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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Оценочные материалы по дисциплине Модели безопасности компьютерных систем

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

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Модели безопасности компьютерных систем и установление уровня сформированности компетенций обучающегося.

ОМ предназначены для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включают оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины Модели безопасности компьютерных систем.

1. Паспорт оценочных материалов по дисциплине «Модели безопасности компьютерных систем»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.1. Имеет практический опыт оценивания уровня безопасности компьютерных систем и сетей, разработки требований по защите, формирования политик безопасности компьютерных систем и сетей, проведения анализа безопасности компьютерных систем, разработки требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	Знать: методы оценки уровня защищенности компьютерных систем и сетей, требования по защите компьютерной инфраструктуры и методологии их разработки, основные принципы построения эффективных политик безопасности компьютерных систем и сетей; методики анализа безопасности информационных систем. Уметь: оценивать уровень безопасности существующих компьютерных систем и сетей; разрабатывать требования по защите компьютерных систем и сетей; формулировать политику безопасности и управлять её реализацией; проводить анализ уязвимости компьютерных систем и определять меры противодействия угрозам. Владеть: навыком проектирования и реализации политик безопасности компьютеризированных инфраструктур; инструментами оценки соответствия требованиям информационной безопасности; практическими методами мониторинга состояния защищённости компьютерных систем и сетей.	Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей.	Реферат (Раздел 1), Тест (раздел 1)	Тест (В1-6)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
	ОПК-11.2. Демонстрирует умение проводить исследование вредоносного программного обеспечения, выявлять аномальную активность в компьютерных системах и сетях, выбирать программно-аппаратные средства защиты информации	Знать: типологию и характеристики современных вредоносных программ; способы выявления аномальной активности в компьютерных системах и сетях; классификацию методов выбора аппаратных и программных средств защиты информации. Уметь: анализировать вредоносное программное обеспечение и выявлять признаки подозрительной активности в сети; определять необходимые средства защиты для нейтрализации конкретных типов атак; выбирать оптимальные решения для защиты информации исходя из особенностей организации. Владеть: техниками исследования поведения вредоносного ПО; способами обнаружения аномалий в работе компьютерных систем и сетевых взаимодействиях; мением подбирать и внедрять современные программно-технические средства защиты.	Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ. Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений	Реферат (Раздел 2-3), Тест (Раздел 2-3)	Тест (В7-12)
	ОПК-11.3. Применяет знания моделей без-опасности и правил разработки документов предприятия по	Знать: современные модели информационной безопасности и правила документирования политики безопасности организаций; принципы управления доступом пользователей и контроль информационных потоков внутри корпоративных ИТ-инфраструктур;	Раздел 4. Виртуальные защищенные сети, VPN	Реферат (Раздел 4), Тест (Раздел 4)	Тест (В13-18)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
	информационной безопасности для разработки политики управления доступом и информационным и потоками в компьютерных системах	нормативно-правовые основы информационной безопасности предприятий. Уметь: создавать политики управления доступом и регулирующими информационными потоками в рамках корпоративной системы; проектировать эффективные схемы контроля над распространением конфиденциальной информации; документально оформлять стандарты и процедуры по обеспечению информационной безопасности. Владеть: умениями анализировать угрозы информационной безопасности и проектировать соответствующие защитные мероприятия; правилами составления регламентов и инструкций по управлению доступом и обеспечением конфиденциальности информации.			
	ОПК-11.4. Демонстрирует умение разрабатывать модель угроз и нарушителя информационной безопасности компьютерных сетей	Знать: современные модели информационной безопасности и правила документирования политики безопасности организаций; принципы управления доступом пользователей и контроль информационных потоков внутри корпоративных ИТ-инфраструктур; нормативно-правовые основы информационной безопасности предприятий.	Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы	Реферат (Раздел 5), Тест (Раздел 5), Практическое задание (1-5)	Тест (В19-25)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
		Уметь: создавать политики управления доступом и регулирующими информационными потоками в рамках корпоративной системы; проектировать эффективные схемы контроля над распространением конфиденциальной информации; документально оформлять стандарты и процедуры по обеспечению информационной безопасности. Владеть: умениями анализировать угрозы информационной безопасности и проектировать соответствующие защитные мероприятия; правилами составления регламентов и инструкций по управлению доступом и обеспечением конфиденциальности информации.	беспроводной связи.		

2. Оценочные материалы по дисциплине «Модели безопасности компьютерных систем»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей.

1. Анализ современных угроз информационной безопасности в компьютерных сетях
2. Типы вредоносного ПО и их влияние на безопасность сетей
3. Социальная инженерия как угроза информационной безопасности: методы и примеры
4. Уязвимости протоколов передачи данных и их влияние на безопасность сетей
5. Роль человеческого фактора в нарушении информационной безопасности
6. Атаки типа DDoS: механизмы, последствия и способы защиты
7. Проблемы обеспечения конфиденциальности данных в облачных вычислениях
8. Безопасность IoT-устройств: угрозы и меры защиты
9. Фишинг и его последствия для информационной безопасности организаций
10. Криптографические угрозы: современные подходы к защите данных
11. Обзор международных стандартов информационной безопасности: ISO/IEC 27001
12. Стандарт NIST Cybersecurity Framework: принципы и применение
13. Сравнительный анализ стандартов ISO 27001 и NIST в контексте защиты информации
14. Роль стандартов в управлении рисками информационной безопасности
15. Стандарты безопасности сетевой инфраструктуры: IEEE 802.1X и другие

Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.. 1. Основные принципы работы межсетевых экранов: фильтрация трафика и управление доступом

2. Типы межсетевых экранов: аппаратные и программные решения
3. Сравнительный анализ статических и динамических межсетевых экранов
4. Роль межсетевых экранов в обеспечении безопасности корпоративных сетей
5. Как настроить межсетевой экран для защиты от внешних угроз
6. Атаки на межсетевые экраны: типичные уязвимости и способы защиты
7. Использование VPN в сочетании с межсетевыми экранами для повышения безопасности
8. Интеграция межсетевых экранов с системами обнаружения и предотвращения вторжений (IDS/IPS)
9. Межсетевые экраны следующего поколения (NGFW): особенности и преимущества
10. Роль межсетевых экранов в защите облачных сервисов
11. Анализ случаев успешных атак на сети, защищенные межсетевыми экранами
12. Сетевые политики и правила фильтрации трафика: лучшие практики
13. Межсетевые экраны в малом бизнесе: доступные решения и рекомендации
14. Будущее межсетевых экранов: тренды и инновации в области сетевой безопасности
15. Схемы сетевой защиты с использованием межсетевых экранов: примеры и практические рекомендации

Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений.

1. Обзор основных категорий сетевых атак: классификация и примеры
2. Атаки на уровне приложений: типы, методы и способы защиты
3. Сетевые атаки на уровне транспортного протокола: TCP/IP и UDP

4. DDoS-атаки: механизмы, последствия и методы защиты
5. Социальная инженерия как метод сетевых атак: анализ и примеры
6. Атаки на беспроводные сети: уязвимости и способы защиты
7. Вредоносное ПО и его роль в сетевых атаках: вирусы, черви, трояны
8. Атаки через уязвимости программного обеспечения: примеры и защита
9. Фишинг и его влияние на безопасность сетей: методы обнаружения и предотвращения
10. Атаки «человек посередине» (MITM): механизмы и способы защиты
11. Системы обнаружения вторжений (IDS): принципы работы и классификация
12. Системы предотвращения вторжений (IPS): отличие от IDS и применение
13. Методы анализа трафика для обнаружения сетевых атак: статистические и сигнатурные подходы
14. Использование машинного обучения для обнаружения сетевых вторжений: перспективы и вызовы
15. Интеграция технологий обнаружения вторжений с другими системами безопасности: лучшие практики

Раздел 4. Виртуальные защищенные сети, VPN.Технология OLAP.

1. История развития виртуальных частных сетей (VPN): от первых решений до современных технологий
2. Принципы работы VPN: как создаются защищенные туннели
3. Сравнение протоколов VPN: преимущества и недостатки OpenVPN, L2TP, PPTP и IKEv2
4. Безопасность в VPN: как шифрование и аутентификация защищают данные
5. VPN для удаленной работы: как обеспечить безопасность сотрудников на дому
6. Использование VPN для защиты конфиденциальности в интернете: правовые аспекты
7. Технологии NAT и их влияние на работу VPN
8. VPN и мобильные устройства: вызовы безопасности и решения
9. Анализ уязвимостей VPN-сервисов: как злоумышленники могут их использовать
10. Сравнение коммерческих и бесплатных VPN-сервисов: что выбрать?
11. VPN в корпоративной среде: преимущества, недостатки и лучшие практики
12. Обход географических ограничений с помощью VPN: этические и правовые вопросы
13. Будущее VPN-технологий: новые тренды и перспективы развития
14. Интеграция VPN с другими технологиями безопасности: фаерволы, IDS/IPS и др.
15. Кейс-стадии использования VPN в различных отраслях: финансы, здравоохранение, образование

Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.

1. Анализ угроз безопасности информационных сетей на промышленных предприятиях
2. Методы защиты информации в системах управления промышленными процессами
3. Роль стандарта ISA/IEC 62443 в обеспечении кибербезопасности на промышленных объектах
4. Сравнительный анализ технологий защиты беспроводных сетей на промышленных предприятиях
5. Использование VPN для защиты данных в беспроводных промышленных системах
6. Кейс-стадии: успешные примеры внедрения систем безопасности на объектах критической инфраструктуры
7. Интернет вещей (IoT) в промышленности: вызовы безопасности и пути их решения
8. Шифрование данных в беспроводных системах связи: современные подходы и технологии
9. Аудит и оценка рисков информационной безопасности на промышленных предприятиях

10. Интеграция систем физической безопасности и кибербезопасности на критических объектах
11. Технологии аутентификации и авторизации в защищенных беспроводных сетях
12. Применение машинного обучения для обнаружения аномалий в промышленных сетях
13. Защита данных в условиях мобильных и беспроводных сетей: лучшие практики
14. Проблемы и перспективы внедрения 5G в промышленные системы и их безопасность
15. Роль сотрудников в обеспечении безопасности информационных систем на предприятиях: обучение и осведомленность

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 практических заданий

Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей.

Угрозы информационной безопасности сети: классификация, виды, причины возникновения. Уязвимости программного и аппаратного обеспечения. Методы защиты информации: организационные, технические, программные. Стандарты информационной безопасности: ISO 27001, PCI DSS, HIPAA. Политика безопасности сети.

Вопросы для самоконтроля:

1. Какие существуют основные виды угроз информационной безопасности сетей?
2. В чем разница между уязвимостью и угрозой?
3. Какие основные организационные и технические меры защиты информации в сети вы знаете?
4. Что такое стандарт ISO 27001 и какие основные требования он предъявляет?
5. Что такое ложноположительное и ложноотрицательное срабатывание системы обнаружения вторжений?
6. Какие основные задачи решают SIEM-системы?

Цель работы - получение теоретических навыков анализа угроз информационной безопасности сети и понимания основных стандартов и инструментов защиты.

В работе используется презентация слайдов, выполненная в MS Powerpoint

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.

Основные функции межсетевых экранов (МЭ). Типы МЭ: пакетные фильтры, stateful inspection, прокси-серверы, NGFW. Принципы работы: фильтрация трафика, NAT, VPN, обнаружение и предотвращение вторжений (IDS/IPS). Архитектуры МЭ: однорукий режим, маршрутизирующий режим, прозрачный режим. Политики безопасности МЭ. Правила фильтрации трафика.

Вопросы для самоконтроля:

1. Какие основные функции выполняет межсетевой экран?
2. В чем разница между пакетным фильтром и межсетевым экраном stateful inspection?
3. Что такое NAT и зачем он используется в межсетевых экранах?
4. Какие преимущества и недостатки использования прокси-сервера в качестве межсетевого экрана?
5. Что такое DMZ и как он используется для защиты сети?
6. Какие основные параметры необходимо учитывать при выборе межсетевого экрана?

Цель работы - получение теоретических и практических навыков настройки межсетевого экрана и построения схем сетевой защиты.

В работе используется презентация слайдов, выполненная в MS Powerpoint.

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений

Основные категории сетевых атак: разведка, сканирование, атаки на отказ в обслуживании (DoS/DDoS), эксплуатация уязвимостей, внедрение вредоносного кода, социальная инженерия. Методы обнаружения вторжений: сигнатурный анализ, статистический анализ, анализ на основе аномалий, анализ протоколов. Типы систем обнаружения вторжений (IDS): сетевые (NIDS), хостовые (HIDS). Методы реагирования на вторжения.

Вопросы для самоконтроля:

1. Какие основные категории сетевых атак существуют?
2. В чем разница между атакой DoS и DDoS?
3. Какие основные методы обнаружения вторжений вы знаете?
4. В чем разница между сигнатурным анализом и анализом на основе аномалий?
5. Какие преимущества и недостатки сетевых (NIDS) и хостовых (HIDS) систем обнаружения вторжений?
6. Как реагировать на обнаруженное вторжение?

Цель работы - получение теоретических и практических навыков анализа сетевых атак и использования технологий обнаружения вторжений.

В работе используется база данных выполненная в MS Access/

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Раздел 4. Виртуальные защищенные сети, VPN.

Основные принципы работы VPN. Типы VPN: site-to-site, remote access. Протоколы VPN: PPTP, L2TP/IPsec, OpenVPN, WireGuard. Шифрование и аутентификация в VPN. Требования к инфраструктурному обеспечению VPN. VPN для защиты трафика в публичных сетях.

Вопросы для самоконтроля:

1. Какие основные принципы работы VPN?
2. В чем разница между site-to-site и remote access VPN?
3. Какие основные протоколы VPN вы знаете?
4. Какие алгоритмы шифрования используются в VPN?
5. Что такое аутентификация в VPN и зачем она нужна?
6. В чем преимущества и недостатки разных протоколов VPN (PPTP, L2TP/IPsec, OpenVPN, WireGuard)?
7. Что такое Split Tunneling и когда его целесообразно использовать?

Цель работы - получение теоретических и практических навыков настройки VPN и анализа его безопасности.

В работе используется презентация слайдов, выполненная в MS Powerpoint.

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила

техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.

Принципы работы защищенных беспроводных сетей**.** Стандарты безопасности для беспроводных сетей (WPA2, WPA3)**.** Методы шифрования и аутентификации в беспроводных сетях**.** Защита от атак на беспроводные сети (например, MITM, DoS)**.** Рекомендации по проектированию и внедрению защищенных беспроводных систем

Вопросы для самоконтроля:

1. Какие основные принципы работы защищенных беспроводных сетей?
2. В чем разница между стандартами WPA2 и WPA3?
3. Какие методы шифрования используются в беспроводных сетях?
4. Что такое аутентификация в контексте беспроводных сетей и какие протоколы для этого применяются?
5. Какие виды атак наиболее распространены в беспроводных сетях и как им противостоять?
6. Каковы рекомендации по проектированию защищенных беспроводных систем на промышленных предприятиях?
7. Что такое VLAN и как он может помочь в защите беспроводных сетей?

Цель работы - получение теоретических и практических навыков настройки защищенных беспроводных сетей, анализа их безопасности и разработки рекомендаций по их улучшению.

В работе используется презентация слайдов, выполненная в MS Powerpoint

Типовые тесты

Тест №1

Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей.

1. Какая из перечисленных ниже классификаций угроз информационной безопасности сетей является наиболее общей?

А) Нарушение конфиденциальности, нарушение целостности, нарушение доступности. +

Б). Вирусы, трояны, черви.

В). Внутренние, внешние, случайные.

Г). Физические, логические, программные.

2. Что такое "уязвимость" в контексте информационной безопасности?

А). Действие злоумышленника, направленное на нанесение вреда системе.

Б). Слабость в системе, которая может быть использована злоумышленником. +

В). Последствие реализации угрозы.

Г). Политика безопасности, определяющая правила защиты системы.

3. Какие из перечисленных ниже мер относятся к организационным мерам защиты

информации?

А). Использование межсетевого экрана.

Б). Настройка системы обнаружения вторжений.

В). Обучение персонала правилам информационной безопасности. +

Г). Шифрование данных.

4. Какой стандарт информационной безопасности наиболее широко применяется для создания системы управления информационной безопасностью (СУИБ)?

А). PCI DSS

Б). HIPAA

В). ISO 27001 +

Г). GDPR

5. Какая из перечисленных ниже мер направлена на обеспечение целостности информации?

А). Использование сложного пароля.

Б). Резервное копирование данных. +

В). Установка антивирусного программного обеспечения.

Г). Шифрование данных.

6. Какая основная цель стандарта PCI DSS?

А). Защита персональных данных пользователей.

Б). Защита данных кредитных карт. +

В). Обеспечение безопасности медицинских данных.

Г). Обеспечение конфиденциальности государственной информации.

7. Что такое "ложноположительное срабатывание" системы обнаружения вторжений (IDS)?

А). Когда IDS пропускает реальную атаку.

Б). Когда IDS идентифицирует легитимное действие как атаку. +

В). Когда IDS правильно определяет атаку.

Г). Когда IDS блокирует сетевой трафик.

8. Что такое "политика безопасности сети"?

А). Набор технических средств защиты сети.

Б). Документ, определяющий правила и процедуры защиты сети. (Правильный ответ)

В). Программное обеспечение для анализа сетевого трафика.

Г). Стандарт шифрования данных.

9. Какие основные задачи решают SIEM-системы?

А). Управление доступом пользователей.

Б). Сбор, анализ и корреляция событий безопасности из различных источников. +

В). Защита от вредоносного программного обеспечения.

Г). Предотвращение утечек данных.

10. Что такое DDoS-атака?

А). Атака, направленная на кражу конфиденциальной информации.

Б). Атака, направленная на нарушение доступности сервиса путем перегрузки сети большим количеством запросов. +

В). Атака, направленная на изменение данных.

Г). Атака, направленная на внедрение вредоносного кода.

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

Тест №2

Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.

1. Какова основная функция межсетевого экрана (МЭ)?

А). Шифрование сетевого трафика.

Б). Обнаружение вредоносного программного обеспечения.

В). Контроль и фильтрация сетевого трафика между сетями. +

Г). Аутентификация пользователей.

2. Какой режим работы МЭ обеспечивает наивысший уровень защиты?

А). Разрешить все.

Б). Запретить все. +

В). Разрешить по умолчанию, запретить исключения.

Г). Запретить по умолчанию, разрешить исключения.

3. Что такое stateful inspection в контексте межсетевых экранов?

А). Фильтрация трафика на основе IP-адресов и портов.

Б). Анализ трафика на уровне приложений.

В). Отслеживание состояния сетевых соединений. +

Г). Использование правил для фильтрации трафика.

4. Какой тип межсетевого экрана работает на сетевом уровне (Network Layer) модели OSI?

А). Proxy-сервер.

Б). МЭ, фильтрующий пакеты. +

В). Web Application Firewall (WAF).

Г). Stateful Inspection Firewall.

5. Что такое DMZ (Demilitarized Zone) в контексте сетевой безопасности?

А). Сеть с высоким уровнем безопасности для хранения конфиденциальной информации.

Б). Сеть, используемая для тестирования новых программных продуктов.

В). Сеть, содержащая общедоступные серверы, отделенная от внутренней сети. +

Г). Резервная сеть для аварийного восстановления.

6. Для чего используются правила (rules) в межсетевом экране?

А). Для определения типа трафика, разрешенного в сети. +

Б). Для шифрования сетевого трафика.

В). Для проведения аутентификации пользователей.

Г). Для анализа вредоносного программного обеспечения.

7. Какой тип атак WAF (Web Application Firewall) помогает предотвратить?

А). DDoS-атаки.

Б). Атаки "человек посередине" (MITM).

В). SQL-инъекции. +

Г). Переполнение буфера.

8. Что такое прокси-сервер (Proxy Server) в контексте сетевой безопасности?

А). Межсетевой экран, фильтрующий пакеты на основе IP-адресов.

Б). Сервер, выступающий посредником между клиентом и сервером в интернете. +

В). Сервер для резервного копирования данных.

Г). Сервер для управления доступом пользователей.

9. Какая из следующих схем сетевой защиты обеспечивает наиболее надежную защиту внутренней сети?

А). Один межсетевой экран.

Б). Два межсетевых экрана в параллельном режиме работы.

В). Два межсетевых экрана в последовательном режиме работы (с DMZ). +

Г). Межсетевой экран и система обнаружения вторжений (IDS).

10. Что такое honeypot в контексте сетевой безопасности?

А). Межсетевой экран.

Б). Система обнаружения вторжений.

В). Ловушка для злоумышленников, имитирующая уязвимый сервер. +

Г). Система для шифрования сетевого трафика.

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

Тест №3

Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений

1. К какой категории сетевых атак относится атака типа "отказ в обслуживании" (DoS)?

А). Атаки на получение несанкционированного доступа.

Б). Атаки на нарушение целостности данных.

В). Атаки на нарушение доступности ресурсов. +

Г). Атаки на конфиденциальность данных.

2. Что такое атака "человек посередине" (Man-in-the-Middle, MITM)?

А). Атака, направленная на подбор пароля.

Б). Атака, при которой злоумышленник перехватывает и изменяет трафик между двумя сторонами. +

В). Атака, направленная на переполнение буфера.

Г). Атака, направленная на блокировку сетевых ресурсов.

3. Какой тип атак использует уязвимости в веб-приложениях для внедрения вредоносного SQL-кода?

А). Межсайтовый скриптинг (XSS).

Б). SQL-инъекция. +

В). Межсайтовая подделка запросов (CSRF).

Г). Переполнение буфера.

4. Что такое фишинг (Phishing)?

А). Атака, направленная на перехват паролей от Wi-Fi сети.

Б). Атака, направленная на получение конфиденциальной информации путем обмана пользователей. +

В). Атака, направленная на взлом веб-сервера.

Г). Атака, направленная на подмену DNS-сервера.

5. Какой метод обнаружения вторжений основывается на анализе сигнатур известных атак

А). Аномальный метод обнаружения.

Б). Метод обнаружения на основе сигнатур. +

В). Метод обнаружения на основе протоколов.

Г). Метод обнаружения на основе статистики.

6. Что такое система обнаружения вторжений (IDS)?

А). Система предотвращения вторжений.

Б). Система обнаружения и регистрации попыток несанкционированного доступа. +

В). Межсетевой экран.

Г). Антивирусная программа.

7. В каком режиме работы IDS только обнаруживает вторжения, не блокируя их?

А). Активный режим.

Б). Пассивный режим. +

В). Автоматический режим.

Г). Интерактивный режим.

8. Какой тип IDS анализирует сетевой трафик?

А). HIDS (Host-based Intrusion Detection System).

Б). NIDS (Network-based Intrusion Detection System). +

В). Hybrid IDS.

Г). Application-based IDS.

9. Что такое атака типа "нулевой день" (Zero-Day Attack)?

А). Атака, которая происходит в полночь.

Б). Атака, использующая уязвимость, для которой еще не существует исправления. +

В). Атака, направленная на обход системы безопасности, работающей в течение 24 часов.

Г). Атака, которая происходит в первый день месяца.

10. Что такое "ложный негатив" в контексте IDS?

А). Обнаружение легитимной активности как подозрительной.

Б). Необнаружение реальной атаки. +

В). Блокировка сетевого трафика.

Г). Идентификация уязвимости в системе.

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

Тест №4

Раздел 4. Виртуальные защищенные сети, VPN.

1. Что такое VPN (Virtual Private Network)?

А). Физическая сеть, используемая для обеспечения безопасности данных.

Б). Технология, позволяющая создать защищенное соединение через публичную сеть.+

В). Локальная сеть с высоким уровнем безопасности.

Г). Протокол для шифрования электронной почты.

2. Какова основная цель использования VPN?

А). Увеличение скорости интернет-соединения.

Б). Обеспечение конфиденциальности и безопасности данных при передаче по незащищенным сетям. +

В). Сокрытие реального IP-адреса.

Г). Все вышеперечисленное.

3. Какой протокол VPN использует для установления защищенного соединения и шифрования трафика?

А). HTTP

Б). FTP

В). IPsec +

Г). SMTP

4. Какой метод аутентификации пользователей чаще всего используется в VPN?

А). Аутентификация по IP-адресу.

Б). Аутентификация по MAC-адресу.

В). Аутентификация по имени пользователя и паролю. +

Г). Аутентификация по GPS координатам.

5. Какие типы VPN существуют в зависимости от назначения?

А). IPsec и SSL VPN.

Б). Site-to-Site VPN и Remote Access VPN. +

В). PPTP и L2TP.

Г). OpenVPN и WireGuard.

6. Что такое Site-to-Site VPN?

А). VPN для подключения отдельного пользователя к корпоративной сети.

Б). VPN для объединения двух или более сетей между собой. +

В). VPN для защиты трафика веб-браузера.

Г). VPN для шифрования электронной почты.

7. Что такое Remote Access VPN?
А). VPN для подключения отдельного пользователя к корпоративной сети. +
Б). VPN для объединения двух или более сетей между собой.
В). VPN для защиты трафика веб-браузера.
Г). VPN для шифрования электронной почты.

8. Какой протокол VPN считается наиболее безопасным и современным?
А). PPTP
Б). L2TP
В). IPsec
Г). WireGuard +

9. Какие функции выполняет VPN-сервер?
А). Шифрует трафик клиентского устройства.
Б). Обеспечивает аутентификацию и авторизацию пользователей.
В). Предоставляет доступ к ресурсам защищенной сети.
Г). Все вышеперечисленное. +

10. В чем заключается преимущество использования VPN для обхода географических ограничений?
А). VPN увеличивает скорость интернет-соединения.
Б). VPN позволяет получить доступ к контенту, недоступному в определенном регионе, маскируя IP-адрес пользователя. +
В). VPN позволяет увеличить объем доступного интернет-трафика.
Г. VPN обеспечивает полную анонимность в интернете.

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

Тест №5

Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.

1. Какие системы обычно используются для управления технологическими процессами на промышленных предприятиях?
А). CRM-системы
Б). ERP-системы
В). SCADA-системы +
Г). SCM-системы

2. Каковы основные риски, связанные с использованием беспроводных сетей в критической инфраструктуре?

А). Перехват данных и несанкционированный доступ к контроллерам. +
Б). Снижение скорости интернет-соединения.
В). Повышенный расход электроэнергии.
Г). Сложность в настройке оборудования.

3. Какой стандарт информационной безопасности особенно важен для защиты критической инфраструктуры?
А). PCI DSS
Б). HIPAA
В). IEC 62443 +
Г). GDPR

4. Что такое "воздушный зазор" (air gap) в контексте промышленной безопасности?
А). Использование воздушного охлаждения для оборудования.
Б) Физическое отделение (изоляция) промышленной сети от внешних сетей (например, интернета). +
В). Использование беспроводной связи вместо проводной.
Г). Наличие свободного места на сервере.

5. Какие меры необходимо предпринять для усиления безопасности беспроводных сетей, используемых для управления SCADA-системами?
А). Использовать сложные пароли, шифрование и аутентификацию. +
Б). Регулярно менять SSID сети.
В). Подключать все устройства к одной беспроводной сети.
Г). Отключить шифрование для повышения скорости передачи данных.

6. Что такое DNP3 и Modbus в контексте промышленных сетей?
А). Стандарты беспроводной связи.
Б). Промышленные протоколы связи. +
В). Операционные системы для промышленных контроллеров.
Г). Антивирусные программы для SCADA-систем.

7. Какое устройство может быть использовано для контроля доступа к беспроводной сети на промышленном предприятии?
А). Концентратор (Hub)
Б). Маршрутизатор с функциями межсетевого экрана. +
В). Репитер (Repeater)
Г). Антенна

8. Для чего используется сегментация сети в промышленных сетях?
А). Для увеличения скорости передачи данных.
Б). Для снижения общей нагрузки на сеть.
В). Для ограничения распространения угроз и защиты критически важных участков сети. +
Г). Для упрощения администрирования сети.

9. Какие методы аутентификации наиболее рекомендованы для защиты беспроводных сетей на промышленных предприятиях?
А). Аутентификация по MAC-адресу.
Б). Многофакторная аутентификация (MFA). +
В). Аутентификация по IP-адресу.
Г. Отсутствие аутентификации.

10. Каковы основные преимущества использования защищенных беспроводных протоколов, таких как WPA3, в промышленных сетях?

А). Увеличение скорости беспроводной связи.

Б). Повышение безопасности и защиты от перехвата данных. +

В). Упрощение настройки беспроводного оборудования.

Г). Снижение стоимости беспроводного оборудования.

2.2 Оценочные материалы для проведения промежуточной аттестации

1. Какая из перечисленных ниже классификаций угроз информационной безопасности сетей является наиболее общей?
А). Нарушение конфиденциальности, нарушение целостности, нарушение доступности. +
Б). Вирусы, трояны, черви.
В). Внутренние, внешние, случайные.
Г). Физические, логические, программные.

2. Что такое "уязвимость" в контексте информационной безопасности?
А). Действие злоумышленника, направленное на нанесение вреда системе.
Б). Слабость в системе, которая может быть использована злоумышленником.
В). Последствие реализации угрозы.
Г). Политика безопасности, определяющая правила защиты системы.

3. Какой стандарт информационной безопасности наиболее широко применяется для создания системы управления информационной безопасностью (СУИБ)?
А). PCI DSS
Б). HIPAA
В). ISO 27001 +
Г). GDPR

4. Какова основная функция межсетевого экрана (МЭ)?
А). Шифрование сетевого трафика.
Б). Обнаружение вредоносного программного обеспечения.
В). Контроль и фильтрация сетевого трафика между сетями. +
Г). Аутентификация пользователей.

5. Какой режим работы МЭ обеспечивает наивысший уровень защиты?
А). Разрешить все.
Б). Запретить все. +
В). Разрешить по умолчанию, запретить исключения.
Г). Запретить по умолчанию, разрешить исключения.

6. Что такое DMZ (Demilitarized Zone) в контексте сетевой безопасности?
А). Сеть с высоким уровнем безопасности для хранения конфиденциальной информации.
Б). Сеть, используемая для тестирования новых программных продуктов.
В). Сеть, содержащая общедоступные серверы, отделенная от внутренней сети. +
Г). Резервная сеть для аварийного восстановления.

7. К какой категории сетевых атак относится атака типа "отказ в обслуживании" (DoS)
А). Атаки на получение несанкционированного доступа.
Б). Атаки на нарушение целостности данных.

В). Атаки на нарушение доступности ресурсов. +
Г). Атаки на конфиденциальность данных.

8. Какой тип атак использует уязвимости в веб-приложениях для внедрения вредоносного SQL-кода?
А). Межсайтовый скриптинг (XSS).
Б). SQL-инъекция. +
В). Межсайтовая подделка запросов (CSRF).
Г). Переполнение буфера.

9. Какой метод обнаружения вторжений основывается на анализе сигнатур известных атак?
А). Аномальный метод обнаружения.
Б). Метод обнаружения на основе сигнатур. +
В). Метод обнаружения на основе протоколов.
Г). Метод обнаружения на основе статистики.

10. В каком режиме работы IDS только обнаруживает вторжения, не блокируя их?
А). Активный режим.
Б). Пассивный режим. +
В). Автоматический режим.
Г). Интерактивный режим.

11. Что такое VPN (Virtual Private Network)?
А). Физическая сеть, используемая для обеспечения безопасности данных.
Б). Технология, позволяющая создать защищенное соединение через публичную сеть. +
В). Локальная сеть с высоким уровнем безопасности.
Г). Протокол для шифрования электронной почты.

12. Какова основная цель использования VPN?
А). Увеличение скорости интернет-соединения.
Б). Обеспечение конфиденциальности и безопасности данных при передаче по незащищенным сетям. +
В). Сокрытие реального IP-адреса.
Г). Все вышеперечисленное.

13. Какой протокол VPN использует для установления защищенного соединения и шифрования трафика?
А). HTTP
Б). FTP
В). IPsec +
Г). SMTP

14. Какие типы VPN существуют в зависимости от назначения?
А). IPsec и SSL VPN.
Б). Site-to-Site VPN и Remote Access VPN. +
В). PPTP и L2TP.
Г). OpenVPN и WireGuard.

15. Какие системы обычно используются для управления технологическими процессами на промышленных предприятиях?
А). CRM-системы
Б). ERP-системы

В). SCADA-системы +
Г). SCM-системы

16. Каковы основные риски, связанные с использованием беспроводных сетей в критической инфраструктуре?
А). Перехват данных и несанкционированный доступ к контроллерам. +
Б). Снижение скорости интернет-соединения.
В). Повышенный расход электроэнергии.
Г). Сложность в настройке оборудования.

17. Какой стандарт информационной безопасности особенно важен для защиты критической инфраструктуры?
А). PCI DSS
Б). HIPAA
В). IEC 62443 +
Г). GDPR

18. Что такое "воздушный зазор" (air gap) в контексте промышленной безопасности?
А). Использование воздушного охлаждения для оборудования.
Б). Физическое отделение (изоляция) промышленной сети от внешних сетей (например, интернета). +
В). Использование беспроводной связи вместо проводной.
Г). Наличие свободного места на сервере.

19. Какие меры необходимо предпринять для усиления безопасности беспроводных сетей, используемых для управления SCADA-системами?
А). Использовать сложные пароли, шифрование и аутентификацию. +
Б). Регулярно менять SSID сети.
В). Подключать все устройства к одной беспроводной сети.
Г). Отключить шифрование для повышения скорости передачи данных.

20. Какое устройство может быть использовано для контроля доступа к беспроводной сети на промышленном предприятии?
А). Концентратор (Hub)
Б). Маршрутизатор с функциями межсетевого экрана. +
В). Репитер (Repeater)
Г). Антенна

21. Какие из перечисленных ниже мер относятся к организационным мерам защиты информации?
А). Использование межсетевого экрана.
Б). Настройка системы обнаружения вторжений.
В). Обучение персонала правилам информационной безопасности. +
Г). Шифрование данных.

22. Что такое honeypot в контексте сетевой безопасности?
А). Межсетевой экран.
Б). Система обнаружения вторжений.
В). Ловушка для злоумышленников, имитирующая уязвимый сервер. +
Г). Система для шифрования сетевого трафика.

23. Что такое DNP3 и Modbus в контексте промышленных сетей?

А). Стандарты беспроводной связи.
Б). Промышленные протоколы связи. +
В). Операционные системы для промышленных контроллеров.
Г). Антивирусные программы для SCADA-систем.

24. Соотнесите элементы из списка «характеристики межсетевого экрана» с соответствующими элементами из списка «описание».

Характеристики МЭ:	Описание:
1. Фильтрация пакетов	А) Обеспечивает защиту веб-приложений от атак, таких как SQL-инъекции и XSS.
2. Прокси-сервер	Б) Отслеживает состояние сетевых соединений для более точной фильтрации трафика.
3. Stateful Inspection	В) Осуществляет контроль трафика на основе правил, анализируя заголовки пакетов.
4. Web Application Firewall (WAF)	Г) Создает буферную зону между внутренней и внешней сетью для размещения общедоступных ресурсов.
5. DMZ (Demilitarized Zone)	Д) Действует как посредник, скрывая внутренние IP-адреса и обеспечивая дополнительный уровень безопасности.

Ответ: А4, Б3, В1, Г5, Д2

25. Вставьте пропущенное слово, чтобы получить правильное определение и описание, относящееся к моделям безопасности компьютерных систем.
___ - это модель защиты информации, в которой доступ к ресурсам предоставляется только после успешной аутентификации и в рамках установленных полномочий. (Контроль доступа)
Ответ:

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

Обновление оценочных материалов дисциплины

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____