КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине программно-аппаратные средства защиты информации

обсуждены и рекомендованы к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрены Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Паспорт оценочных материалов по дисциплине «Программно-аппаратные средства защиты информации»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1 Применяет знания основных уязвимостей программного обеспечения при разработке компонент программных и программно-аппаратных средств защиты информации в компьютерных системах	Знает: основные программные компоненты КЗИ и их назначение, принципы работы аппаратных компонентов КЗИ, особенности реализации политики ИБ, принципы защиты от основных угроз. Умеет: настраивать основные компоненты программно-аппаратных КЗИ, проводить плановые мероприятия по обслуживанию аппаратных компонент КЗИ, выполнять настройку политики ИБ. Владеет: навыками решения типовых задач ИБ на программно-аппаратных КСЗ, опытом оценки качества работы аппаратных средств защиты.	Тема 1. Введение. Общие вопросы ОБИ и дисциплины ПАСЗИ. Тема 2. Защита от РПВ (ПМВ).	1. Тематика рефератов (тема 1) 2.Лабораторная работа (Тема 1) 3. Тестовые задания для текущего контроля (вопросы 1-8) 1. Тематика рефератов (тема 2) 2.Лабораторная работа (Тема 2) 3. Тестовые задания для текущего контроля (вопросы 9-16)	1. Тестовые задания для проведения промежуточный аттестации №1-5,9 2. Вопросы к зачету 1-5 1. Тестовые задания для проведения промежуточный аттестации №6-8,10 2. Вопросы к зачету 6-10

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
			Тема 3. Защита данных.	1. Тематика рефератов (тема 3) 2.Лабораторная работа (Тема 3) 3.Тестовые задания для текущего (вопросы 16-21)	1. Тестовые задания для проведения промежуточный аттестации №11-13 2. Вопросы к зачету 11-16
	ОПК-13.3 Демонстрирует умение проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах	Знает: принципы анализа защищенности КСЗ. Умеет: собирать и анализировать данные, предоставляемые КЗИ об угрозах и уязвимостях ИС. расходами на ИТ предприятия; Владеет: практическим опытом оценки качества работы и выбора подходящих средств защиты.	Тема 4. Защита программ.	1. Тематика рефератов (тема 4) 2.Лабораторная работа (Тема 4) 3.Тестовые задания для текущего (вопросы 22-26)	1. Тестовые задания для проведения промежуточный аттестации №14-18, 20,21 2. Вопросы к зачету 17-21
			Тема 5. Программные и программно-технические средства обеспечения безопасности.	1. Тематика рефератов (тема 5) 2.Лабораторная работа (Тема 5) 3.Тестовые задания для текущего (вопросы 27-30)	1. Тестовые задания для проведения промежуточный аттестации №19, 22-24 2. Вопросы к зачету 22-25

2. Оценочные материалы по дисциплине «Программно-аппаратные средства защиты информации»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Введение. Общие вопросы обеспечения безопасности информации и дисциплины ПАСЗИ

1. Эволюция угроз информационной безопасности и развитие программно-аппаратных средств защиты
2. Взаимосвязь понятий: защищенность, уязвимость, угроза, нарушитель в современных компьютерных системах
3. Анализ рисков информационной безопасности и место ПАСЗИ в системе управления рисками
4. Сравнительный анализ технических и программно-аппаратных средств защиты информации
5. Основные каналы утечки информации в компьютерных системах и методы их блокирования
6. Нормативно-правовая база применения программно-аппаратных средств защиты информации
7. Принципы построения комплексных систем защиты информации на предприятии
8. Современные тенденции развития программно-аппаратных комплексов защиты информации

Тема 2. Защита от вредоносного программного обеспечения (РПВ)

1. Классификация современных программных закладок и методы их обнаружения
2. Анализ методов работы троянов и утилит скрытого администрирования
3. Технологии руткитов уровня ядра и пользователя: принципы работы и методы противодействия
4. Современные антивирусные технологии: от сигнатурного анализа к поведенческому анализу
5. Системы предотвращения вторжений (IPS) и их место в защите от РПВ
6. Технологии песочницы (sandboxing) для анализа подозрительных программ
7. Защита от сетевых червей и почтовых вирусов в корпоративных сетях
8. Угрозы информационной безопасности мобильных устройств и методы защиты
9. Принципы работы белых и черных списков (Whitelisting/Blacklisting) в современных ОС
10. Методы внедрения вредоносного ПО через автозагрузку Windows и способы защиты

Тема 3. Защита данных

1. Современные системы резервного копирования: от Acronis до облачных решений
2. Технологии восстановления данных после сбоев и атак
3. DLP-системы: архитектура, принципы работы и практическое применение
4. Сравнительный анализ хостовых и шлюзовых DLP-систем
5. Методы и средства криптографической защиты данных
6. Технологии гарантированного уничтожения конфиденциальной информации
7. Системы контроля целостности программ и данных в реальном времени
8. Защита от утечки данных через внешние носители и порты компьютера
9. Использование RAID-массивов для обеспечения отказоустойчивости и защиты данных

10 Программные средства анализа остаточной информации на носителях

Тема 4. Защита программного обеспечения

1. Методы защиты программ от несанкционированного копирования и распространения
2. Технологии обфускации кода как метод защиты от реверс-инжиниринга
3. Электронные ключи защиты: от аппаратных dongle до программных лицензий
4. Системы защиты от отладки и дизассемблирования
5. Методы привязки программного обеспечения к уникальным характеристикам оборудования
6. Защита с помощью регистрационных кодов: алгоритмы и уязвимости
7. Современные протекторы программного обеспечения: ASProtect, Themida, VMProtect
8. Технологии защиты от модификации исполняемых файлов
9. Методы противодействия взлому программного обеспечения

Тема 5. Программные и программно-технические средства обеспечения безопасности

1. Аппаратные модули доверенной загрузки: принципы работы и практическое применение
2. Средства безопасной аутентификации: от RuToken до биометрических систем
3. Комплексные системы защиты информации SecretNet Studio: архитектура и возможности
4. Программные средства анализа защищенности сетей и компьютеров
5. Системы управления ключевой информацией и сертификатами
6. Средства защиты от несанкционированного доступа в корпоративных сетях
7. Технологии безопасного удаленного доступа и VPN
8. Системы обнаружения и предотвращения вторжений (IDS/IPS)
9. Средства защиты веб-приложений и сервисов

Критерии оценки выполнения рефератов по учебной дисциплине

Оценка «отлично» выставляется студенту, если тема реферата раскрыта в полной мере и все требования по написанию реферата соблюдены.

Оценка «хорошо» выставляется студенту, если недостаточно раскрыта тема реферата, но все требования по написанию реферата соблюдены.

Оценка «удовлетворительно» выставляется студенту, если недостаточно раскрыта тема реферата, не все требования по написанию реферата соблюдены, присутствуют ошибки и неточности в работе.

Оценка «неудовлетворительно» выставляется студенту, если отсутствует реферат.

Рекомендации по написанию реферата:

Реферат — письменная работа, выполняемая обучающимся в течение определенного срока.

Реферат — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях). Реферат — не механический пересказ работы, а изложение ее существа.

Кроме реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата предлагает преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.

2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.

4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.

5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.

6. Приложение может включать графики, таблицы, расчеты.

7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;

2. Изложение результатов изучения в виде связного текста;

3. Устное сообщение по теме реферата.

1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся

с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями.

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и фиксируют устойчивые и несомненные суждения. В текстах-рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, - т. е. выявляется

практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать, и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение.

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемыек оформлению реферата

Объемы рефератов – от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,

– дословное переписывание книг, статей, заимствования рефератов из интернета и т. д.

При проверке реферата преподавателем оцениваются:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество и ценность полученных результатов (степень завершенности

реферативного исследования, спорность или однозначность выводов).

5. Использование литературных источников.
6. Культура письменного изложения материала.
7. Культура оформления материалов работы.

Комплект типовых лабораторных работ

Тема 1. Введение. Общие вопросы ОБИ и дисциплины ПАСЗИ

Лабораторная работа №1: «Анализ угроз информационной безопасности и классификация ПАСЗИ»

Цель работы: Изучить основные угрозы информационной безопасности и классификацию программно-аппаратных средств защиты.

Задачи:

1. Проанализировать модели нарушителей и возможные каналы утечки информации
2. Исследовать классификацию ПАСЗИ по функциональному назначению
3. Составить матрицу угроз и соответствующих средств защиты
4. Провести анализ рисков для типовой информационной системы

Оборудование и ПО: Персональный компьютер, ОС Windows/Linux, СПС КонсультантПлюс, табличный процессор.

Критерии оценивания:

«Отлично»: Полный анализ угроз, корректная классификация ПАСЗИ, грамотно составленная матрица угроз

«Хорошо»: Незначительные ошибки в классификации, неполный анализ рисков

«Удовлетворительно»: Выполнены только базовые задачи, наличие существенных ошибок

«Неудовлетворительно»: Работа не выполнена или содержит критические ошибки

Тема 2. Защита от РПВ (ПМВ)

Лабораторная работа №2: «Исследование методов защиты от вредоносного программного обеспечения»

Цель работы: Освоить практические навыки защиты от различных типов вредоносного ПО.

Задачи:

1. Исследовать методы обнаружения и нейтрализации троянов и руткитов
2. Настроить политику белых и черных списков (Whitelisting/Blacklisting)
3. Проанализировать механизмы автозагрузки в Windows и методы защиты
4. Провести анализ системы на наличие признаков заражения

Оборудование и ПО: ПК с ОС Windows, утилиты Autoruns, Process Explorer, антивирусное ПО.

Критерии оценивания:

«Отлично»: Полное выполнение всех задач, грамотная настройка политик безопасности

«Хорошо»: Незначительные ошибки в настройке, неполный анализ системы
«Удовлетворительно»: Выполнены только основные задачи работы
«Неудовлетворительно»: Работа не выполнена или настройки неэффективны

Тема 3. Защита данных

Лабораторная работа №3: «Настройка системы резервного копирования и восстановления данных»

Цель работы: Освоить технологии резервного копирования и восстановления данных.

Задачи:

1. Настроить политику резервного копирования с использованием Acronis Backup
2. Выполнить резервное копирование критически важных данных
3. Отработать процедуру восстановления данных из резервной копии
4. Настроить расписание автоматического резервного копирования

Оборудование и ПО: ПК с ОС Windows, Acronis Backup, тестовые наборы данных.

Критерии оценивания:

«Отлично»: Корректная настройка всех компонентов, успешное восстановление данных
«Хорошо»: Незначительные ошибки в настройке расписания
«Удовлетворительно»: Ручное копирование выполнено, автоматизация не настроена
«Неудовлетворительно»: Процедуры копирования/восстановления не работают

Тема 4. Защита программ

Лабораторная работа №4: «Защита программного обеспечения от несанкционированного копирования»

Цель работы: Изучить методы защиты ПО от НСД и НСК.

Задачи:

1. Исследовать методы обфускации кода
2. Настроить защиту с использованием электронных ключей
3. Реализовать привязку ПО к характеристикам оборудования
4. Протестировать устойчивость защиты к взлому

Оборудование и ПО: ПК с ОС Windows, средства обфускации, электронные ключи, тестовое ПО.

Критерии оценивания:

«Отлично»: Реализованы все методы защиты, проведено полное тестирование
«Хорошо»: Реализованы основные методы, тестирование неполное
«Удовлетворительно»: Выполнены только базовые задачи
«Неудовлетворительно»: Методы защиты не работают

Тема 5. Программные и программно-технические средства обеспечения безопасности

Лабораторная работа №5: «Настройка аппаратного модуля доверенной загрузки»

Цель работы: Освоить принципы работы и настройки электронного замка.

Задачи:

1. Установить и настроить аппаратный модуль доверенной загрузки «Соболь»
2. Настроить политики безопасной загрузки
3. Протестировать работу системы при попытке несанкционированного доступа
4. Настроить систему аудита и протоколирования событий

Оборудование и ПО: ПК с ОС Windows, аппаратный модуль «Соболь», средства настройки.

Критерии оценивания:

«Отлично»: Полная настройка модуля, корректная работа всех политик

«Хорошо»: Основные функции настроены, дополнительные политики неактивны

«Удовлетворительно»: Базовая настройка выполнена, тестирование неполное

«Неудовлетворительно»: Модуль не настроен или не функционирует

Тестовые задания для текущего контроля

1. Что означает аббревиатура ПАСЗИ?
а) Программно-аппаратные системы защиты информации
б) Программно-технические средства защиты информации
в) Протоколы аутентификации и защиты информации
г) Профилактика атак и защита информации
Правильный ответ: а

2. Основное отличие программно-аппаратных средств защиты от технических заключается в:
а) Использовании специализированного программного обеспечения
б) Наличии аппаратных компонентов
в) Комплексном использовании программных и аппаратных компонентов
г) Более высокой стоимости

Правильный ответ: в

3. К какому типу угроз относится утечка информации через электромагнитное излучение?
а) Программно-технические угрозы
б) Аппаратные угрозы
в) Физические угрозы
г) Организационные угрозы

Правильный ответ: в

4. Что понимается под "защищенностью" информационной системы?
а) Отсутствие уязвимостей в системе
б) Способность системы противостоять угрозам
в) Наличие средств защиты информации
г) Соответствие требованиям нормативных документов

Правильный ответ: б

5. Основной целью нарушителя при проведении атаки является:
а) Демонстрация своих возможностей
б) Нанесение ущерба владельцу информации
в) Получение несанкционированного доступа к информации
г) Проверка работы системы защиты

Правильный ответ:в

6. Каналы утечки информации классифицируются на:
а) Прямые и косвенные
б) Естественные и искусственные
в) Внутренние и внешние
г) Все перечисленные

Правильный ответ: г

7. Риск в информационной безопасности - это:
а) Вероятность реализации угрозы
б) Возможный ущерб от реализации угрозы
в) Комбинация вероятности и последствий реализации угрозы
г) Мера защищенности информации

Правильный ответ:в

8. К программно-аппаратным средствам защиты НЕ относятся:
а) Аппаратные модули доверенной загрузки
б) Межсетевые экраны
в) Системы видеонаблюдения
г) Средства криптографической защиты

Правильный ответ:в

9. Аббревиатура РПВ расшифровывается как:
а) Разрушающее программное воздействие
б) Вредоносное программное обеспечение
в) Риск программного воздействия
г) Резервное программное обеспечение
Правильный ответ:а

10. К троянским программам относятся:
а) Вирусы-шифровальщики
б) Программы скрытого администрирования
в) Сетевые черви
г) Все перечисленные
Правильный ответ:б

11. Основное отличие руткитов от других видов вредоносного ПО:
а) Способность к саморазмножению
б) Сокрытие своего присутствия в системе
в) Похищение конфиденциальной информации
г) Блокировка работы системы
Правильный ответ:б

12. Метод Blacklisting предполагает:
а) Разрешение выполнения только доверенных программ
б) Запрет выполнения известных вредоносных программ
в) Анализ поведения программ в реальном времени
г) Проверку цифровых подписей программ
Правильный ответ:б

13. Ключи автозагрузки в реестре Windows находятся в разделе:
а) HKEY_LOCAL_MACHINE
б) HKEY_CURRENT_USER
в) Оба раздела
г) Ни один из разделов
Правильный ответ:в

14. Антивирусное ПО использует для обнаружения угроз:
а) Сигнатурный анализ
б) Эвристический анализ
в) Поведенческий анализ
г) Все перечисленные методы
Правильный ответ:г

15. Программные закладки характеризуются:
а) Наличием недокументированных возможностей
б) Легальным способом распространения
в) Отсутствием вредоносного функционала
г) Все варианты верны
Правильный ответ:а

16. Основная задача DLP-систем:
а) Защита от вирусов
б) Предотвращение утечек информации
в) Резервное копирование данных
г) Шифрование информации
Правильный ответ:б

17. Хостовые DLP-системы работают на уровне:
а) Сетевого оборудования
б) Отдельных рабочих станций
в) Серверов приложений
г) Всех перечисленных
Правильный ответ:б

18. Технология EFS в Windows предназначена для:
а) Сжатия данных
б) Шифрования файлов и папок
в) Резервного копирования
г) Управления доступом
Правильный ответ:б

19. Гарантированное уничтожение данных предполагает:
а) Простое удаление файлов
б) Форматирование диска

в) Многократную перезапись секторов
г) Физическое уничтожение носителя
Правильный ответ:в

20. RAID 1 обеспечивает:
а) Повышение скорости доступа
б) Зеркальное копирование данных
в) Распределенное хранение
г) Резервное копирование
Правильный ответ:б

21. Программа Acronis Backup используется для:
а) Шифрования данных
б) Резервного копирования
в) Защиты от вирусов
г) Управления доступом
Правильный ответ:б

22. Основная цель защиты программ от НСК:
а) Предотвращение несанкционированного копирования
б) Защита от вирусов
в) Обеспечение целостности
г) Все перечисленное
Правильный ответ:а

23. Обфускация кода предназначена для:
а) Ускорения выполнения программы
б) Усложнения анализа алгоритмов
в) Сжатия размера программы
г) Всех перечисленных целей
Правильный ответ:б

24. Электронные ключи защиты обеспечивают:
а) Аппаратную привязку ПО
б) Программную защиту
в) Сетевую аутентификацию
г) Все перечисленное
Правильный ответ:г

25. К протекторам программ относятся:
а) ASProtect
б) Armadillo
в) VMProtect
г) Все перечисленные
Правильный ответ:г

26. Метод защиты "черный ящик" предполагает:
а) Сокрытие исходного кода
б) Использование сложных математических преобразований
в) Аппаратную защиту
г) Все перечисленное
Правильный ответ:б

27. Аппаратный модуль доверенной загрузки "Соболь" обеспечивает:

а) Контроль целостности ПО при загрузке

б) Защиту от несанкционированного доступа

в) Шифрование данных на диске

г) Все перечисленное

Правильный ответ:г

28. RuToken относится к средствам:

а) Криптографической защиты

б) Аутентификации пользователей

в) Управления ключами

г) Всех перечисленных

Правильный ответ:г

29. СЗИ SecretNet Studio обеспечивает:

а) Мандатное управление доступом

б) Аудит безопасности

в) Защиту от утечек информации

г) Все перечисленные функции

Правильный ответ:г

30. Программные средства анализа защищенности ("Ревизор") позволяют:

а) Выявлять уязвимости в системе

б) Проверять соответствие политикам безопасности

в) Генерировать отчеты о защищенности

Правильный ответ:г

Критерии оценивания тестовых заданий для текущего контроля

Максимальное количество баллов за решение одного теста составляет 5 баллов, которые переводятся в академические оценки следующим образом:

- оценка «отлично» (5 баллов) выставляется при условии правильного ответа студента не менее чем на 85% контрольных заданий

- оценка «хорошо» (4 балла) выставляется при условии правильного ответа студента не менее чем на 70% контрольных заданий

- оценка «удовлетворительно» (3 балла) выставляется при условии правильного ответа студента не менее чем на 51% контрольных заданий

- оценка «неудовлетворительно» (1-2 балла) выставляется при условии правильного ответа студента менее чем на 50% контрольных заданий

2.2 Оценочные материалы для проведения промежуточной аттестации

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Дайте определение программно-аппаратным средствам защиты информации (ПАСЗИ).
2. В чём состоит основное отличие ПАСЗИ от технических и программных средств защиты?
3. Раскройте взаимосвязь понятий: «угроза», «уязвимость», «риск», «атака».
4. Назовите основные классы каналов утечки информации.
5. Каковы цели и задачи дисциплины «Программно-аппаратные средства защиты информации»?
6. Дайте классификацию вредоносного программного обеспечения (РПВ).
7. Что такое программная закладка? Какие виды ПЗ вы знаете?
8. Опишите механизмы работы троянских программ и руткитов.
9. Каковы современные методы защиты от сетевых червей и почтовых вирусов?
10. Что такое «эксплойт» и в чём заключается его опасность?
11. Перечислите основные направления и методы защиты данных.
12. Опишите технологии и средства резервного копирования (на примере Acronis Backup).
13. Что такое DLP-система? Назовите её основные компоненты и функции.
14. В чём разница между хостовыми и шлюзовыми DLP-системами?
15. Дайте сравнительную характеристику технологий шифрования EFS и BitLocker.
16. Что понимается под гарантированным уничтожением данных? Назовите методы.
17. Назовите основные направления защиты программного обеспечения
18. Что такое обфускация кода и какие методы обфускации вам известны?
19. Опишите механизм защиты программ с помощью электронных ключей.
20. Какие виды электронных ключей существуют и в чём их различия?
21. Как работают системы защиты от несанкционированного копирования (НСК)?
22. Что такое аппаратный модуль доверенной загрузки? Приведите пример («Соболь»).
23. Опишите назначение и функции средств безопасной аутентификации (RuToken).
24. Какие возможности предоставляет комплексная система защиты Secret Net Studio?
25. Как используются средства анализа защищённости сети (например, «Ревизор»)?

Тестовые задания для проведения промежуточной аттестации №1:

ОПК-13(ОПК-13.1, ОПК-13.3)

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

ОПК-13.1 Применяет знания основных уязвимостей программного обеспечения при разработке компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

знать	основные программные компоненты КЗИ и их назначение, принципы работы аппаратных компонентов КЗИ, особенности реализации политики ИБ, принципы защиты от основных угроз.
уметь	настраивать основные компоненты программно-аппаратных КЗИ, проводить плановые мероприятия по обслуживанию аппаратных компонент КЗИ, выполнять настройку политики ИБ.
владеть	навыками решения типовых задач ИБ на программно-аппаратных КСЗ, опытом оценки качества работы аппаратных средств защиты

1. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какое из перечисленных средств обеспечивает контроль целостности программного обеспечения на этапе загрузки операционной системы?
а) Межсетевой экран
б) Антивирусное ПО
в) Аппаратный модуль доверенной загрузки
г) DLP-система
Ответ: в
Обоснование: Аппаратный модуль доверенной загрузки (например, «Соболь») выполняет проверку целостности компонентов BIOS, загрузчика и критических файлов ОС до ее полной загрузки, предотвращая запуск модифицированного или вредоносного кода.

2. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Что понимается под термином «угроза информационной безопасности» в контексте ПАСЗИ?
а) Реализованная уязвимость системы
б) Потенциальная возможность нарушения безопасности информации
в) Наличие ошибки в программном коде
г) Отсутствие средств защиты информации
Ответ: б
Обоснование: Угроза — это потенциальное событие или действие, которое может利用 уязвимость системы и нанести ущерб конфиденциальности, целостности или доступности информации.

3. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Основная функция DLP-системы заключается в:
а) Защите от сетевых атак
б) Предотвращении утечек конфиденциальной информации

в) Ускорении работы сети
г) Резервном копировании данных
Ответ: б
Обоснование: Data Loss Prevention (DLP) системы предназначены для мониторинга, обнаружения и блокировки попыток несанкционированной передачи конфиденциальных данных за пределы контролируемой периметром зоны.

4. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Технология RAID 1 (зеркалирование) обеспечивает в первую очередь:
а) Повышение скорости чтения/записи
б) Отказоустойчивость и защиту данных от потери
в) Шифрование данных на диске
г) Экономию дискового пространства
Ответ: б
Обоснование: Уровень RAID 1 создает точную копию (зеркало) данных на двух или более дисках, что обеспечивает отказоустойчивость и защиту от потери данных в случае выхода из строя одного из дисков.

5. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какой метод защиты от вредоносного ПО основан на запрете выполнения программ, внесенных в специальный список?
а) Whitelisting
б) Эвристический анализ
в) Blacklisting
г) Поведенческий анализ
Ответ: в
Обоснование: Blacklisting (черные списки) — это метод, при котором системе запрещено выполнять программы, чьи сигнатуры или хеши находятся в списке известных вредоносных объектов.

6. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какие из перечисленных компонентов относятся к программно-аппаратным средствам защиты информации (ПАСЗИ)?
1. Аппаратный модуль доверенной загрузки
2. Текстовый процессор
3. Средство криптографической защиты информации (СКЗИ) с аппаратным ускорителем
4. Электронный ключ (RuToken)
5. Графический редактор

Ответы: 1, 3, 4
Обоснование: ПАСЗИ характеризуются неразрывной интеграцией программных и

аппаратных компонентов. Аппаратный модуль загрузки, СКЗИ с аппаратным модулем и электронные ключи используют специализированное аппаратное обеспечение для выполнения критичных функций безопасности, управляемое программным обеспечением.

7. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какие из перечисленных мер необходимы для настройки базовой политики информационной безопасности рабочей станции?

1. Установка пароля на BIOS/UEFI
2. Настройка политики блокировки экрана после 15 минут бездействия
3. Регулярное обновление операционной системы и приложений
4. Установка последней версии медиаплеера
5. Отключение брандмауэра для удобства работы в сети

Ответы: 1, 2, 3
Обоснование: Эти меры directly влияют на безопасность: пароль на BIOS предотвращает изменение порядка загрузки, политика блокировки экрана защищает от НСД в отсутствие пользователя, а обновления ОС устраняют известные уязвимости.

8. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какие из перечисленных технологий используются для защиты данных на диске?

1. Шифрование средствами EFS (Encrypting File System)
2. Использование технологии BitLocker
3. Настройка списков контроля доступа (ACL)
4. Применение RAID-массива уровня 0 (Stripe)
5. Гарантированное уничтожение данных методом многократной перезаписи

Ответы: 1, 2
Обоснование: EFS и BitLocker являются технологиями шифрования, предназначенными specifically для защиты конфиденциальности данных, хранящихся на диске, от несанкционированного доступа, в том числе при физическом изъятии носителя.

9. Задание закрытого типа на установление соответствия. Уровень сложности повышенный. Время выполнения 5 мин.
Установите соответствие между типом вредоносного программного обеспечения (РПВ) и его основной характеристикой.

Тип РПВ	Характеристика
1. Троянская программа	A) Сокрытие своего присутствия в системе и активности других программ
2. Руткит (Rootkit)	B) Выполнение несанкционированных действий под видом легитимной программы
3. Сетевой червь	C) Самостоятельное распространение по сети без необходимости заражения файлов

4. Шифровальщик (Ransomware)	D) Блокировка доступа к данным с требованием выкупа

Ответ:
1 - B
2 - A
3 - C
4 - D
Обоснование: Каждому типу вредоносного ПО соответствует уникальный механизм действия: трояны маскируются, руткиты скрываются, черви самораспространяются, а шифровальщики блокируют данные.

10. Задание закрытого типа на установление соответствия. Уровень сложности повышенный. Время выполнения 5 мин.
Установите соответствие между средством защиты и его основным назначением.

Средство защиты	Назначение
1. Аппаратный модуль доверенной загрузки	A) Криптографическая защита данных на дисковом накопителе
2. DLP-система	B) Контроль целостности и аутентичности ПО на этапе загрузки
3. BitLocker	C) Предотвращение утечки конфиденциальной информации
4. Acronis Backup	D) Создание и управление резервными копиями данных для восстановления

Ответ:
1 - B
2 - C
3 - A
4 - D
Обоснование: Каждое средство решает специфическую задачу: модуль загрузки обеспечивает целостность, DLP — защиту от утечек, BitLocker — шифрование, Acronis — резервное копирование.

11. Задание закрытого типа на установление последовательности. Уровень сложности повышенный. Время выполнения 5 мин.
Установите правильную последовательность этапов настройки политики резервного копирования.
A) Определение критически важных данных для копирования
B) Тестирование процедуры восстановления из резервной копии
C) Выбор программного средства для копирования (напр., Acronis Backup)

D) Настройка расписания автоматического создания резервных копий
E) Определение места хранения и количества хранимых копий (ретеншн-политика)
Правильная последовательность: A - C - E - D - B
Обоснование: Сначала необходимо определить, что копировать (A), затем выбрать инструмент (C), после — установить правила хранения (E) и расписание (D). Завершающим и критически важным этапом является проверка работоспособности резервных копий путем тестового восстановления (B).

12. Задание закрытого типа на установление последовательности. Уровень сложности повышенный. Время выполнения 5 мин.
Установите последовательность действий при обнаружении признаков заражения рабочей станции вредоносным ПО.
A) Отключение станции от сети для локализации угрозы
B) Сканирование системы антивирусным ПО с обновленными базами
C) Идентификация типа вредоносного ПО и способа заражения
D) Восстановление системы из чистой резервной копии или лечение
E) Составление отчета об инциденте и принятие мер по недопущению повторного заражения
Правильная последовательность: A - B - C - D - E
Обоснование: Первым действием всегда является изоляция (A) для предотвращения распространения. Затем проводится диагностика (B, C), после — восстановление работоспособности (D). Завершает процесс анализ инцидента (E) для улучшения защитных мер.

13. Задание открытого типа с развернутым ответом. Уровень сложности высокий. Время выполнения 10 мин.
Опишите основные этапы настройки аппаратного модуля доверенной загрузки «Соболь» для защиты рабочей станции.
Ответ:

1. **Физическая установка:** Монтаж аппаратного модуля «Соболь» в соответствующий слот материнской платы компьютера.
2. **Установка ПО:** Инсталляция драйверов и программного обеспечения управления, поставляемого вместе с модулем.
3. **Инициализация модуля:** Первый запуск ПО, генерация и безопасное хранение ключевой информации внутри модуля.
4. **Настройка политик безопасности:**
    - **Контроль целостности:** Настройка расчета и проверки эталонных хеш-сумм критических файлов (загрузчика, ядра ОС, системных файлов).
    - **Аутентификация:** Настройка требования предъявления токена или пароля для продолжения загрузки.
    - **Запрет загрузки с внешних носителей:** Изменение настроек модуля для блокировки загрузки с CD/DVD, USB-флешек.
5. **Создание резервной копии конфигурации:** Сохранение настроек и ключей на внешний носитель для аварийного восстановления.
6. **Тестирование:** Проверка работы системы при штатной загрузке, а также при попытках несанкционированного доступа (например, подключение другого жесткого диска или попытка загрузки с флешки).

Обоснование: Данная последовательность обеспечивает комплексную настройку, начиная с аппаратной части и заканчивая проверкой эффективности. Она гарантирует, что система будет загружаться только в том случае, если ее компоненты не были изменены, а пользователь прошел аутентификацию.

ОПК-13.3 Демонстрирует умение проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

знать	принципы анализа защищенности КСЗ
уметь	собирать и анализировать данные, предоставляемые КЗИ об угрозах и уязвимостях ИС.
владеть	практическим опытом оценки качества работы и выбора подходящих средств защиты.

14. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.

Основная цель обфускации исходного кода программы — это:

а) Увеличение скорости выполнения программы

б) Уменьшение размера исполняемого файла

в) Затруднение анализа и понимания алгоритмов программы

г) Улучшение пользовательского интерфейса

Ответ: в

Обоснование: Обфускация преобразует код в трудночитаемую форму, сохраняя его функциональность. Это усложняет проведение реверс-инжиниринга, анализ уязвимостей и создание взломанных версий программного обеспечения.

15. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.

Что из перечисленного является преимуществом использования аппаратных электронных ключей (например, RuToken) для защиты ПО?

а) Полное отсутствие стоимости внедрения

б) Невозможность копирования и распространения ключа

в) Отсутствие необходимости в драйверах

г) Автоматическое обновление программного обеспечения

Ответ: б

Обоснование: Аппаратный ключ представляет собой физический объект, который сложно скопировать программными средствами. Это обеспечивает надежную привязку лицензии программного обеспечения к конкретному устройству или пользователю.

16. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.

Комплексная система защиты информации Secret Net Studio обеспечивает:
а) Только антивирусную защиту
б) Только управление паролями
в) Мандатное управление доступом, аудит и защиту от утечек
г) Только шифрование почтового трафика
Ответ: в
Обоснование: Secret Net Studio — это комплексное решение, которое включает в себя функции контроля доступа (включая мандатный), регистрации событий безопасности (аудит) и механизмы для предотвращения утечки информации.

17. Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какой принцип лежит в основе анализа защищенности с помощью средства «Ревизор»?
а) Сравнение текущего состояния системы с эталонным
б) Нагрузочное тестирование сетевых интерфейсов
в) Анализ экономической эффективности ИТ-инфраструктуры
г) Оптимизация скорости работы приложений
Ответ: а
Обоснование: Средства контроля целостности, такие как «Ревизор», работают по принципу сравнения текущих контрольных сумм (хешей) файлов и реестра с эталонными значениями, зафиксированными в «чистом» состоянии системы.

18. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
Какие из перечисленных методов используются для защиты программного обеспечения от реверс-инжиниринга и взлома?
1. Обфускация кода
2. Использование программных протекторов (ASProtect, Themida)
3. Привязка к уникальным характеристикам hardware (HDD, CPU)
4. Настройка корректного цвета окон приложения
5. Добавление в код подробных комментариев на английском языке

Ответы: 1, 2, 3
Обоснование: Эти методы directly направлены на усложнение анализа: обфускация запутывает код, протекторы затрудняют отладку и дизассемблирование, а аппаратная привязка ограничивает несанкционированное копирование.

19. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.
При выборе подходящего средства криптографической защиты информации (СКЗИ) необходимо учитывать:
1. Соответствие требованиям стандартов (например, ГОСТ)
2. Наличие действующего сертификата ФСТЭК России
3. Скорость шифрования/расшифрования

4. Цвет корпуса аппаратного модуля
5. Совместимость с операционными системами предприятия

Ответы: 1, 2, 3, 5

Обоснование: Критерии выбора СКЗИ должны включать нормативное соответствие, официальное подтверждение безопасности (сертификат), производительность (скорость) и практическую применимость в существующей ИТ-инфраструктуре (совместимость).

20. Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора. Уровень сложности базовый. Время выполнения 3 мин.

Какие из перечисленных функций относятся к системам анализа защищенности (например, «Ревизор»)?

1. Выявление несанкционированных изменений в файлах
2. Контроль целостности системного реестра
3. Мониторинг сетевого трафика в реальном времени
4. Генерация отчетов о detected отклонениях
5. Автоматическое исправление всех найденных уязвимостей

Ответы: 1, 2, 4

Обоснование: Системы контроля целостности (например, «Ревизор») специализируются на обнаружении изменений (1, 2) и документировании этих изменений (4). Они, как правило, не занимаются глубинным сетевым мониторингом (3) и не всегда могут автоматически исправлять найденные проблемы (5), так как это может нарушить работу системы.

21. Задание закрытого типа на установление соответствия. Уровень сложности повышенный. Время выполнения 5 мин.

Установите соответствие между методом защиты программного обеспечения и его описанием.

Метод защиты	Описание
1. Обфускация	A) Затруднение анализа программы путем запутывания исходного или машинного кода
2. Аппаратная привязка	B) Связывание лицензии программы с уникальными идентификаторами оборудования
3. Защита от отладки	C) Использование методов обнаружения и противодействия работе отладчика
4. Электронный ключ (HASP)	D) Использование внешнего аппаратного устройства для аутентификации и запуска ПО

Ответ:

1 - A

2 - B
3 - C
4 - D
Обоснование: Каждый метод решает свою задачу: обфускация скрывает логику, привязка ограничивает запуск, защита от отладки препятствует динамическому анализу, а электронный ключ обеспечивает аппаратную аутентификацию.

22. Задание закрытого типа на установление последовательности. Уровень сложности повышенный. Время выполнения 5 мин.
Установите последовательность этапов проведения анализа защищенности рабочей станции с помощью средства контроля целостности.
A) Фиксация эталонного состояния системы (снятие «слепка»)
B) Регулярное сканирование системы и сравнение с эталоном
C) Анализ отчета о выявленных изменениях
D) Принятие решения по результатам анализа (игнорировать/расследовать/откатить)
E) Восстановление целостности системы (при необходимости)
Правильная последовательность: A - B - C - D - E
Обоснование: Процесс начинается с создания эталона в доверенном состоянии (A). Затем производится текущая проверка (B) и анализ расхождений (C). На основе анализа принимается решение (D), и если изменения были несанкционированными, выполняется восстановление (E).

23. Задание закрытого типа на установление последовательности. Уровень сложности повышенный. Время выполнения 5 мин.
Установите последовательность действий при развертывании системы защиты от несанкционированного копирования (НСК) для нового программного продукта.
A) Выбор и интеграция метода защиты (обфускация, протектор, электронный ключ)
B) Анализ угроз НСК и формулировка требований к защите
C) Тестирование защищенной версии ПО на устойчивость к взлому
D) Разработка политики лицензирования и распространения
E) Выпуск и распространение защищенной версии продукта
Правильная последовательность: B - D - A - C - E
Обоснование: Сначала необходимо оценить риски и определить цели (B), затем — как будет реализована лицензия (D). После этого выбирается и внедряется технический метод (A), который обязательно тестируется (C). Финальный этап — релиз (E).

24. Задание открытого типа с развернутым ответом. Уровень сложности высокий. Время выполнения 10 мин.
Опишите, какой комплекс мер защиты программно-аппаратных средств необходимо реализовать для обеспечения безопасности сервера с конфиденциальными данными. В ответе укажите не менее 5 различных мер, относящихся к разным темам курса.
Ответ:
Для комплексной защиты сервера с конфиденциальными данными необходимо реализовать следующие меры:

1. **Физический и аппаратный уровень (Тема 1, 5):** Размещение сервера в охраняемом помещении с контролем доступа. Установка аппаратного модуля доверенной загрузки

(например, «Соболь») для контроля целостности и предотвращения загрузки несанкционированного ПО.

2. **Защита данных (Тема 3):** Обязательное использование полнодискового шифрования (например, BitLocker) для всех дисковых накопителей сервера. Это защитит данные в случае физического изъятия дисков.
3. **Резервное копирование и восстановление (Тема 3):** Настройка автоматизированной системы резервного копирования (например, на базе Acronis Backup) с регулярным созданием резервных копий критичных данных и их хранением на изолированном носителе. Обязательное регулярное тестирование процедуры восстановления.
4. **Защита от вредоносного ПО (Тема 2):** Установка и настройка специализированного антивирусного ПО для серверов с регулярным обновлением сигнатур и включением функций поведенческого анализа.
5. **Контроль доступа и аудит (Тема 4, 5):** Реализация строгой политики разграничения прав доступа (принцип наименьших привилегий). Внедрение системы аудита и протоколирования (как часть решения типа Secret Net Studio или средствами ОС) для фиксации всех действий пользователей и администраторов. Регулярный анализ логов.

Обоснование: Предложенный комплекс мер обеспечивает многоуровневую защиту (Defense in Depth). Он охватывает все ключевые аспекты: от физического доступа и целостности ПО на этапе загрузки до конфиденциальности данных, их доступности (бэкапы) и контроля действий в системе. Это позволяет противостоять широкому спектру угроз.

Критерии оценки для проведения зачета по дисциплине (тестирование)

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

Оценка	Уровень сформированности компетенции	Критерии
«Отлично» («зачтено»)	Высокий	Выполнено более 80% заданий предложенного теста
«Хорошо» («зачтено»)	Хороший	Выполнено 60-80% заданий предложенного теста
«Удовлетворительно» («зачтено»)	Достаточный	Выполнено 35-60% заданий предложенного теста
«Неудовлетворительно» («не зачтено»)	Недостаточный	Выполнено менее 35% заданий предложенного теста