МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ЗАЩИТА ПРОГРАММ И ДАННЫХ

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

Год набора на ОПОП
2025

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Защита программ и данных» 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	0000000000E9896C
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Защита программ и данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой программ и данных; формирование у обучаемых профессиональных компетенций в эксплуатационно технической и научно-исследовательской областях профессиональной деятельности в соответствии с ОП специальности 10.05.03 - «Информационная безопасность автоматизированных систем».

Задачи дисциплины «Защита программ и данных» - обеспечить освоение:

- основных принципов анализа ПО; - основ низкоуровневого программирования;
- принципов низкоуровневой отладки и исследован

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)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности	РД4	Знание	особенности построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы и особенности их эксплуатации
			РД5	Умение	настраивать системы обеспечения безопасности, анализировать их работу; проектировать построение системы безопасности в рамках информационной системы
			РД6	Знание	методикой управления и модернизация подсистем безопасности; навыками организации работы по разработке, эксплуатации и внедрению автоматизированной системы с учетом

					требований информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах	РД1	Знание	основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; особенности построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы
			РД2	Умение	обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; проектировать построение системы безопасности в рамках информационной системы; проводить контрольные проверки работоспособности применяемых программных средств защиты информации
			РД3	Навык	определения необходимого облика защищаемой системы

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		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Внимательность к деталям

Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Взаимопомощь и взаимоуважение	Активная жизненная позиция
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Взаимопомощь и взаимоуважение	Дисциплинированность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Служение Отечеству и ответственность за его судьбу	Внимательность к деталям

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится к части, формируемая участниками образовательных отношений и опирется на дисциплины: Программно-аппаратные средства обеспечения информационной безопасности и необходима для прохождения Производственная профессиональная 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.В	9	4	83	36	36	0	1	10	61	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		Кол-во часов, отведенное на	Форма

		Код результата обучения	Лек	Практ	Лаб	СРС	текущего контроля
1	Анализ программных реализаций, защита программ от анализа	РД1, РД2, РД3, РД4, РД5	2	4	0	15	отчет по практической работе, собеседование
2	Особенности анализа некоторых видов программ	РД1, РД2, РД3, РД4, РД5	8	4	0	14	отчет по практической работе, собеседование
3	Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	РД1, РД2, РД3, РД4, РД5	8	4	0	14	отчет по практической работе, собеседование
4	Методы внедрения и выявления программных закладок	РД1, РД2, РД3, РД4, РД5	8	4	0	14	отчет по практической работе, собеседование
5	Компьютерные вирусы как особый класс программных закладок	РД1, РД2, РД3, РД4, РД5	10	20	0	14	отчет по практической работе, собеседование
Итого по таблице			**36**	**36**	**0**	**71**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Анализ программных реализаций, защита программ от анализа .

Содержание темы: Введение в «защиту программ и данных». Основные термины и понятия. Метод экспериментов с «черным ящиком». Статический метод. Динамический метод. Программные отладочные средства. Методика изучения программ динамическим методом. Метод маяков. Метод Step-Trace первого этапа. Метод аппаратной точки останова. Метод Step-Trace второго этапа. Знакомство с дизассемблером IDA. Знакомство с отладчиками режима пользователя. Освоение статического и динамического методов на простых примерах.

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 Особенности анализа некоторых видов программ .

Содержание темы: Особенности анализа оверлейных программ. Особенности анализа графических программ Windows. Пример анализа графической программы Windows. Особенности анализа параллельного кода. Особенности анализа кода в режиме ядра Windows. Вспомогательные инструменты анализа программ. Монитор активности процессов ProcMon. Утилита управления процессами Process Explorer. Защита программ от анализа. Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение. Динамическое изменение кода программы. Искусственное усложнение структуры программы. Нестандартные обращения к функциям операционной системы. Искусственное усложнение алгоритмов обработки данных. Выявление факта выполнения программы под отладчиком. Методы обфускации запутывания программного кода). Создание простой системы защиты программного кода от анализа. Знакомство с методами преодоления защиты программного кода от анализа. Программирование алгоритмов обфускации.

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 Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам.

Содержание темы: Понятие программной закладки. Классификация программных закладок. Субъектно-ориентированная модель компьютерной системы. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. Знакомство с программными закладками. Построение политики безопасности, обеспечивающей высокую защищенность от программных закладок Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя. Несанкционированное использование средств динамического изменения полномочий. Порождение дочернего процесса системным процессом. Модификация машинного кода монитора безопасности объектов. Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. Переполнения буферов. Отсутствие необходимых проверок входных данных. GetAdmin. Уязвимость %00. Некорректный контекст безопасности. AdminTrap. Системные окна на рабочем столе пользователя. Устаревшие функции. NetDDE Exploit. WMF Exploit (MS06-001). Другие уязвимости. Уязвимость program.exe. Отсутствие необходимых проверок входных данных: GetAdmin, Уязвимость %00. Некорректный контекст безопасности: AdminTrap, системные окна на рабочем столе пользователя. Устаревшие функции: NetDDE Exploit, WMF Exploit (MS06-001). Уязвимость program.exe.

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 Методы внедрения и выявления программных закладок.

Содержание темы: Маскировка программной закладки под прикладное программное обеспечение. Маскировка программной закладки под системное программное обеспечение. Подмена системного программного обеспечения. Прямое ассоциирование. Косвенное ассоциирование. Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Принципы построения поли. Настройка и использование специализированного антивирусного программного обеспечения. Изолированная программная среда и программные ловушки. Локализация и пресечение вирусных атак. Программирование и внедрение закладок.

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

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

Тема 5 Компьютерные вирусы как особый класс программных закладок.

Содержание темы: Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML. вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии,

полиморфные преобразования кода. Средства и методы защиты от программных закладок. Сканирование системы на предмет наличия известных программных закладок. Контроль целостности программного обеспечения. Контроль целостности конфигурации защищаемой системы. Антивирусный мониторинг информационных потоков. Программные ловушки. Организационные и административные меры антивирусной защиты. Инструктирование пользователей. Просмотр и анализ данных регистрации и мониторинга. Контроль качества аутентификационных данных пользователей. Регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной защиты сети, в случае успешных вирусных атак. Регулярные инспекции состояния антивирусной защиты. Выявление программных закладок в ручном режиме.

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. Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 настоящей РПД. Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 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. Агальцов, В. П. Базы данных : учебник : в 2 книгах. Книга 1. Локальные базы данных / В.П. Агальцов. — Москва : ФОРУМ : ИНФРА-М, 2025. — 352 с. : ил. — (Высшее образование). - ISBN 978-5-8199-0377-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2162084 (Дата обращения - 05.09.2025)
2. Современные технологии сбора информации : учебное пособие для обучающихся специальности 10.05.01 «Компьютерная безопасность», направлений подготовки 27.03.04 «Управление в технических системах», 27.04.04 «Управление в технических системах» / Д. М. Кирюхин, Е. П. Ляпина, Д. А. Меркулов, В. Г. Сидоренко. - Москва : РУТ (МИИТ), 2023. - 56 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2135308 (Дата обращения - 05.09.2025)
3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016533-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1178148 (Дата обращения - 05.09.2025)

7.2 Дополнительная литература

1. Сидорова, Н. П. Информационное обеспечение и базы данных : практикум по дисциплине «Информационное обеспечение, базы данных» : учебное пособие / Н. П. Сидорова. — Королёв : МГОТУ, 2019. — 84 с. — ISBN 978-5-4475-9996-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149444 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.
2. Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

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

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

Программное обеспечение:

- Kaspersky
- Microsoft Office 2003 Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ЗАЩИТА ПРОГРАММ И ДАННЫХ

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

Год набора на ОПОП
2025

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)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах

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 ПКВ-1 «Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации»

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	
ПКВ-1.1к : идентифицирует бизнес-процессы происходящие в организации, определяет возможные угрозы информационной безопасности	РД 4	Знание	особенности построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы и особенности их эксплуатации	решение тестовых заданий
	РД 5	Умение	настраивать системы обеспечения безопасности, анализировать их работу; проектировать построение системы безопасности в рамках информационной системы	выполнение практических заданий
	РД 6	Знание	методикой управления и модернизация подсистем безопасности; навыками организации работы по разработке, эксплуатации и внедрению автоматизированной системы с учетом требований информационной безопасности	выполнение практических заданий

Компетенция ПКВ-2 «Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.»

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	
ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах	РД 1	Знание	основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; особенности и построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы	корректное применение полученных знаний при решении практических задач
	РД 2	Умение	обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; проектировать построение системы безопасности в рамках информационной системы; проводить контрольные проверки работоспособности применяемых программных средств защиты информации	выполнение практических заданий
	РД 3	Навык	определения необходимого облика защищаемой системы	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 : основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;	1.1. Анализ программных реализаций, защита программ от анализа	Тест	Опрос
		1.2. Особенности анализа некоторых видов программ	Тест	Опрос

	особенности построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы	1.3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	Тест	Опрос
		1.4. Методы внедрения и выявления программных закладок	Тест	Опрос
		1.5. Компьютерные вирусы как особый класс программных закладок	Тест	Опрос
РД2	Умение : обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; проектировать построение системы безопасности в рамках информационной системы; проводить контрольные проверки работоспособности применяемых программных средств защиты информации	1.1. Анализ программных реализаций, защита программ от анализа	Практическая работа	Опрос
		1.2. Особенности анализа некоторых видов программ	Практическая работа	Опрос
		1.3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	Практическая работа	Опрос
		1.4. Методы внедрения и выявления программных закладок	Практическая работа	Опрос
		1.5. Компьютерные вирусы как особый класс программных закладок	Практическая работа	Опрос
РД3	Навык : определения необходимого облика защищаемой системы	1.1. Анализ программных реализаций, защита программ от анализа	Практическая работа	Опрос
		1.2. Особенности анализа некоторых видов программ	Практическая работа	Опрос
		1.3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	Практическая работа	Опрос
		1.4. Методы внедрения и выявления программных закладок	Практическая работа	Опрос
		1.5. Компьютерные вирусы как особый класс программных закладок	Практическая работа	Опрос
РД4	Знание : особенности построения и функционирования основных видов систем обеспечения безопасности, их место в инфраструктуре информационной системы и особенности их эксплуатации	1.1. Анализ программных реализаций, защита программ от анализа	Тест	Опрос
		1.2. Особенности анализа некоторых видов программ	Тест	Опрос
		1.3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	Тест	Опрос
		1.4. Методы внедрения и выявления программных закладок	Тест	Опрос

		1.5. Компьютерные вирусы как особый класс программных закладок	Тест	Опрос
РД5	Умение : настраивать системы обеспечения безопасности, анализировать их работу; проектировать построение системы безопасности в рамках информационной системы	1.1. Анализ программных реализаций, защита программ от анализа	Практическая работа	Опрос
		1.2. Особенности анализа некоторых видов программ	Практическая работа	Опрос
		1.3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам	Практическая работа	Опрос
		1.4. Методы внедрения и выявления программных закладок	Практическая работа	Опрос
		1.5. Компьютерные вирусы как особый класс программных закладок	Практическая работа	Опрос

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	Практическое занятие	Экзамен	Итого
Лекционные занятия	20			20
Практическое занятие		60		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 компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» /	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

	«неудовлетворительно»	

5 Примерные оценочные средства

5.1 Контрольный тест

1. Кто является основным ответственным за определение уровня классификации информации?

А) Руководитель среднего звена

Б) Высшее руководство

В) Владелец

Г) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

А) Сотрудники

Б) Хакеры

В) Атакующие

Г) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

А) Снизить уровень безопасности этой информации для обеспечения её доступности и удобства использования

Б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

В) Улучшить контроль за безопасностью этой информации

Г) Снизить уровень классификации этой информации

4. Какая из приведённых техник является самой важной при выборе конкретных защитных мер?

А) Анализ рисков

Б) Анализ затрат / выгоды

В) Результаты ALE

Г) Выявление уязвимостей и угроз, являющихся причиной риска

5. Что лучше всего описывает цель расчёта ALE?

А) Количественно оценить уровень безопасности среды

Б) Оценить возможные потери для каждой контрмеры

В) Количественно оценить затраты / выгоды

Г) Оценить потенциальные потери от угрозы в год

6. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

А) Поддержка

Б) Выполнение анализа рисков

В) Определение цели и границ

Г) Делегирование полномочий

7. Что такое COBIT и как он относится к разработке систем информационной безопасности и программ безопасности?

А) Список стандартов, процедур и политик для разработки программы безопасности

Б) Текущая версия ISO 17799

В) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

Г) Открытый стандарт, определяющий цели контроля

8. Защита информации от утечки — это деятельность по предотвращению:

А) Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовых документов или собственником, владельцем информации прав или правил доступа к защищаемой информации

Б) Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокировке доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

В) Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений

Г) Неконтролируемого распространения защищаемой информации от её разглашения, несанкционированного доступа

Д) Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации

9. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путём подсчёта и сравнения с эталоном контрольной суммы:

А) Детектор

Б) Доктор

В) Сканер

Г) Ревизор

Д) Сторож

10. Антивирус не только находит заражённые вирусами файлы, но и "лечит" их, то есть удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

А) Детектор

Б) Доктор

В) Сканер

Г) Ревизор

Д) Сторож

11. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

А) Детектор

Б) Доктор

В) Сканер

Г) Ревизор

Д) Сторож

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.

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 Примерные вопросы

1. В чем заключается опасность программных закладок?
2. Какие программные закладки вы знаете?
3. Что такое информационный поток?

4. Как в рамках субъектно-ориентированной модели описывается операция порождения нового субъекта доступа?
5. Какими двумя причинами может вызываться НСД в рамках субъектноориентированной модели?
6. Что такое программная закладка?
7. Какие модели взаимодействия программной закладки с атакуемой системой вы знаете?
8. Как формально определяется модель «наблюдатель»?
9. Для чего чаще всего применяются программные закладки модели «наблюдатель»?
10. Каковы типичные недостатки программных закладок модели «наблюдатель»?
11. Как программные закладки модели «наблюдатель» обычно обеспечивают свою повторную активизацию после перезагрузки атакованной операционной системы?
12. Как выглядит общая схема взаимодействия клиентской и серверной частей программной закладки модели «наблюдатель»?
13. Какие преимущества дает программной закладке модели «наблюдатель» модульная архитектура?
14. Как формально определяется модель «перехват»?
15. Как устроены перехватчики паролей первого рода?
16. Как устроены перехватчики паролей второго рода?
17. Как устроены перехватчики паролей третьего рода?
18. Как устроены мониторы файловых систем?
19. Как устроены мониторы сети?
20. Как формально определяется модель «уборка мусора»?
21. Как формально определяется модель «искажение»?

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

Практическое задание №1: Проектирование системы защиты конфиденциальных данных

Цель задания: разработать систему управления правами доступа к конфиденциальной информации в организации.

Задания:

Определите классификацию данных в вашей организации согласно уровню конфиденциальности.

Разработайте матрицу доступа для разных ролей сотрудников, включая уровни доступа к документам и ресурсам.

Предложите механизм аудита и мониторинга доступа к данным.

Подготовьте инструкцию по действиям в случае инцидента безопасности.

Результат: презентация модели системы защиты и отчет с описанием механизмов реализации.

Практическое задание №2: Обзор антивирусных решений

Цель задания: провести сравнительный анализ популярных антивирусных продуктов и выбрать оптимальное решение для конкретного типа организаций.

Задания:

Исследуйте рынок современных антивирусных программ (Kaspersky, Dr.Web, ESET NOD32).

Проведите тестирование выбранных антивирусов на виртуальной машине с использованием тестовых вредоносных файлов.

Составьте таблицу сравнения по критериям: эффективность, производительность, стоимость лицензии, удобство интерфейса.

Сделайте вывод о лучшем продукте исходя из ваших потребностей.

Результат: таблица сравнения и письменный отчёт с выводами.

Практическое задание №3: Шифрование данных

Цель задания: научиться применять криптографические методы для защиты данных.

Задания:

Создать зашифрованный архив методом симметричного шифрования AES-256.

Реализовать процесс дешифровки архива с использованием ключа.

Проверить целостность зашифрованных данных с помощью цифровых подписей.

Продемонстрировать работу сценария на примерах реальных файлов.

Результат: демонстрационный сценарий шифрования-дешифрации и отчет с инструкциями.

Практическое задание №4: Разработка защитного механизма программного продукта

Цель задания: создать приложение с элементами защиты от взлома и модификации.

Задания:

Напишите простое приложение на Python или JavaScript с базовым функционалом (например, калькулятор).

Добавьте механизмы защиты приложения: хэширование важных компонентов, проверку целостности исполняемого файла.

Покажите процедуру обхода разработанных вами защитных механизмов.

Опишите способы повышения устойчивости вашего приложения против атак.

Результат: рабочий прототип приложения с защитой и доклад с результатами тестирования.

Практическое задание №5: Моделирование атаки на веб-приложение

Цель задания: изучить типы уязвимостей веб-приложений и разработать меры противодействия.

Задания:

Выберите популярное веб-приложение с открытым кодом (например, WordPress).

Найдите и продемонстрируйте SQL-инъекции, XSS-уязвимости, межсайтовое выполнение скриптов.

Настройте WAF (Web Application Firewall) для предотвращения выявленных атак.

Докажите работоспособность защиты с помощью повторного тестирования.

Результат: подробный отчёт с описаниями найденных уязвимостей и способов защиты.

Краткие методические указания

Для успешного выполнения практических работ студенты должны последовательно пройти этапы проектирования, анализа, тестирования и документирования результатов. Рекомендуется использование специализированных инструментов и технологий (антивирусные продукты, средства шифрования, инструменты анализа уязвимостей).

Итоговые отчёты должны содержать четкое изложение целей, выполненных этапов, полученные результаты и выводы по каждому заданию. Особое внимание уделяется самостоятельному исследованию рынка решений и выбору оптимальных подходов для конкретной ситуации.

Шкала оценки

Оценка	Баллы	Описание
5	45-60	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	30-44	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	14-29	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-13	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.