Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Основы построения защищенных компьютерных сетей

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ПК-3. Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.4.1 Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания безопасности компьютерных систем и сетей.

ИОПК-1.4.2 Определяет уровень защищенности компьютерных систем и сетей и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-1.4.3 Оценивает соответствие механизмов безопасности требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИОПК-10.1 Понимает принципы формирования политики информационной безопасности в соответствии с нормативными требованиями.

ИОПК-10.2 Умеет организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности на защищаемом объекте.

ИОПК-10.3 Демонстрирует навыки формирования и реализации политики информационной безопасности на защищаемом объекте.

ИОПК-12.1 Понимает принципы работы информационных систем, средств обеспечения защиты информации, методики построения моделей угроз безопасности информации.

ИОПК-12.2 Демонстрирует навыки формирования исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ИПК-3.1. Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2. Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3. Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторные работы;

– контрольные задания и задачи.

Лабораторные работы (ОПК-1.4, ОПК-10, ОПК-12, ПК-3):

1. Сетевая атака: ARP Spoofing;
2. Сетевая атака: MAC Flooding;
3. Сетевая атака: MAC Spoofing;

4. Сетевая атака: VLAN Hopping;
5. Сетевая атака: IP Spoofing;
6. Сетевая атака STP Claiming Root Role
7. Сетевая атака: TCP Hijacking;
8. DoS- и DDoS-атаки.

Критерии оценивания лабораторных работ:

«Зачтено» – знание теоретического материала и умение реализовать изученные методы

«Не зачтено» – незнание большей части теоретического материала и неумение реализовать изученные методы

Примеры контрольных заданий (ИОПК-1.4.2, ИОПК-1.4.3, ИОПК-10.2, ИОПК-10.3, ИПК-3.1)

1. Проанализировать конфигурационный файл. Перечислить все недостатки и уязвимости конфигурации маршрутизатора.
2. Проанализировать конфигурационный файл и перечислить все способы получения конфигурации с устройства, настроенного в соответствии с этим файлом.
3. Для заданной атаки написать правило для IDS Suricata.

Примеры задач заданий (ИОПК-1.4.2, ИОПК-1.4.3, ИОПК-10.2, ИОПК-10.3, ИПК-3.1, ИПК-3.2)

1. Сгенерировать цепочку сертификатов (корневой, промежуточный, клиента, сервера и т.д.). Настроить аутентификацию клиента перед веб-сервером по сертификату.
2. На защищаемом сервере установить и настроить систему обнаружения и предотвращения атак Suricata или Snort. Написать следующие правила, реализующие:
   - обнаружение взаимодействия зараженных браузеров с сервером BeEF;
   - обнаружение атаки Heartbleed;
   - обнаружение атаки SSRF;
   - обнаружение вредоносного узла сети;
   - обнаружения эксплоита PHPMailer;
   - обнаружения эксплоита bnageTragic;
   - обнаружения эксплоита DROWN;
   - обнаружение атаки LDAP Injection.
3. В тестовом окружении реализовать атаку ARP Spoofing.
4. В тестовом окружении реализовать атаку MAC Flooding.
5. В тестовом окружении реализовать атаку HeartBleed.
6. В тестовом окружении реализовать атаку подбора паролей для SSH.
7. Настроить механизмы защиты от НСД маршрутизатора.
8. Настроить механизмы защиты от НСД коммутатора.

9. Обнаружить вредоносную активность по дапму сетевой активности.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен проводится в письменной форме по билетам. Экзаменационный билет содержит два теоретических вопроса. Примеры теоретических вопросов на экзамене (ИОПК-1.4.1, ИОПК-1.4.2, ИОПК-10.1, ИОПК-12.1, ИПК-3.1, ИПК-3.2, ИПК-3.3.)

1. Что такое атака на канальном уровне и каковы ее основные типы?
2. Как можно предотвратить ARP-спуфинг в локальной сети?
3. Опишите основные механизмы защиты, которые могут быть внедрены в переключателях.
4. Какие протоколы используются при создании VPN и в чем их отличия?
5. Что такое атака DoS и как она отличается от DDoS атаки?
6. Какие методы защиты существуют для снижения риска атак DDoS?
7. Каковы основные принципы безопасной конфигурации протоколов маршрутизации?
8. Какие функции выполняет протокол TLS?
9. Каково значение шифрования на транспортном уровне?
10. Что такое межсетевой экран и какие типы межсетевых экранов вы знаете?
11. Как межсетевые экраны помогают в защите сети?
12. В чем разница между сигнатурным и аномалийным обнаружением вторжений?
13. Каково назначение системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS)?
14. Какие инструменты используются для сканирования защищенности сетей?
15. Каковы шаги в процессе тестирования на проникновение?
16. Каким образом можно защитить сетевые устройства от несанкционированного доступа?
17. Каковы риски, связанные с использованием недокументированных функций в оборудовании?
18. Что такое VLAN и как он может улучшить безопасность в сети?
19. Зачем в сетевой безопасности используются списки контроля доступа (ACL)?
20. Как защитить данные, передаваемые через VPN?
21. Какие потенциальные уязвимости могут существовать в протоколах маршрутизации?
22. Каково влияние распределенных систем на защиту сетевой инфраструктуры?
23. Какие параметры могут использоваться для оценки защищенности сети?
24. Что такое нападение на уровне приложения и как оно связано с транспортным уровнем?
25. Какие ошибки часто допускаются при проектировании защищенных сетей?
26. Какую роль в безопасности сети играют обновления программного обеспечения?
27. Как можно анализировать и фиксировать инциденты безопасности в сети?
28. Каковы основные цели проектирования безопасных сетей?
29. Какие существуют ограничения и преимущества в использовании межсетевых экранов?
30. Как обеспечивается управление доступом к сетевым ресурсам?
31. Какие меры по устранению угрозы IP -спуфинга существуют?
32. Назначение протокола SNMP
33. Уязвимости протокола STP
34. Атаки на STP.
35. Методы и технологии защиты от атак канального уровня.
36. Протоколы GRE и IPSec.

37. Технология SYN Cookie и SYN Proxy.
38. Методы защиты от IP Spoofing.
39. Методы защиты протоколов маршрутизации.
40. Протоколы SSL/TLS.
41. Защищенная настройка TLS.
42. Защищенная настройка маршрутизаторов и коммутаторов.
43. Технологии NAT, statefiil inspection, stateless inspection.
44. Методы обнаружения вторжений в сетях.
45. Атаки MAC Flooding, MAC Spoofing, VLAN Hopping, ARP Spoofing.

Примеры экзаменационных билетов:
Билет 1
1. Что такое атака на канальном уровне и каковы ее основные типы?
2. В чем разница между сигнатурным и аномалийным обнаружением вторжений?

Билет 2
1. Какие протоколы используются при создании VPN и в чем их отличия?
2. Уязвимости протокола STP

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Условием допуска к экзамену является выполнение более 50% лабораторных работ. Сдача более 80% лабораторных работ является условием получения оценки «хорошо» или «отлично» на экзамене.

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; сдано более 80% лабораторных работ.

«Хорошо»: ответ на вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не исказившие содержание ответа; сдано более 80% лабораторных работ.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; сдано не менее 50% лабораторных работ.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей/наиболее важной части вопроса; сдано менее 50% лабораторных работ.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИОПК-1.4.1, ИОПК-1.4.2, ИОПК-10.1, ИОПК-12.1, ИПК-3.1, ИПК-3.2, ИПК-3.3.)

1. Методы обнаружения вторжений в сетях.
2. Каким образом можно защитить сетевые устройства от несанкционированного доступа?
3. Что такое атака DoS и как она отличается от DDoS атаки?
4. Атаки на STP.
5. Методы и технологии защиты от атак канального уровня.
6. Методы защиты от IP Spoofing.

7. Методы защиты протоколов маршрутизации.
8. Защищенная настройка маршрутизаторов и коммутаторов.
9. Атаки MAC Flooding,
10. Атаки MAC Spoofing,
11. Атаки VLAN Hopping,
12. Атаки ARP Spoofing.
13. Как защитить данные, передаваемые через VPN?
14. Какие меры по устранению угрозы IP -спуфинга существуют?
15. Какие функции выполняет протокол TLS?

Теоретические вопросы для проверки остаточных знаний предполагают краткое раскрытие основного содержания соответствующего вопроса.

Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности.