

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 защищённых компьютерных сетей

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

ОПК-18 Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик

ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик

ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях

ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности

ИОПК-18.2 Оценивает соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам

ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных

ИПК-3.1 Разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- лабораторные работы;
- контрольные задания и задачи.

Лабораторные работы (ИОПК-16.1, ИОПК-16.2, ИОПК-16.3, ИОПК-18.1, ИОПК-18.2, ИОПК-18.3, ИПК-3.1):

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: TCP Hijacking;
7. DoS- и DDoS-атаки.

Примеры контрольных заданий (ИОПК-16.1, ИОПК-16.2, ИОПК-16.3, ИОПК-18.1, ИОПК-18.2, ИОПК-18.3)

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

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

Вопросы к зачету (ИОПК-9.1, ИОПК-9.2)

1. Атаки на STP.
2. Методы и технологии защиты от атак канального уровня.
3. Протоколы GRE и IPSec.
4. Технология SYN Cookie и SYN Proxy.
5. Методы защиты от IP Spoofing.
6. Методы защиты протоколов маршрутизации.
7. Протоколы SSL/TLS.
8. Защищенная настройка TLS.
9. Защищенная настройка маршрутизаторов и коммутаторов.
10. Технологии NAT, stateful inspection, stateless inspection.
11. Методы обнаружения вторжений в сетях.
12. Атаки MAC Flooding, MAC Spoofing, VLAN Hopping, ARP Spoofing.

Результаты зачета с оценкой в седьмом семестре определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности.

«Хорошо»: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не искавшие содержание ответа.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей или наиболее важной части вопроса.

Результаты зачета в восьмом семестре определяются оценками

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

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

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

Теоретические вопросы (ИОПК-9.1, ИОПК-9.2)

1. Атаки на STP.
2. Методы и технологии защиты от атак канального уровня.
3. Методы защиты от IP Spoofing.
4. Методы защиты протоколов маршрутизации.
5. Протоколы SSL/TLS.
6. Защищенная настройка TLS.
7. Защищенная настройка маршрутизаторов и коммутаторов.
8. Технологии NAT, stateful inspection, stateless inspection.

9. Методы обнаружения вторжений в сетях.

10. Атаки MAC Flooding,

11. Атаки MAC Spoofing,

12. Атаки VLAN Hopping,

13. Атаки ARP Spoofing.

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.