МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Программно-аппаратные средства защиты информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000EA7C66
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цели дисциплины изучение возможностей применения программно-аппаратных средств в компьютерных сетях для повышения их защищенности; работа в компьютерных вычислительных сетях (ВС) с применением программных средств защиты и использования существующих, встроенных в архитектуру ОС, программно-аппаратных средств.

Задачи дисциплины

- изучение способов создания защищенного сетевого соединения, защищенных протоколов связи, защиты от несанкционированного доступа сообщений электронной почты, сетевых ресурсов
- изучение принципов работы брандмауэров, аппаратных средств предотвращения вторжений, антивирусных программ на основе использования аппаратных средств защиты
- развитие навыков настройки и анализа программных средств защиты, политик безопасности, использования программных отладчиков, сетевых анализаторов

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1к : понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	РД1	Знание	содержание мер по обеспечению информационной безопасности и состав программных и программно-аппаратных средств защиты информации в компьютерных системах и сетях
			РД2	Умение	производить выбор средств обеспечения информационной безопасности для использования их в компьютерных системах и сетях с целью обеспечения требуемого уровня защищенности
		ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного	РД3	Навык	навыками администрирования средств защиты информации и управления процессом реализации комплекса мер по обеспечению

		производства, для решения задач профессиональной деятельности			информационной безопасности на объекте защиты
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации	РД4	Знание	основы формирования политики информационной безопасности
			РД5	Умение	анализировать исходные данные с целью их применения при проектировании подсистем, средств обеспечения защиты информации
			РД6	Навык	навыками администрирования программно-аппаратных средств защиты информации в компьютерных системах и сетях

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Гражданственность	Дисциплинированность
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Гражданственность	Ответственность
Формирование научного мировоззрения и культуры мышления		
Формирование культуры интеллектуального труда и научной этики	Созидательный труд	Мотивированность
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Гражданственность	Ответственность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем».

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Программно-аппаратные средства обеспечения информационной безопасности». На данную дисциплину опираются «Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты», «Производственная преддипломная практика»

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	10	4	70	18	36	0	1	15	74	Э
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	9	4	70	18	36	0	1	15	74	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1 семестр							
1	Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	РД1, РД2, РД3, РД4, РД5, РД6	6	12	0	30	практическое задание

2	Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	РД1, РД2, РД3, РД4, РД5, РД6	6	12	0	30	практическое задание
3	Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	РД1, РД2, РД3, РД4, РД5, РД6	6	12	0	30	практическое задание
2 семестр							
1	Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	РД1, РД2, РД3, РД4, РД5, РД6	4	8	0	21	практическое задание
2	Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	РД1, РД2, РД3, РД5, РД6	4	8	0	23	практическое задание
3	Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	РД1, РД2, РД3, РД5, РД6	4	8	0	23	практическое задание
4	Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	РД1, РД2, РД3, РД5, РД6	6	12	0	23	практическое задание
Итого по таблице			**36**	**72**	**0**	**180**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

1 семестр

Тема 1 Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты.

Содержание темы: Предмет и задачи защиты информации в компьютерных сетях с помощью программно-аппаратных средств, ее взаимосвязь с другими дисциплинами. Краткая история развития. Актуальность защиты компьютерной информации в современном мире. Причины возникновения аппаратных и программных уязвимостей, общие принципы построения систем защиты (triple functions). Понятие политики безопасности и необходимости оценки рисков, критерии, используемые для классификации уровня защищенности (безопасности компьютерных сетей).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.

Содержание темы: Основные понятия, классификация задач, решаемых программно- аппаратными средствами идентификации и аутентификации. Идентификация субъекта с помощью аппаратных средств, понятие протокола идентификации, идентифицирующая информация. Методы аутентификации: парольная схема, биометрический и token способы, многофакторная и взаимная аутентификации. Протоколы идентификации с нулевой передачей знаний. Схемы идентификации Фейге-Фиата-Шамира, Гиллоу-Куискуотера и основные проблемы при их аппаратно-программной реализации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.

Содержание темы: Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа. Иерархический принцип доступа к файлу. Аппаратная защита сетевого файлового ресурса. Программная фиксация доступа к файлам. Дискреционная (разграничительная) модель управления доступом на основе формальной модели Take-Grant и проблемы при ее аппаратной реализации. Способы программно-аппаратной фиксации факта доступа. Надежность систем ограничения доступа. Управление доступом на основе ролей – RBAC. Базовая модель RBAC. Мандатная (представительная) модель управления доступом. Программная реализации мандатной модели доступа. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

2 семестр

Тема 1 Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows.

Содержание темы: Инструменты и методы обеспечения информационной безопасности в среде операционной системы Windows. Основные компоненты локальной политики безопасности, настройка параметров учетных записей, парольная политика, механизм аудита событий, управление правами доступа и группами пользователей.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.

Содержание темы: Теория и практика идентификации и аутентификации пользователей и объектов доступа. Ограничение доступа программ к системным ресурсам. Методы защиты машинных носителей информации (шифрование, контроль доступа, средства защиты от утечек). Принципы и методы регистрации событий безопасности (логирование, аудит). .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации.

Содержание темы: Принципы работы антивирусных программ. Методы обнаружения и нейтрализации вредоносного ПО. Критерии выбора и настройка антивирусных решений. Средства и методы обнаружения вторжений (IDS/IPS). Алгоритмы анализа аномалий и сигнатурный анализ. Режимы работы систем обнаружения вторжений. Методы анализа защищённости (сканирование уязвимостей, Penetration Testing). Регулярный мониторинг безопасности (журналирование событий, анализ логов). Разработка планов реагирования на инциденты.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.

Содержание темы: Обеспечение целостности информационной системы и информации. Обеспечение доступности информации. Защита среды виртуализации. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение

аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Бутин, А. А. Программно-аппаратные средства защиты информации : учебное пособие / А. А. Бутин, Н. И. Глухов, С. И. Носков. — 2-е изд., перераб. и доп. — Иркутск : ИрГУПС, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342113 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

2. Жмуров, Д. Б. Программно-аппаратные средства защиты информации : учебное пособие / Д. Б. Жмуров, С. В. Жуков. — Самара : Самарский университет, 2022. — 80 с. — ISBN 978-5-7883-1799-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336515 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

3. Шевцов, В. Ю. Программно-аппаратная защита локальных АРМ с использованием ПО Secret Net : учебно-методическое пособие / В. Ю. Шевцов, Е. В.

Булгакова. - Москва ; Вологда : Инфра-Инженерия, 2024. - 80 с. - ISBN 978-5-9729-1918-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169714 (Дата обращения - 22.10.2025)

7.2 Дополнительная литература

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, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070 (дата обращения: 15.10.2025).

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

Программное обеспечение:

- Microsoft Office Standard 2007 Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1к : понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства
		ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-2.1к : понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	РД 1	Знание	содержание мер по обеспечению информационной безопасности и состав программных и программно-аппаратных средств защиты информации в компьютерных системах и сетях	решение тестовых заданий
	РД 2	Умение	производить выбор средств обеспечения информационной безопасности для использования их в компьютерных системах и сетях с целью обеспечения требуемого уровня защищенности	выполнение практических заданий

ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД 3	Навык	навыками администрирования средств защиты информации и управления процессом реализации комплекса мер по обеспечению информационной безопасности на объекте защиты	выполнение практических заданий

Компетенция ОПК-9 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации	РД 4	Знание	основы формирования политики информационной безопасности	решение тестовых заданий
	РД 5	Умение	анализировать исходные данные с целью их применения при проектировании подсистем, средств обеспечения защиты информации	выполнение практических заданий
	РД 6	Навык	навыками администрирования программно-аппаратных средств защиты информации в компьютерных системах и сетях	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : содержание мер по обеспечению информационной безопасности и состав программных и программно-аппаратных средств защиты информации в компьютерных системах и сетях	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Тест	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-ап	Тест	Экзамен в устной форме

		паратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация		
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Тест	Экзамен в устной форме
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Тест	Экзамен в устной форме
		2.2. Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	Тест	Экзамен в устной форме
		2.3. Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	Тест	Экзамен в устной форме
		2.4. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	Тест	Экзамен в устной форме
РД2	Умение : производить выбор средств обеспечения информационной безопасности для использования их в компьютерных системах и сетях с целью обеспечения требуемого уровня защищенности	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Практическая работа	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	Практическая работа	Экзамен в устной форме
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их	Практическая работа	Экзамен в устной форме

		влияние на конфигурацию программно-аппаратной части защиты информации.		
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Практическая работа	Экзамен в устной форме
		2.2. Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	Практическая работа	Экзамен в устной форме
		2.3. Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	Практическая работа	Экзамен в устной форме
		2.4. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	Практическая работа	Экзамен в устной форме
РД3	Навык : навыками администрирования средств защиты информации и управления процессом реализации комплекса мер по обеспечению информационной безопасности на объекте защиты	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Практическая работа	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	Практическая работа	Экзамен в устной форме
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Практическая работа	Экзамен в устной форме
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Практическая работа	Экзамен в устной форме

		2.2. Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	Практическая работа	Экзамен в устной форме
		2.3. Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	Практическая работа	Экзамен в устной форме
		2.4. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	Практическая работа	Экзамен в устной форме
РД4	Знание : основы формирования политики информационной безопасности	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Тест	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	Тест	Экзамен в устной форме
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Тест	Экзамен в устной форме
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Тест	Экзамен в устной форме
РД5	Умение : анализировать исходные данные с целью их применения при проектировании подсистем, средств обеспечения защиты информации	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Практическая работа	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутент	Практическая работа	Экзамен в устной форме

		ификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация		
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратной части защиты информации.	Практическая работа	Экзамен в устной форме
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Практическая работа	Экзамен в устной форме
		2.2. Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	Практическая работа	Экзамен в устной форме
		2.3. Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	Практическая работа	Экзамен в устной форме
		2.4. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	Практическая работа	Экзамен в устной форме
РД6	Навык : навыками администрирования программно-аппаратных средств защиты информации в компьютерных системах и сетях	1.1. Архитектура программноаппаратных средств защиты ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты	Практическая работа	Экзамен в устной форме
		1.2. Основные понятия, классификация задач, решаемых программно-аппаратными средствами идентификации и аутентификации. Многофакторная идентификация субъекта, понятие протокола идентификации, идентифицирующая информация	Практическая работа	Экзамен в устной форме
		1.3. Основные аппаратные подходы к защите данных от НСД. Абстрактные модели доступа, их влияние на конфигурацию программно-аппаратн	Практическая работа	Экзамен в устной форме

		ой части защиты информации.		
		2.1. Инструменты обеспечения защиты информации операционных систем. Локальная политика безопасности операционной системы Windows	Практическая работа	Экзамен в устной форме
		2.2. Идентификация и аутентификация субъектов доступа и объектов доступа.Ограничение программной среды. Защита машинных носителей информации. Регистрация событий безопасности.	Практическая работа	Экзамен в устной форме
		2.3. Антивирусная защита. Обнаружение вторжений. Контроль (анализ) защищенности информации	Практическая работа	Экзамен в устной форме
		2.4. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			80
Практические занятия		60		
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным к

		омпетенциям, студент испытывает значительные затруднения при оперировани и знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недос таточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или прак тически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливается _____ (сколько?) классов защищённости государственной информационной системы.

а) 1;
б) 2;
в) 3;
г) 4.

2 Согласно Постановлению Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливается ___ (сколько?) уровней защищённости информационной системы персональных данных.

а) 1;
б) 2;
в) 3;
г) 4.

3 Согласно Постановлению Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» уровень защищенности информационной системы зависит от

а) типа актуальных угроз;
б) масштаба системы;
в) категории персональных данных;
г) типа актуальных угроз и масштаба системы;
д) масштаба системы и категории персональных данных;
е) типа актуальных угроз и категории персональных данных.

4 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» класс защищенности информационной системы зависит от

а) уровня значимости информации;
б) масштаба системы;
в) уровня значимости информации и масштаба системы;
г) уровня значимости информации и категории персональных данных.

5 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливается ___ (сколько?) степеней возможного ущерба.

а) 1;
б) 2;
в) 3;
г) 4.

1 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет высокий уровень значимости (УЗ 1), если

а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

8 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет средний уровень значимости (УЗ 2), если

а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

9 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» информация имеет низкий уровень значимости (УЗ 3), если

а) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба;

б) хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;

в) для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

10 Согласно приказу ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» при обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) а) определятся отдельно для каждого вида информации;

в) является единым для всех. определены низкие степени ущерба.

11 Какое из перечисленных средств защиты информации не обеспечивает защиту от несанкционированного доступа

а) Secret Net Studio;

б) Dallas Lock;

в) Dr. Web.

12. Что такое антивирусная программа?

А)Программа для архивации данных

б) Средство защиты от вредоносного ПО

в) Сервис для синхронизации данных

г) Приложение для шифрования информации

13. Как называется метод обнаружения вторжений, использующий сигнатуру известных атак?

А)Сигнатурный анализ

б) Аналитический анализ

в) Логический анализ

г) Функциональный анализ

14. Что значит «Penetration Testing»?

А) Атака методом грубой силы

б) Авторизация в системе

в) Имитация кибератаки для проверки безопасности

г) Распространение вируса

15. Какие функции выполняют системы обнаружения вторжений (IDS)?

А) Обнаруживают попытки вторжения и предупреждают о них

б) Осуществляют мониторинг интернет-трафика

в) Кодируют данные для защиты

г) Поддерживают стабильность сети

16. Какая из указанных систем занимается активным отпугиванием и остановкой атакующих?

А)SIEM

б) IDS

в) IPS

г) WAF

17. Какой метод анализа безопасности подразумевает постоянное наблюдение за поведением пользователей и программ?

А)Журналирование событий

б) Проактивный анализ

в) Активный мониторинг

г) Аномалии поведения

18. Как называются системы, предназначенные для анализа логов и выявления инцидентов безопасности?

А)Antivirus systems

б) Intrusion Detection Systems

в) Security Information and Event Management (SIEM)

г) Data Loss Prevention (DLP)

19. Какая задача решается при помощи анализа защищённости информации?

А)Очистка жёсткого диска от мусора

б) Обновление драйверов устройств

в) Оценка уровня защиты информационных систем

г) Увеличение быстродействия компьютеров

20. Что такое уязвимость информационной системы?

А)Открытость системы для внешнего мира

б) Прогрессирующая атака хакера

в) Ошибка или недостаток, позволяющий осуществить атаку

г) Высокая производительность системы

21. Как называется средство защиты, предназначенное для анализа входящих и исходящих данных и защиты от атак на уровне приложений?

А)Web Application Firewall (WAF)

б) Network Firewall

в) Virtual Private Network (VPN)

г) Domain Name System (DNS)

22. Что такое шпионское ПО (spyware)?

А)Специальное ПО для сбора секретной информации о пользователе

б) Антивирусная программа

в) Бесплатное приложение для просмотра фильмов

г) Программу для редактирования фотографий

23. Какие действия предпринимает система предотвращения вторжений (IPS) при обнаружении атаки?

А)Блокирует атакующего и уведомляет администратора

б) Отправляет уведомление пользователю сайта

в) Передаёт файлы на сервер для архивации

г) Просто регистрирует попытку атаки

24. Какой тип анализа основан на сравнении текущих событий с известными моделями атак?

А)Семантический анализ

б) Аналитический анализ

в) Профилирующий анализ

г) Сигнатурный анализ

25. Что подразумевается под категорией "Threat Intelligence"?

А)Искусственный интеллект

б) Информация о киберугрозах и методах борьбы с ними

в) Заранее установленный шаблон сообщений

г) Устройство для усиления сигнала Wi-Fi

26. Какой термин характеризует процедуру автоматического уведомления администратора о нарушениях политики безопасности?

А)Alerting system

б) Debugging process

в) Backup mechanism

г) Archiving protocol

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Вопросы к экзамену

1. Что такое администрирование средств защиты информации?

2. Какие основные задачи выполняет администратор средств защиты информации?

3. Какие типы угроз информационной безопасности могут возникнуть в компьютерных системах и сетях?

4. Что такое аутентификация и почему она важна для обеспечения безопасности?

5. Какие методы аутентификации можно использовать?

6. Что такое авторизация и как она связана с аутентификацией?

7. Какие методы авторизации можно использовать?

8. Что такое шифрование и как оно помогает защитить информацию?

9. Какие алгоритмы шифрования широко используются в сетях?

10. Что такое брандмауэр и как он обеспечивает безопасность сети?

11. Какие типы брандмауэров существуют?

12. Какие функции выполняет брандмауэр?

13. Какие методы обнаружения вторжений (IDS) существуют?

14. Как IDS помогает обнаружить и предотвратить атаки на сеть?

15. Что такое вирус и какие методы защиты от них существуют?

16. Какие типы вредоносных программ существуют?

17. Какие методы обнаружения и удаления вредоносных программ существуют?

18. Что такое антивирусное программное обеспечение и как оно работает?

19. Какие методы обнаружения и предотвращения DDoS-атак существуют?

20. Что такое VPN и как оно помогает обеспечить безопасность соединения?

21. Какие типы VPN-соединений существуют?

22. Какие методы защиты от перехвата данных существуют?

23. Что такое аудит безопасности и почему он важен?

24. Какие инструменты аудита безопасности можно использовать?

25. Что такое политика безопасности и как она помогает обеспечить безопасность информации?

26. Какие основные элементы политики безопасности существуют?

27. Какие методы резервного копирования данных существуют?

28. Что такое фильтрация содержимого и как она помогает обеспечить безопасность информации?

29. Какие методы фильтрации содержимого существуют?

30. Что такое многофакторная аутентификация и как она помогает обеспечить безопасность?

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.

5.3 Примеры заданий для выполнения практических работ

I. Средства защиты Dallas Lock 8.0

Практическая работа №1. Настройка управления доступом к файлам и папкам

Цель: научиться устанавливать и проверять права доступа к файлам и папкам средствами Dallas Lock.

Ход работы:

1. Создать несколько пользователей с различным уровнем доступа.
2. Настроить индивидуальные права доступа к общим папкам и файлам.
3. Проверить, как работают права доступа, пытаясь изменить или удалить файлы с разных аккаунтов.
4. Оформить отчёт с результатами экспериментов и выводами.

Практическая работа №2. Методы шифрования данных

Цель: исследовать механизмы шифрования и расшифровки файлов и папок.

Ход работы:

1. Создать зашифрованный файл-контейнер и поместить туда важные данные.
2. Попробовать скопировать и перенести файл-контейнер на другую машину.
3. Провести восстановление данных из контейнера на целевой машине.
4. Сделать выводы о надёжности и простоте метода шифрования.

Практическая работа №3. Контроль целостности файлов и программ

Цель: настроить проверку целостности файлов и увидеть поведение системы при нарушении целостности.

Ход работы:

1. Настроить регулярную проверку целостности определённых файлов и программ.
2. Искусственно изменить один из проверенных файлов и проанализировать реакции системы.
3. Исправить нарушение целостности и повторить эксперимент.
4. Составить отчёт о ходе эксперимента и рекомендациях по применению механизма.

Практическая работа №4. Защита от несанкционированного доступа к носителям

Цель: применить методику защиты от использования внешних устройств.

Ход работы:

1. Настроить запрет на использование внешних носителей (USB, CD/DVD).
2. Проверить реакцию системы при попытках подключения и использования запрещённых устройств.
3. Настроить исключение для конкретного внешнего устройства.
4. Подготовить рекомендации по безопасной работе с устройствами хранения.

II. Средства защиты Secret Net Studio

Практическая работа №1. Управление полноформочным доступом

Цель: разобраться в практике разграничения доступа к конфиденциальным данным.

Ход работы:

1. Организовать разграничение доступа пользователей к файлам и папкам с разной степенью конфиденциальности.
2. Назначить каждому пользователю уровень допуска и попробовать получить доступ к защищённым файлам.
3. Исследовать механизм полной запретки потока данных между объектами разного уровня конфиденциальности.
4. Представить отчёт с выводами и оценкой полезности данного инструмента.

Практическая работа №2. Контроль целостности системы

Цель: познакомиться с механизмом контроля целостности и его эффективностью.

Ход работы:

1. Настроить расписание проверок целостности системы и определить частоту проверок.
2. Модифицировать тестовый файл и посмотреть, как среагирует система.
3. Посмотреть событие нарушения целостности в журнале системы.
4. Выводы о целесообразности регулярного контроля целостности.

Практическая работа №3. Теневое копирование и маркировка документов

Цель: реализовать процессы резервного копирования и маркировки документов.

Ход работы:

1. Настроить теневое копирование файлов на внешние носители.
2. Автоматически маркировать отпечатанные документы соответствующими грифами конфиденциальности.
3. Проверить эффективность обеих процедур на реальных примерах.

4. Написать отчёт с рекомендациями по улучшению процесса.

Практическая работа №4. Закрытая программная среда
Цель: организовать закрытый круг разрешённых программ.
Ход работы:

1. Определить перечень разрешённых приложений для сотрудников.
2. Настроить среду таким образом, чтобы остальные программы не могли быть запущены.
3. Проверить функциональность системы при различных ситуациях (попытка запуска сторонних программ, обновление существующих приложений).
4. Предоставить отчёт с пояснением принципов работы закрытой программной среды.

III. Средства защиты Astra Linux SE
Практическая работа №1. Базовая настройка идентификации и аутентификации
Цель: изучить основы работы с инструментами аутентификации в Astra Linux SE.
Ход работы:

1. Настроить двухфакторную аутентификацию для одного пользователя.
2. Продемонстрировать случаи успешной и неуспешной аутентификации.
3. Рассмотреть преимущества и недостатки предложенного способа аутентификации.
4. Составить итоговый отчёт с подробным описанием проделанной работы.

Практическая работа №2. Организационные аспекты мандатного разграничения доступа
Цель: выяснить, как работает мандатное разграничение доступа в Astra Linux SE.
Ход работы:

1. Присвоить пользователям уровни конфиденциальности и наблюдать последствия попыток доступа к файлам.
2. Изучить различия между дискреционным и мандатным способами разграничения доступа.
3. Понять, почему мандатное разграничение эффективнее против внутренних угроз.
4. Итоговый отчёт с выявленными особенностями.

Практическая работа №3. Поддержка протоколов и регулирование работы сети
Цель: внедрить и испытать сетевую защиту на Astra Linux SE.
Ход работы:

1. Настроить фильтрацию пакетов и контроль за передачей данных по сети.
2. Осуществить передачу данных внутри сети и зафиксировать события фильтрации.
3. Проанализировать статистику пропускания данных и оценить качество работы защитного механизма.
4. Оформить отчёт с заключениями и рекомендациями.

Практическая работа №4. Замкнутая программная среда
Цель: реализовать ограничительную политику относительно используемых программ.
Ход работы:

1. Выделить одобренные программы и исключить возможность запуска иных приложений.
2. Проверить реакцию системы на попытки запуска запрещённых программ.
3. Произвести эксперименты по модификации существующих программ и обновить их в рамках разрешённых условий.
4. Завершить исследование созданием отчёта с обсуждением результатов и выводов.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.