Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе модуля)

# «Безопасность вычислительных сетей»

основной профессиональной образовательной программы специалитета по специальности

**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Специализация

**«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»**

ИНСТИТУТ цифровых технологий

РАЗРАБОТЧИК кафедра информационной безопасности

## 1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

| Код и наименование компетенции | Дисциплина | Результаты обучения (владения, умения и знания), соотнесенные с компетенциями |
|---|---|---|
| ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем; | Безопасность вычислительных сетей | *Знать:*<br>- способы реализации угроз безопасности в вычислительных сетях; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях;<br>- способы реализации угроз безопасности в вычислительных сетях;<br>- способы реализации угроз безопасности в автоматизированных системах;<br>- программно-аппаратные средства обеспечения защиты информации автоматизированных систем.<br>*Уметь:*<br>- определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты вычислительных сетей; - классифицировать и оценивать угрозы безопасности информации для автоматизированной системы;<br>- анализировать возможные уязвимости информационных систем;<br>- выявлять известные уязвимости информационных систем.<br>*Владеть:*<br>- навыком определения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем;<br>- навыком выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; |
| ОПК-13. Способен организовывать и проводить диагностику и тестирование систем | | |

| | | |
|---|---|---|
| защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем | | - навыком проведения оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах; |

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

- типовые задания по курсовому проекту;

- экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

1.3 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

| Система оценок / Критерий | **2** | **3** | **4** | **5** |
|---|---|---|---|---|
| | **0-40%** | **41-60%** | **61-80 %** | **81-100 %** |
| | **«неудовлетворительно»** | **«удовлетворительно»** | **«хорошо»** | **«отлично»** |
| | **«не зачтено»** | **«зачтено»** | | |
| **1 Системность и полнота знаний в отношении изучаемых объектов** | Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой) | Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект | Обладает набором знаний, достаточным для системного взгляда на изучаемый объект | Обладает полнотой знаний и системным взглядом на изучаемый объект |

| Система оценок / Критерий | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| | **0-40%** | **41-60%** | **61-80 %** | **81-100 %** |
| | **«неудовлетворительно»** | **«удовлетворительно»** | **«хорошо»** | **«отлично»** |
| | **«не зачтено»** | **«зачтено»** | | |
| **2 Работа с информацией** | Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи | Может найти необходимую информацию в рамках поставленной задачи | Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи | Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи |
| **3 Научное осмысление изучаемого явления, процесса, объекта** | Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений | В состоянии осуществлять научно корректный анализ предоставленной информации | В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные | В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи |
| **4 Освоение стандартных алгоритмов решения профессиональных задач** | В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки | В состоянии решать поставленные задачи в соответствии с заданным алгоритмом | В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма | Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи |

## 2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОПК-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

**Тестовые задания закрытого типа:**

1. Пакеты, передаваемые в рамках сессии PPTP, имеют в своей структуре:

a) заголовок канального уровня, используемый внутри Интернета, например, заголовок кадра Ethernet;

b) заголовок IP, содержащий адреса отправителя и получателя пакета;

c) заголовок общего метода инкапсуляции для маршрутизации GRE (Generic Routing Encapsulation);

d) исходный пакет PPP, включающий пакет IP, IPX или NetBEUI;

**e) заголовок TCP.**

2. Укажите протокол, который **НЕ** используется при аутентификации удаленного пользователя в реализации протокла PPTP:

a) протокол аутентификации по паролю PAP (Password Authentication Protocol);

**b) протокол IPSec;**

c) протокол аутентификации при рукопожатии MSCHAP (Microsoft Challenge-Hand-shaking Authentication Protocol);

протокол аутентификации EAP-TLS (Extensible Authentication ProtocolTransport Layer Security).

3. Протокол L2TP применяет в качестве транспорта протокол

**a) UDP**

b) ESP

c) AH

d) IP

4. В качестве порта отправителя и получателя протокол L2TP использует:

**a) UDP-порт 1701**

b) UDP-порт 1601

c) UDP-порт 1501

d) UDP-порт 1401

5. В зависимости от выбранного типа политики безопасности стека протоколов IPSec протокол L2TP может

**a) шифровать UDP-сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окончание IPSec ESP Authentication**

b) шифровать TCP-сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окончание IPSec ESP Authentication

c) шифровать ESP -сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окончание IPSec ESP Authentication

d) шифровать AH -сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окончание IPSec ESP Authentication

6. Укажите действие из списка ответов, которое происходит при приеме пакета данных по протоколу L2TP после обработки заголовка и окончания PPP.

**a) убирает заголовок IP**

b) добавляет заголовок IP

c) убирает заголовок ESP

d) убирает заголовок AH

7. Укажите тип аутентификации, который обеспечивает протокол L2TP, работающий поверх IPSec:

**a) аутентификацию на уровнях «пользователь» и «компьютер», а также выполняет аутентификацию и шифрование данных**

b) аутентификацию на уровне только «пользователь», а также выполняет аутентификацию и шифрование данных

**c)** аутентификацию на уровне только «компьютер», а также выполняет аутентификацию и шифрование данных

**d)** Протокол L2TP поверх IPSec не обеспечивает аутентификацию.

ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

**Тестовые задания открытого типа:**

8. Протокол L2TP. Согласно спецификации протокола L2TP, роль сервера для удаленного доступа провайдера должен выполнять:

**Ответ:** концентратор доступа **(LAC - L2TP Access Concentrator)**

9. Этапы формирования защищенного виртуального канала в протоколе L2TP:

**Ответ:**

**a)** установление соединения с сервером удаленного доступа локальной сети;

b) аутентификация пользователя;

c) тестирование туннеля;

d) конфигурирование защищенного туннеля.

10. Идентификатор, который присваивается новому соединению при создании туннеля между LAC и LNS протокола L2TP, называется:

**Ответ:** идентификатор вызова Call ID

11. Фильтры пакетов МЭ пропускают:

**Ответ:** содержание запросов HTTP;

12. Применение схемы NAT позволяет:

**Ответ:** использовать внутри организации пул IP-адресов меньшего размера.

13. Для различения соединений внешних и внутренних узлов при динамической трансляции NAT Overloading, когда отлаживается соответствие множества адресов локальной сети единственному IP-адресу, используются:

**Ответ:** номера портов (Port Address Translation, PAT).

14. Межсетевые экраны уровня соединения проверяют факт того, что пакет:

**Ответ:** является либо запросом на TCP-соединение, либо представляет данные, относящиеся к уже установленному соединению, либо относится к виртуальному соединению между двумя транспортными уровнями (достаточно привести один вариант из перечисленных)

15. Домен безопасности – это:

**Ответ:** собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

16. Модули PAM – это:

**Ответ:** набор открытых библиотек подключаемых модулей аутентификации

17. При успешной аутентификации пользователя по протоколу L2TP между концентратором доступа LAC провайдера и сервером LNS локальной сети создается:

**Ответ:** защищенный туннель

18. Каждая proxy-служба, являясь специфичной для каждого протокола, позволяет осуществить:

**Ответ:** усиленный контроль доступа, проверку данных, генерацию записей аудита.

19. Недостатки proxy-служб в следующем:

**Ответ:** служба proxy требует замены сетевого стека на сервере МЭ; слушает порт, но не может его использовать, большая временная задержка (входной пакет обрабатывается дважды – приложением и proxy), proxy уязвимы к ошибкам ОС и ПО прикладного уровня.

20. Домен безопасности Active Directory (AD ) – это:

**Ответ:** иерархическая служба каталога от компании Microsoft, которая используется в доменной среде Windows для организации и централизованного управления различными типами объектов: компьютерами, пользователями, серверами, принтерами. AD является центральным элементом управления и аутентификации в сетях Windows.

21. Правила, которые позволяют межсетевому экрану отслеживать состояние соединений и автоматически обновлять свои параметры в зависимости от текущей активности сети, называются:

**Ответ:** динамические правила

22. Правила МЭ, которые определяются заранее и **НЕ** изменяются в процессе работы системы, называются:

**Ответ:** статическими

23. Администратор имеет возможность создать правила, определяющие, какие протоколы или определенные виды трафика необходимо отслеживать. Когда соединение начинается с использованием отслеживаемого протокола, IPtables добавляет записи в таблицу состояний всего соединения. Запись в таблице состояний включает в себя следующую информацию:

**Ответ:**

− протокол, используемый для соединения;

− IP-адреса источника и назначения;

− номера портов источника и назначения;

− листинг с обращенными адресами и номерами портов (для контроля возвращаемого трафика);

− время, по истечению которого соединение будет удалено;

− состояние TCP-соединения (только для TCP); − состояние отслежива-емого соединения.

24. При принятии решения о разрешении прохождения пакета межсетевой экран проверит его последовательно по следующим структурам данных:

**Ответ:**

− таблица состояний

– зарегистрировано ли соединение для данного входящего пакета (если да, то пакет передается без дальнейшей проверки);

− политика безопасности

– если правило разрешает прохождение пакета, то пакет будет передан, а для его сеанса соединения будет добавлена запись в таблицу состояний.

25. Копирование конфигурации в режиме перезаписи в Cisco IOS осуществляется командой:

**Ответ:** router#copy running-config startup-config

26. Параметры интерфейсов, протоколов 2-го уровня, а также статистика отправленных и полученных кадров в режиме администратора просматривается командой:

**Ответ:** router#show interface

27. Краткая сводная таблица состояний IP-интерфейсов выводится командой:

**Ответ:** router#show ip interface brief

28. Просмотреть таблицу маршрутов можно по команде:

**Ответ:** router#**show ip route**

29. Маршрут по умолчанию (стандартный маршрут) назначается командой:

**Ответ:** router(config)#**ip route** 0.0.0.0 0.0.0.0

30. Просмотреть уровень доступа в системе и текущую конфигурацию можно командой:

**Ответ:** router#show privilege

31. Соединение по протоколу TCP оканчивается флагом:

Ответ: FIN

32. Соединение по протоколу TCP начинается флагом:

Ответ: ACK

## 3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

**Учебным планом предусмотрен курсовой проект. Иные типы работ данного раздела не предусматриваются**

Курсовой проект направлена на закрепление полученных теоретических знаний и приобретение умений и навыков в области выполнения настроек, эксплуатации средств ЗИ, поиска вредоносных объектов в ОС.

Тема 1. Сетевая безопасность с использованием МЭ

Цель углубление знаний в области обеспечения безопасности компьютерных сетей, изучение работы МЭ.

Задачи работы:

1. Исследовать специфику интеграции правил сетевой безопасности в МЭ.
2. Определить топологию сети и ее пропускную способность.
3. Сформулировать требования к безопасности сети
4. Настроить правила фильтрации пакетов в МЭ с учетом пропускной способности сети.
5. Провести имитацию атаки на сетевую инфраструктуру с подключенным МЭ.
6. Разработать алгоритм отражения атаки, отразить атаку, используя настройки межсетевого экрана.

Тема 2. Исследование стойкости защитных процессов ОС МЭ

Цель: изучение организации управления доступом в ОС МЭ, перекрытие несанкционированного доступа к учётным данным.

Задачи курсовой работы:

1. Исследовать ОС МЭ;

2. Изучить основы организации ОС МЭ;

3. Определить порядок внедрения правил безопасности.

4. Ознакомиться со средствами обеспечения безопасности в ОС МЭ при идентификации и аутентификации;

5. Внедрить правила контроля несанкционированного доступа с возможностью изменения прав пользователей с минимальным снижением пропускной способности сети.

Тема 3. Исследование защитных процессов ОС маршрутизатора.

Цель: изучение организации управления доступом протокола OSPF системе.

Задачи курсовой работы:

1. Исследовать специфику ИБ протокола OSPF;
2. Изучить основы организации маршрутизации на основе OSPF;
3. Определить правила безопасности для протокольной среды OSPF
4. Внедрить защиту протокола OSPF с возможностью изменения прав пользователей с минимальным снижением пропускной способности сети.
5. Проверить устойчивость маршрутизации при компрометирующем воздействии на траффик.

## 4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Безопасность вычислительных сетей» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Преподаватель-разработчик – В.В. Подтопельный

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29 августа 2024 г).

Председатель методической комиссии  О.С. Витренко