Политики безопасности и их реализация в современных ОС.
3. Механизмы идентификации пользователей в ПАСЗИ SecretNetStudio.
4. Идентификация пользователей в ПАСЗИ DallasLock.

Лабораторная работа 3(8 ч.). Регистрация событийбезопасности ПАСЗИ защиты от НСД- проверка сформированности компетенций ОПК-10,ОПК-12, УК-2

Цель работы: получение практических навыков в проведении аудита и регистрации событий ИБ.
Указания по выполнению задания: обратить внимание на обязательность требований РД ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей».
Выполнение задания:
В ходе практической работы проводится аудит и анализируются события ИБ на предмет угроз.
Контрольные вопросы:
1. Понятие аудит безопасности
2. Классификация событий ИБ на предмет угроз.
3. Составление отчета о проведенной аудите.
4. Работа с журналами безопасности.
НастройкааудитавПАСЗИDallasLockиSecretNetStudio.

Лабораторная работа 4(8 ч.). Средства контроля целостности ПАЗСИ защиты от НСД- проверка сформированности компетенций ОПК-10,ОПК-12, УК-2

Цель работы: получение практических навыков в исследовании средств контроля целостности.
Указания по выполнению задания: обратить внимание на современные программно-аппаратные средства контроля целостности.
Выполнение задания:
В ходе практической работы студенты приобретают навыки работы со средствами гарантированного удаления информации, знакомятся с принципами контроля целостности ПО.
Контрольные вопросы:
1.Средства доверенной загрузки.
2. Понятие BIOSи механизмы контроля целостности ОС на этапе загрузки.
3. Примеры популярных на рынке решений ПО по контролю целостности.

6 семестр

Лабораторная работа 1 (8 ч.). Исследование траффика с помощью сниффера - проверка сформированности компетенций ОПК-10, ОПК-12, УК-2
Задания:
1. Проанализировать возможные угрозы и атаки на АИС организации.
2. Изучение траффика с помощью WireShark.
Указания по выполнению заданий:
1. Изучить теоритический материал по теме.

2. Ответить на теоритические вопросы в конце лабораторной работы

Лабораторная работа 2 (10 ч.). Исследование методов сетевой фильтрации на примере набора межсетевых экранов ОС Windows- проверка сформированности компетенций ОПК-10, ОПК-12, УК-2
Задания:
1. Настройка и конфигурирование межсетевого экрана для ОС Windows.
2. Создание демилитаризованной зоны.
3. Тестирование функциональности.

Указания по выполнению заданий:
1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Лабораторная работа 3 (8 ч.). Исследование защищенности ОС Linux на примере iptables - проверка сформированности компетенций ОПК10, ОПК-12, УК-2
Задания:
1. Настроить безопасное взаимодействие двух IP-сетей между собой через сеть общего пользования (Интернет), средствами программного продукта OpenVPN.
2. Создать ключи и сертификаты безопасности.
3. Настроить конфигурационный файл VPN-клиента.
4. Настроить iptables.Проверить применение правил фильтрации.

Указания по выполнению заданий:
1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Лабораторная работа 4 (6 ч.). Средство обнаружения вторжения Snort - проверка сформированности компетенций ОПК-10, ОПК-12, УК-2
Задания:
1. Установить систему обнаружения вторжений Snort
2. Настроить Snort под задачи организации.

Указания по выполнению заданий:
1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Приложение 1. Аннотация рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Программно-аппаратные средства защиты информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.
Задачи: изучение основ построения подсистем информационной безопасности, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем.
Дисциплина направлена на формирование следующих компетенций:

- УК-2 – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ОПК-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
- ОПК-12 – Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

В результате освоения дисциплины обучающийся должен:
Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации.
Уметь: осуществлять настройку политики ученых записей, выполнять администрирование учетных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестра,анализировать ограничения вычислительных ресурсов, выбирать оптимальный набор программно-аппаратных ПАСЗИ
Владеть: навыками администрирования подсистем безопасности, настройки системы, политик безопасности, управления учетными записями, навыками использования положений стандартов при разработке, настройке и эксплуатации ПАСЗИ.

По дисциплине предусмотрена промежуточная аттестация в форме зачета (5 семестр) и экзамена (6 семестр).
Общая трудоёмкость освоения дисциплины составляет 4 зачетных единиц.