МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«Безопасность сетей ЭВМ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем,
специализация Анализ безопасности информационных систем

Ставрополь
2026

ЛАБОРАТОРНАЯ РАБОТА №1
НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ CISCO

Цель работы:
Ознакомление с основами конфигурации операционной системы Cisco IOS, получение практических навыков первоначальной настройки маршрутизаторов и коммутаторов, а также обеспечение базовой сетевой безопасности через интерфейс командной строки.

Теоретическая часть:
Операционная система Cisco IOS (Internetwork Operating System) представляет собой программное обеспечение, управляющее всеми функциями маршрутизаторов и коммутаторов Cisco. Настройка устройств с данной ОС осуществляется через CLI (Command Line Interface), где каждая команда влияет на конфигурацию, маршрутизацию и политику безопасности оборудования.

Основные режимы работы в CLI включают:
User EXEC Mode – предоставляет ограниченный доступ, обычно используется для базовой диагностики.
Privileged EXEC Mode – предоставляет доступ ко всем командам IOS.
Global Configuration Mode – позволяет вносить изменения в конфигурацию устройства.
Interface Configuration Mode – используется для настройки отдельных интерфейсов.

При первой настройке устройства особое внимание уделяется следующим задачам: установка имени устройства, настройка паролей доступа, конфигурация интерфейсов и базовые параметры безопасности.

Кроме того, следует учитывать, что правильная настройка безопасности на этапе установки существенно снижает риски несанкционированного доступа. Настройка паролей, отключение неиспользуемых служб, фильтрация по IP и применение списков контроля доступа (ACL) — базовые меры безопасности при работе с Cisco-устройствами.

Вопросы и задания
Вопросы для обсуждения:

1. Какие существуют режимы доступа в интерфейсе CLI на оборудовании Cisco?
2. Чем отличается пользовательский режим от привилегированного?
3. Что представляет собой глобальный конфигурационный режим и как в него перейти?
4. Какие базовые меры безопасности применяются при начальной настройке устройств Cisco?
5. Что такое пароли Enable, Console и VTY? В чём их назначение?
6. Зачем используется команда `copy running-config startup-config`?
7. Как можно ограничить доступ к маршрутизатору или коммутатору?
8. Какие существуют виды интерфейсов и как их настраивать?
9. Что такое баннер приветствия и зачем он нужен?
10. Как осуществляется сохранение конфигурации на устройстве Cisco?

Практические задания
Задание 1. Выполните первичную настройку маршрутизатора или коммутатора Cisco:

1. Назначьте имя устройству командой `hostname`.
2. Установите пароль для режима `enable`.
3. Настройте пароль на консольный вход и доступ по VTY.
4. Включите шифрование паролей с помощью команды `service password-encryption`.

Задание 2. Настройте IP-адреса на одном или нескольких интерфейсах устройства:

1. Войдите в интерфейс с помощью команды `interface`.
2. Присвойте IP-адрес с использованием `ip address`.
3. Активируйте интерфейс командой `no shutdown`.

Задание 3. Настройте баннер приветствия (`banner motd`), содержащий уведомление о правилах доступа к системе.

Задание 4. Сохраните текущую конфигурацию устройства:

1. Сначала выполните команду `copy running-config startup-config`.
2. Перезагрузите устройство и проверьте, что настройки сохранились.

Задание 5. Проведите тестирование подключения к устройству с помощью команды `ping`, убедитесь в корректности IP-настроек.

Задание 6. Используя таблицу ниже, отразите различия между командами настройки в различных режимах Cisco CLI:

Режим CLI	Команда входа	Основные возможности
User EXEC	`>`	Базовые команды мониторинга
Privileged EXEC	`enable`	Все команды, включая сохранение настроек
Global Configuration	`configure terminal`	Конфигурация системы в целом
Interface Configuration	`interface [name]`	Настройка конкретного интерфейса

Вывод:
В результате выполнения лабораторной работы студент получает навыки первоначальной настройки оборудования Cisco, знакомится с многоуровневой структурой интерфейса командной строки, осваивает базовые меры безопасности и учится правильно документировать и сохранять настройки. Эти знания составляют основу любой сетевой практики и необходимы для дальнейшего изучения маршрутизации, коммутации и обеспечения информационной безопасности сетей.

ЛАБОРАТОРНАЯ РАБОТА №2
ЗАЩИТА ИНФРАСТРУКТУРЫ МАРШРУТИЗАЦИИ

Цель работы:
Освоение методов и средств обеспечения безопасности инфраструктуры маршрутизации в IP-сетях. Получение практических навыков настройки механизмов защиты маршрутизаторов, маршрутов и маршрутизируемого трафика.

Теоретическая часть:
Инфраструктура маршрутизации является ключевым компонентом любой сетевой архитектуры. Нарушение её работоспособности может привести к потере связи между сетевыми сегментами, перехвату трафика, перенаправлению маршрутов (атаки типа route hijacking) и другим угрозам. Поэтому безопасность маршрутизации — одна из важнейших задач сетевого администратора.

Существует два типа маршрутизации: статическая и динамическая. При динамической маршрутизации широко используются протоколы RIP, EIGRP, OSPF, BGP. Несмотря на их функциональность, эти протоколы могут стать объектами различных атак: подделка обновлений маршрутов, инъекции ложных маршрутов, DoS-атаки на маршрутизаторы.

Методы защиты маршрутизации включают в себя:

- Аутентификацию маршрутизаторов друг перед другом (например, с использованием MD5 или SHA);
- Фильтрацию маршрутов (route filtering);
- Использование Access Control Lists (ACL) для ограничения доступа к маршрутизатору;
- Контроль целостности маршрутов и блокировку нестандартных обновлений;
- Разделение плоскости управления (management plane), плоскости передачи данных (data plane) и плоскости маршрутизации (control plane).

В Cisco IOS для защиты используются команды настройки фильтров, списков доступа, механизмов аутентификации в протоколах маршрутизации, а также Control Plane Policing (CoPP) и Management Plane Protection (MPP).

Вопросы и задания
Вопросы для обсуждения:

1. В чём заключается угроза безопасности при использовании динамической маршрутизации?
2. Как работает аутентификация маршрутизаторов в протоколах OSPF и EIGRP?
3. Что такое фильтрация маршрутов и как она может быть реализована?
4. Какие механизмы в Cisco IOS используются для защиты плоскости управления и маршрутизации?
5. Что такое CoPP и как он защищает маршрутизатор?
6. Как осуществляется настройка ACL для защиты маршрутизатора?
7. В чём различие между control plane и data plane?

8. Какие команды позволяют отслеживать попытки несанкционированного изменения маршрутов?

Практические задания
Задание 1. Настройка аутентификации маршрутизаторов в сети OSPF:

1. Задайте идентификаторы маршрутизаторов (router-id).
2. Включите OSPF на интерфейсах и активируйте аутентификацию.
3. Примените ключ аутентификации с использованием MD5.
4. Проверьте состояние соседства командой `show ip ospf neighbor`.

Задание 2. Реализуйте базовую защиту маршрутизатора с помощью ACL:

1. Создайте стандартный ACL, разрешающий доступ только с определённых IP-адресов.
2. Примените ACL к интерфейсу на входящем трафике.
3. Проверьте работу фильтрации с помощью `ping` и `telnet`.

Задание 3. Настройка фильтрации маршрутов:

1. Определите список маршрутов, которые необходимо отфильтровать.
2. Создайте prefix-list или route-map, ограничивающую распространение этих маршрутов.
3. Примените фильтрацию на соответствующем интерфейсе или в настройках протокола маршрутизации.

Задание 4. Реализуйте защиту control plane с помощью CoPP:

1. Создайте class-map и policy-map для разрешённого трафика (например, SSH, ICMP).
2. Примените политику на control plane командой `control-plane`.
3. Проверьте фильтрацию и статистику с помощью `show policy-map control-plane`.

Задание 5. Настройка Management Plane Protection (MPP):

1. Ограничьте доступ к устройству через Telnet/SSH только на определённых интерфейсах.
2. Проверьте доступ с разрешённых и запрещённых IP-адресов.

Вывод:
В рамках лабораторной работы были рассмотрены и практически реализованы механизмы защиты маршрутизируемой инфраструктуры, включая аутентификацию, фильтрацию маршрутов, списки доступа и защиту управляющей плоскости маршрутизатора. Эти меры позволяют значительно повысить устойчивость сетевой архитектуры к внешним и внутренним угрозам, обеспечить целостность и доверенность маршрутов, а также ограничить несанкционированный доступ к управлению маршрутизаторами. При

грамотной настройке защиты маршрутизации достигается высокий уровень информационной безопасности в локальных и корпоративных сетях.

ЛАБОРАТОРНАЯ РАБОТА №3
ЗАЩИТА ИНФРАСТРУКТУРЫ КОММУТАЦИИ

Цель работы:
Изучить потенциальные угрозы, связанные с коммутацией в локальных сетях, и овладеть методами защиты коммутаторов и связанных с ними технологий, включая VLAN, STP, ARP, а также контроль доступа к портам.

Теоретическая часть:
Коммутационные устройства (коммутаторы) играют ключевую роль в построении локальных сетей. В отличие от маршрутизаторов, они функционируют в канальном уровне модели OSI и обеспечивают соединение конечных устройств внутри одного или нескольких сегментов сети. Коммутаторы управляют фреймами на основе MAC-адресов и таблиц коммутации.

Однако именно в силу своей архитектуры и места в сетевой топологии коммутаторы уязвимы к ряду атак, среди которых:

- **MAC flooding** — переполнение таблицы коммутации для перевода устройства в режим широковещательной передачи;
- **ARP spoofing** — подделка ARP-ответов для перехвата трафика;
- **VLAN hopping** — несанкционированный доступ к другим VLAN;
- **BPDU spoofing** — вмешательство в работу протокола STP;
- **Подключение неавторизованных устройств**.

Методы защиты коммутационной инфраструктуры включают:

- Настройку защиты от MAC flooding (Port Security);
- Защиту ARP с помощью DHCP snooping и Dynamic ARP Inspection (DAI);
- Использование Private VLAN для изоляции устройств в одной VLAN;
- Защиту от VLAN hopping с использованием правильной конфигурации trunk-портов и удаления неиспользуемых VLAN;
- Внедрение контроля доступа к портам с ограничением количества MAC-адресов;
- Использование BPDU Guard и Root Guard для защиты STP-дерева.

Современные коммутаторы Cisco предоставляют все необходимые функции безопасности через команды Cisco IOS, которые позволяют гибко и точно контролировать поведение сети на уровне канального уровня.

Вопросы и задания

Вопросы для обсуждения:

1. Какие угрозы характерны для уровня коммутации?

2. В чём заключается атака MAC flooding и как от неё защититься?
3. Что такое VLAN hopping и как его предотвратить?
4. Как работает Port Security и какие режимы он поддерживает?
5. Для чего используются DHCP snooping и DAI?
6. В чём разница между BPDU Guard и Root Guard?
7. Что такое Private VLAN и где целесообразно её применять?
8. Как можно ограничить доступ к портам коммутатора?

Практические задания

Задание 1. Настройка Port Security на коммутаторе:

1. Назначьте порт в access-режим и привяжите его к конкретной VLAN.
2. Ограничьте число допустимых MAC-адресов (например, один MAC).
3. Настройте режим ограничения: protect, restrict или shutdown.
4. Проверьте срабатывание защиты при подключении другого устройства.

Задание 2. Защита от атак VLAN hopping:

1. Запретите автоматическое согласование trunk'а с помощью команды `switchport nonegotiate`.
2. Настройте trunk-порт и явно определите разрешённые VLAN.
3. Убедитесь, что нежелательные VLAN недоступны.

Задание 3. DHCP snooping и Dynamic ARP Inspection:

1. Включите DHCP snooping на уровне VLAN и настройте доверенные порты.
2. Включите DAI и свяжите его с DHCP snooping-базой.
3. Выполните проверку: скомпрометируйте ARP-ответ с недоверенного порта и убедитесь, что он блокируется.

Задание 4. Защита STP с помощью BPDU Guard и Root Guard:

1. Назначьте порт edge (граничным) и активируйте BPDU Guard.
2. Включите Root Guard на портах, которые не должны стать Root.
3. Смоделируйте попытку атаки и проверьте защитные действия.

Задание 5. Настройка Private VLAN:

1. Создайте основную и изолированные/общие под-VLAN.
2. Назначьте порты и роли: isolated, community, promiscuous.
3. Проверьте доступность между хостами в разных под-VLAN.

Вывод:
В ходе лабораторной работы были рассмотрены основные угрозы, связанные с коммутацией в локальных сетях, а также реализованы на практике методы защиты инфраструктуры коммутации. Настройка механизмов защиты — таких как Port Security,

DHCP snooping, DAI, BPDU Guard, Private VLAN — обеспечивает устойчивость коммутаторов к типовым атакам, предотвращает несанкционированный доступ к сетевым ресурсам и повышает общий уровень информационной безопасности. Эти навыки являются необходимыми для проектирования, администрирования и эксплуатации современных защищённых сетей.

ЛАБОРАТОРНАЯ РАБОТА №4
ЗАЩИТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (ЛВС) ОТ ПЕТЕЛЬ НА КАНАЛЬНОМ УРОВНЕ

Цель работы:
Изучить причины возникновения петель в сетях Ethernet, рассмотреть механизмы, предотвращающие их формирование, и на практике реализовать защиту от петель на уровне коммутаторов с использованием протоколов Spanning Tree (STP), Rapid Spanning Tree (RSTP), а также технологий защиты, таких как BPDU Guard, Loop Guard и PortFast.

Теоретическая часть:
Петля на канальном уровне возникает, когда два и более пути соединяют одно и то же множество коммутаторов без должной фильтрации широковещательного и многоадресного трафика. Из-за отсутствия механизма TTL (в отличие от сетевого уровня) широковещательные фреймы начинают бесконечно циркулировать в замкнутом контуре. Это приводит к серьёзным последствиям: перегрузке каналов связи, росту задержек, отказу в обслуживании и даже полной блокировке сети.

Для борьбы с этим явлением применяются протоколы семейства Spanning Tree Protocol (STP), целью которых является построение дерева без петель (spanning tree), в рамках которого один путь между любыми двумя коммутаторами остаётся активным, а дублирующие соединения переводятся в резерв.

Ключевые понятия:

- **STP (IEEE 802.1D)** — классический протокол построения дерева без петель. Медленно реагирует на изменения в топологии.
- **RSTP (IEEE 802.1w)** — усовершенствованная версия STP с более быстрым временем сходимости.
- **BPDU (Bridge Protocol Data Unit)** — служебные кадры, используемые STP для обмена информацией между коммутаторами.
- **PortFast** — ускоряет переход порта в состояние forwarding при подключении конечного устройства.
- **BPDU Guard** — отключает порт при получении BPDU-кадра на порту с включенным PortFast.
- **Loop Guard** — предотвращает возврат порта в активное состояние при потере BPDU на канале связи.
- **Root Guard** — защищает от смены корневого коммутатора.

Значение защиты от петель:
Поскольку ЛВС часто строится с избыточными связями для повышения

отказоустойчивости, возникает опасность ошибочной конфигурации или физического подключения, ведущего к петлям. Без механизмов STP сеть может выйти из строя за считаные секунды после появления замкнутого контура.

Вопросы и задания

Вопросы для самоконтроля:

1. Что такое петля на канальном уровне и почему она опасна?
2. Как работает STP и какие состояния может принимать порт?
3. Чем RSTP отличается от STP?
4. Что такое PortFast и когда его следует использовать?
5. Как BPDU Guard защищает сеть от петель?
6. В каких случаях применяется Loop Guard?
7. Каков порядок определения корневого коммутатора в STP?

Практические задания

Задание 1. Симуляция петли в ЛВС

1. Постройте простую топологию из трёх коммутаторов с резервными соединениями.
2. Отключите STP на коммутаторах и проверьте, как широковещательный трафик влияет на сеть.
3. Проанализируйте поведение сети в условиях петли.

Задание 2. Настройка STP/RSTP

1. Включите STP (или RSTP) на всех коммутаторах.
2. Назначьте один коммутатор вручную как root bridge.
3. Проверьте состояние портов и убедитесь в построении дерева без петель.
4. Измените топологию и проанализируйте время сходимости.

Задание 3. PortFast и BPDU Guard

1. Назначьте порты, подключённые к ПК, как PortFast.
2. Включите BPDU Guard на этих портах.
3. Подключите к ним другой коммутатор и проверьте отключение порта при получении BPDU.

Задание 4. Loop Guard

1. Активируйте Loop Guard на корневых портах резервного соединения.
2. Симулируйте потерю BPDU между коммутаторами.
3. Убедитесь, что порты остаются заблокированными для предотвращения петель.

Вывод:
В ходе лабораторной работы были рассмотрены причины возникновения петель в ЛВС и

реализованы основные механизмы защиты от них. Использование STP и его производных, таких как RSTP, а также включение PortFast, BPDU Guard и Loop Guard обеспечивают стабильность и безопасность канального уровня сети. Практические навыки по настройке данных функций позволяют своевременно предотвращать аварийные ситуации и гарантировать бесперебойную работу сетевой инфраструктуры.

ЛАБОРАТОРНАЯ РАБОТА №5
ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Цель работы:
Изучить методы и механизмы обеспечения безопасности сетевой инфраструктуры, ознакомиться с уязвимостями, присущими сетевым устройствам и протоколам, и отработать практические навыки по реализации политики безопасности в корпоративной сети.

Теоретическая часть:
Сетевая инфраструктура — это совокупность оборудования и программного обеспечения, обеспечивающая взаимодействие всех элементов компьютерной сети. Она включает маршрутизаторы, коммутаторы, брандмауэры, серверы, каналы передачи данных и сетевые протоколы. Современные угрозы для сетевой инфраструктуры охватывают широкий спектр атак: от банального несанкционированного доступа до сложных сетевых атак, таких как spoofing, man-in-the-middle, DDoS и других.

Надёжная защита сетевой инфраструктуры требует комплексного подхода, включающего как технические, так и организационные меры. Среди них — сегментирование сети, настройка списков контроля доступа (ACL), фильтрация трафика, контроль целостности, аутентификация устройств, шифрование данных, настройка правил безопасности и постоянный мониторинг событий.

Основные направления защиты:
1. Безопасная конфигурация устройств.
Необходимо удалить или отключить неиспользуемые службы, сменить пароли по умолчанию, применить минимально необходимые привилегии и использовать защищённые каналы администрирования (например, SSH вместо Telnet).

2. Контроль доступа.
Списки контроля доступа позволяют ограничить доступ к управлению устройствами и сетевым ресурсам на основе IP-адресов, портов и протоколов.

3. VLAN и сегментация.
Разделение сети на логические сегменты позволяет изолировать критические ресурсы и ограничить распространение потенциальных атак.

4. Протоколы безопасности.
Использование аутентифицированных протоколов маршрутизации (например, OSPF с MD5, EIGRP с ключами) препятствует вмешательству в таблицы маршрутизации.

5. Защита от атак типа MAC flooding, DHCP spoofing, ARP poisoning.
Для этого применяются функции динамического ARP-инспектирования, DHCP snooping, портовая безопасность (Port Security) и настройка защиты уровня 2.

6. Логирование и аудит.
Настройка систем журналирования позволяет своевременно обнаруживать и расследовать инциденты безопасности.

7. Регулярное обновление прошивок и патчей.
Все сетевые устройства должны поддерживаться в актуальном состоянии, чтобы исключить известные уязвимости.

Вопросы и задания

Вопросы для самоконтроля:

1. Какие элементы входят в состав сетевой инфраструктуры?
2. Какие виды угроз наиболее характерны для сетевых устройств?
3. Что такое ACL и как они применяются для фильтрации трафика?
4. Какие преимущества даёт сегментирование сети с помощью VLAN?
5. Как осуществляется защита от MAC-флудинга и ARP-спуфинга?
6. В чём заключается важность протоколов безопасности при маршрутизации?
7. Почему важно использовать безопасные протоколы администрирования?

Практические задания

Задание 1. Безопасная настройка коммутатора и маршрутизатора
Настройте базовую защиту устройств Cisco:
– отключите неиспользуемые порты и службы
– задайте уникальные пароли и включите шифрование паролей
– настройте доступ к консоли и через SSH
– создайте резервное копирование конфигурации на удалённый сервер

Задание 2. Настройка списков контроля доступа (ACL)
– Создайте расширенные ACL для ограничения доступа к административному интерфейсу устройств
– Настройте фильтрацию входящего и исходящего трафика по IP-адресам и портам
– Проверьте работу ACL, подключаясь к устройствам из разных подсетей

Задание 3. Реализация VLAN и межвлановой фильтрации
– Разделите сеть на VLAN: администрация, пользователи, серверы
– Ограничьте взаимодействие между VLAN, кроме специально разрешённых
– Настройте DHCP Snooping, Dynamic ARP Inspection и Port Security

Задание 4. Защита протоколов маршрутизации
– Настройте аутентификацию для OSPF/EIGRP
– Внесите изменения в конфигурацию, протестируйте устойчивость к подмене маршрутов

– Проанализируйте журнал безопасности при отключении/вмешательстве в процесс маршрутизации

Задание 5. Логирование и аудит
– Настройте отправку логов с маршрутизатора на syslog-сервер
– Реализуйте логирование входов и команд администрирования
– Проанализируйте журналы на наличие подозрительных событий

Вывод:
В ходе выполнения лабораторной работы обучающиеся освоили ключевые подходы к защите сетевой инфраструктуры. Были рассмотрены методы защиты от наиболее распространённых угроз, такие как межсетевое экранирование, контроль доступа, сегментирование сети и настройка протоколов безопасности. Практические навыки позволили закрепить понимание важности комплексной защиты сетевых устройств и протоколов, что является основой надёжного функционирования всей ИТ-инфраструктуры предприятия.

ЛАБОРАТОРНАЯ РАБОТА №6
ЗАЩИТА ПЕРИМЕТРА СЕТИ

Цель работы:
Изучить теоретические и практические аспекты защиты сетевого периметра, познакомиться с архитектурой систем периметральной безопасности, освоить методы настройки межсетевых экранов и фильтрации трафика для предотвращения несанкционированного доступа.

Теоретическая часть:
Периметр сети представляет собой границу между внутренней локальной сетью организации и внешними сетями, в первую очередь — с сетью Интернет. Защита периметра является важнейшей составляющей общей политики информационной безопасности, поскольку именно через периметр чаще всего совершаются попытки несанкционированного доступа, атак и распространения вредоносного программного обеспечения.

Традиционно защита периметра основывается на использовании межсетевых экранов (firewall), систем обнаружения и предотвращения атак (IDS/IPS), шлюзов безопасности, NAT/PAT, а также систем контроля и мониторинга трафика. Помимо этого, активно применяются прокси-серверы, системы фильтрации веб-контента и почтовых сообщений, DMZ-сегментация и другие элементы.

Ключевые аспекты защиты периметра:

1. Межсетевые экраны (firewalls).
Основное средство защиты, выполняющее фильтрацию сетевого трафика на основе заданных правил. Современные брандмауэры могут функционировать на нескольких уровнях модели OSI, включая уровень приложений.

2. NAT и PAT.
Механизмы трансляции адресов позволяют скрыть внутреннюю структуру сети от внешнего мира, обеспечивая тем самым дополнительную степень защиты.

3. Демилитаризованная зона (DMZ).
Это сегмент сети, в котором размещаются общедоступные серверы (веб-серверы, почтовые сервера, DNS и т. д.). Сегмент изолируется от внутренней сети и защищается как с внешней, так и с внутренней стороны.

4. IDS/IPS.
Системы обнаружения и предотвращения вторжений анализируют сетевой трафик в режиме реального времени, выявляя подозрительные или аномальные действия.

5. Прокси-серверы и контент-фильтрация.
Применяются для контроля и ограничения доступа пользователей к веб-ресурсам, фильтрации входящей информации, сканирования на наличие угроз и соблюдения корпоративной политики безопасности.

6. Виртуальные частные сети (VPN).
Используются для безопасного соединения удалённых пользователей и филиалов с внутренней сетью предприятия через зашифрованные каналы.

Вопросы и задания

Вопросы для самоконтроля:

1. Что такое сетевой периметр и какие угрозы для него характерны?
2. Какую роль играет межсетевой экран в архитектуре безопасности?
3. Чем отличаются NAT и PAT?
4. В чём суть концепции DMZ и какие преимущества она даёт?
5. Как работают IDS и IPS?
6. Почему важно применять контент-фильтрацию на уровне периметра?
7. Какие риски могут быть связаны с отсутствием защиты периметра?

Практические задания

Задание 1. Настройка межсетевого экрана
– Настройте брандмауэр на маршрутизаторе Cisco, определите правила доступа:
– Разрешить только веб-трафик (HTTP/HTTPS) из внутренней сети наружу
– Запретить входящие подключения снаружи за исключением определённого IP
– Проверить логирование всех отклонённых соединений

Задание 2. Конфигурация DMZ-сегмента
– Организуйте DMZ для размещения веб-сервера
– Настройте правила доступа: внутренним пользователям — полный доступ, внешним — только по HTTP
– Обеспечьте мониторинг сетевого трафика между сегментами

Задание 3. Применение NAT и PAT
– Настройте трансляцию внутренних IP-адресов на внешний
– Реализуйте статический NAT для доступа к серверу из интернета
– Используйте PAT для организации доступа нескольких клиентов через один внешний IP

Задание 4. Установка и настройка IDS/IPS (на симуляторе или стенде)
– Ознакомьтесь с интерфейсом системы
– Настройте сигнатуры атак и автоматическую реакцию
– Проведите имитацию атаки и проанализируйте результат

Задание 5. Контент-фильтрация и прокси-сервер
– Установите прокси-сервер Squid или аналог
– Настройте фильтрацию доступа к веб-ресурсам по категориям
– Ограничьте доступ к социальным сетям и видео-сайтам

Вывод:
Защита периметра сети — один из фундаментальных элементов построения надёжной системы информационной безопасности. В ходе лабораторной работы обучающиеся познакомились с архитектурой периметральной защиты, освоили методы настройки брандмауэров, NAT, организации DMZ и внедрения IDS/IPS. Практические упражнения закрепили навыки конфигурирования и анализа сетевых устройств и сервисов, что является необходимым условием для обеспечения устойчивости и безопасности корпоративной сети.

ЛАБОРАТОРНАЯ РАБОТА №7
ЗАЩИТА ЛВС ОТ АТАК КАНАЛЬНОГО УРОВНЯ

Цель работы:
Ознакомиться с основными типами атак на канальном уровне модели OSI, изучить методы их обнаружения и предотвращения, освоить настройку защитных механизмов на сетевом оборудовании для повышения устойчивости локальной вычислительной сети (ЛВС) к подобным угрозам.

Теоретическая часть:
Канальный уровень модели OSI отвечает за надёжную передачу кадров данных между двумя узлами, расположенными в одной физической сети. Он играет критически важную роль в функционировании ЛВС, особенно в средах с коммутацией, таких как Ethernet. Атаки на этом уровне часто направлены на уязвимости протоколов или ошибок в конфигурации сетевых устройств.

Наиболее распространённые типы атак канального уровня:

1. MAC flooding (переполнение таблицы MAC-адресов)
При атаке типа MAC flooding злоумышленник отправляет большое количество кадров с поддельными MAC-адресами, заполняя таблицу коммутации коммутатора. Когда таблица переполняется, коммутатор начинает рассылать кадры на все порты, превращаясь в концентратор. Это позволяет перехватывать трафик, не предназначенный атакующему.

2. ARP spoofing (или ARP poisoning)
В данной атаке злоумышленник отправляет фальшивые ARP-ответы, заставляя другие устройства считать его MAC-адрес допустимым для конкретного IP. Это позволяет выполнять перехват трафика (Man-in-the-Middle), модификацию данных или отказ в обслуживании.

3. VLAN hopping (перепрыгивание между VLAN)
Некорректно настроенные VLAN могут быть подвержены атакам, при которых злоумышленник получает доступ к трафику из другого VLAN, что нарушает логическую сегментацию сети.

4. BPDU spoofing
Атака на протокол STP, при которой злоумышленник отправляет ложные BPDU-сообщения, чтобы изменить топологию сети и перенаправить трафик.

Методы защиты ЛВС от атак канального уровня:

Port Security — ограничение количества MAC-адресов, допустимых на порту коммутатора. Может быть настроен как на фиксированный список, так и на динамически обучаемые адреса с автоматической блокировкой при нарушении.

Dynamic ARP Inspection (DAI) — технология, позволяющая проверять ARP-пакеты, сопоставляя их с доверенными источниками (DHCP Snooping) и блокировать подозрительные ARP-ответы.

DHCP Snooping — предотвращает подделку DHCP-серверов путём маркировки портов как доверенных или недоверенных. Позволяет строить базу соответствий IP-MAC и портов.

BPDU Guard и Root Guard — функции защиты от атак на STP. BPDU Guard отключает порт при получении неожиданного BPDU-сообщения, а Root Guard предотвращает изменение корневого коммутатора.

VLAN segregation и настройка Native VLAN — правильная настройка VLAN, включая запрет trunk'ов на неиспользуемых портах и указание нестандартной Native VLAN, снижает риск VLAN hopping.

Вопросы и задания

Вопросы для самоконтроля:

1. В чём заключается угроза атаки MAC flooding и как она реализуется?
2. Опишите процесс ARP spoofing и его последствия.
3. Какие меры позволяют противостоять VLAN hopping?
4. Чем отличаются BPDU Guard и Root Guard?
5. Как связаны технологии DHCP Snooping и Dynamic ARP Inspection?
6. Какие признаки могут указывать на реализацию атаки на канальном уровне?

Практические задания

Задание 1. Настройка Port Security на коммутаторе Cisco
– Ограничьте количество MAC-адресов на порту
– Установите режим "restrict" или "shutdown" при нарушении
– Проведите тест с подключением нового устройства и проверьте реакцию системы

Задание 2. Включение и конфигурация DHCP Snooping
– Определите доверенные и недоверенные порты
– Проверьте работу DHCP Snooping в тестовой сети
– Ознакомьтесь с таблицей соответствия IP–MAC–порт

Задание 3. Реализация Dynamic ARP Inspection
– Активируйте DAI на коммутаторе
– Настройте фильтрацию ARP на основе DHCP Snooping
– Проведите имитацию ARP spoofing и проверьте реакцию системы

Задание 4. Внедрение BPDU Guard
– Настройте защиту на портах доступа
– Отправьте тестовое BPDU-сообщение и зафиксируйте поведение коммутатора

Задание 5. Анализ VLAN hopping и устранение уязвимостей
– Проверьте настройки trunk-портов и Native VLAN
– Настройте запрет trunk'ов на портах доступа
– Убедитесь в изоляции трафика между VLAN

Вывод:
Атаки на канальном уровне являются одними из самых скрытных, но потенциально разрушительных угроз в структуре ЛВС. Их успешное обнаружение и предотвращение требует не только понимания сетевых протоколов и архитектуры Ethernet, но и грамотной настройки сетевого оборудования. В ходе лабораторной работы были рассмотрены как типовые векторы атак, так и эффективные способы защиты, включая использование DHCP Snooping, Port Security, DAI и других функций. Это формирует у студентов навыки создания защищённых сетевых инфраструктур и понимание важности комплексной защиты на всех уровнях взаимодействия.

ЛАБОРАТОРНАЯ РАБОТА №8
ПОСТРОЕНИЕ МАРШРУТИЗИРУЕМОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (ЛВС)

Цель работы:
Овладеть навыками проектирования и настройки маршрутизируемой локальной вычислительной сети, научиться применять маршрутизацию для обеспечения связности между сегментами сети, а также изучить базовые принципы IP-адресации, протоколов маршрутизации и конфигурации маршрутизаторов.

Теоретическая часть:
Маршрутизируемая ЛВС представляет собой сеть, разделённую на несколько логических или физических сегментов (подсетей), соединённых между собой через маршрутизаторы. Такие сети применяются в организациях, где необходимо логическое разделение трафика, контроль доступа и оптимизация маршрутов передачи данных. Применение маршрутизации позволяет повысить производительность и безопасность сети, ограничить широковещательный трафик и гибко управлять маршрутом прохождения данных.

Ключевые понятия:

1. IP-адресация и подсетирование
Каждому устройству в сети присваивается уникальный IP-адрес. В рамках одной ЛВС может быть несколько подсетей, для каждой из которых требуется своя маска. Подсетирование позволяет эффективно использовать адресное пространство и организовывать маршрутизацию между сегментами.

2. Маршрутизатор (Router)
Сетевое устройство, обеспечивающее пересылку пакетов между различными подсетями. Использует таблицы маршрутизации для определения наилучшего пути следования данных.

3. Таблица маршрутизации
Это база данных, хранящая информацию о возможных маршрутах до различных сетей. В таблице указывается сеть назначения, шлюз (next hop), интерфейс и метрика (стоимость маршрута).

4. Типы маршрутизации

- **Статическая маршрутизация** — маршруты прописываются вручную администратором. Подходит для небольших или стабильных сетей.
- **Динамическая маршрутизация** — используется протокол маршрутизации (например, RIP, OSPF), который позволяет маршрутизаторам автоматически обмениваться маршрутной информацией и перестраивать маршруты при изменениях в сети.

5. Протоколы маршрутизации

- **RIP (Routing Information Protocol)** — простой протокол, использующий количество переходов как метрику.
- **OSPF (Open Shortest Path First)** — более сложный протокол, использующий метрику на основе стоимости интерфейса, обеспечивает быструю конвергенцию и масштабируемость.
- **EIGRP, BGP** — протоколы, применяемые в более крупных или межсетевых инфраструктурах.

6. VLAN и маршрутизация между VLAN
В случае использования виртуальных локальных сетей (VLAN) необходима

маршрутизация между ними. Это может быть реализовано с помощью маршрутизатора (Router-on-a-stick) или многослойного коммутатора (Layer 3 switch).

Практические задания

Задание 1. Проектирование маршрутизируемой ЛВС
– Определите количество необходимых подсетей, их IP-диапазоны, маски и шлюзы.
– Нарисуйте схему сети, включающую маршрутизатор, коммутаторы и клиентские устройства.
– Распределите IP-адреса в соответствии с подсетями.

Задание 2. Настройка маршрутизатора
– Сконфигурируйте интерфейсы маршрутизатора, присвоив им IP-адреса соответствующих подсетей.
– Пропишите статические маршруты между подсетями.
– Убедитесь в наличии связности (ping, traceroute) между хостами разных сегментов.

Задание 3. Внедрение динамической маршрутизации (OSPF или RIP)
– Активируйте выбранный протокол маршрутизации.
– Настройте участие интерфейсов в маршрутизируемых зонах.
– Проверьте автоматическое построение маршрутов и реакцию на отключение одного из сегментов.

Задание 4. Маршрутизация между VLAN (если используется)
– Настройте VLAN на коммутаторе.
– Настройте subinterface на маршрутизаторе с использованием trunk-порта.
– Обеспечьте обмен данными между клиентами в разных VLAN через маршрутизатор.

Задание 5. Защита маршрутизируемой сети (дополнительно)
– Ограничьте доступ к интерфейсам управления (telnet, SSH).
– Настройте фильтрацию IP-трафика (ACL) между подсетями.

Вопросы и задания

1. Что такое маршрутизируемая сеть и в чём её преимущества по сравнению с обычной ЛВС?
2. Объясните разницу между статической и динамической маршрутизацией.
3. Как влияет маска подсети на процесс маршрутизации?
4. Что такое таблица маршрутизации и какие данные она содержит?
5. Почему в современных ЛВС часто применяют маршрутизацию между VLAN?
6. Какие риски безопасности связаны с маршрутизацией и как их можно минимизировать?

Вывод:
В ходе лабораторной работы было выполнено проектирование маршрутизируемой ЛВС с несколькими подсетями, освоены принципы настройки маршрутизатора и реализации статической и динамической маршрутизации. Такие навыки являются важнейшими в

построении корпоративных и распределённых сетей, где требуется высокая управляемость, масштабируемость и изоляция трафика. Кроме того, студент получил представление о методах организации межсетевого взаимодействия, контроля маршрутов и обеспечения устойчивости маршрутизируемых структур.

ЛАБОРАТОРНАЯ РАБОТА №9
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Цель работы:
Изучить принципы криптографической защиты информации при передаче по открытым каналам, ознакомиться с протоколами защищённого взаимодействия, научиться настраивать средства шифрования и реализовывать защищённый обмен данными с использованием современных алгоритмов.

Теоретическая часть:
Современные информационные сети подвергаются различным видам атак, включая перехват и модификацию данных при передаче. Основной способ защиты от подобных угроз — использование криптографических методов, обеспечивающих конфиденциальность, целостность и подлинность информации.

Криптография — область, занимающаяся методами преобразования информации таким образом, чтобы сделать её недоступной для неавторизованных лиц. В контексте передачи данных основную роль играют симметричные и асимметричные алгоритмы шифрования, а также протоколы безопасного обмена ключами.

Симметричное шифрование (например, AES, DES) использует один ключ как для шифрования, так и для расшифровки данных. Оно отличается высокой скоростью, но требует безопасного способа передачи ключа.

Асимметричное шифрование (например, RSA, ECC) применяет пару ключей — публичный и приватный. Публичный ключ используется для шифрования, а приватный — для расшифровки. Такие схемы удобны для защиты каналов, где отсутствует возможность обмена секретами заранее.

Гибридные схемы используют преимущества обеих систем: асимметричное шифрование для обмена ключами, после чего данные шифруются симметрично. Примером такого подхода служит протокол TLS.

Протоколы защищённого взаимодействия
На практике для защиты каналов используются протоколы SSL/TLS (в веб-приложениях), IPSec (в VPN), SSH (для защищённого доступа), HTTPS (шифрование HTTP), а также протоколы защиты электронной почты (PGP, S/MIME).

Цифровые сертификаты и центры сертификации (CA) применяются для верификации подлинности ключей и установления доверенных соединений.

Практические задания

Задание 1. Теоретический анализ алгоритмов шифрования
Изучите основные алгоритмы симметричного и асимметричного шифрования (AES, RSA, ECC). Проанализируйте их особенности, преимущества, область применения и уязвимости. Подготовьте краткую сравнительную таблицу характеристик.

Задание 2. Настройка защищённого соединения с использованием TLS/SSL
– Сгенерируйте самоподписанный сертификат с использованием утилиты OpenSSL.
– Настройте защищённый веб-сервер (например, Apache или nginx) с использованием HTTPS.
– Проверьте работу защищённого канала через браузер и проанализируйте сертификат.

Задание 3. Использование SSH для защищённого доступа
– Настройте SSH-соединение между двумя виртуальными машинами.
– Сгенерируйте ключевую пару RSA и реализуйте доступ без пароля.
– Убедитесь в шифровании передаваемой информации и настройте ограничение доступа по ключам.

Задание 4. Исследование работы VPN на базе IPSec или OpenVPN
– Поднимите VPN-соединение с использованием OpenVPN.
– Настройте обмен ключами и зашифрованный туннель.
– Проверьте прохождение трафика через защищённый канал и проанализируйте его средствами анализа сетевого трафика (Wireshark).

Задание 5. Пример гибридного шифрования
– Напишите простое приложение, использующее RSA для обмена симметрическим ключом и AES для шифрования данных.
– Зашифруйте текстовое сообщение, передайте его по открытому каналу, затем расшифруйте с использованием приватного ключа.

Вопросы и задания

1. Чем отличается симметричное шифрование от асимметричного? Приведите примеры.
2. Что такое гибридная криптосистема? Какие её преимущества?
3. Какие протоколы используются для защиты веб-трафика?
4. Что такое TLS и какие основные этапы происходят при его установлении?
5. Как работает цифровой сертификат и зачем он нужен?
6. Какие особенности имеет VPN на базе IPSec?
7. Как осуществляется аутентификация в SSH-соединениях?

Вывод:
В рамках лабораторной работы были рассмотрены основные подходы к криптографической защите передаваемой информации, от симметричных и асимметричных алгоритмов до комплексных защищённых протоколов. Практическое применение этих технологий позволяет надёжно защитить сетевой трафик, предотвратить перехват конфиденциальных данных и обеспечить доверенные каналы взаимодействия.

Умение настраивать и применять такие механизмы является неотъемлемой частью компетенции специалиста в области информационной безопасности.

ЛАБОРАТОРНАЯ РАБОТА №10
СБОР ПРЕДВАРИТЕЛЬНОЙ ИНФОРМАЦИИ

Цель работы:
Ознакомиться с основными этапами и методами сбора предварительной информации при проектировании защищённых компьютерных сетей, освоить методы разведки в рамках тестирования на проникновение, а также научиться использовать специализированные инструменты для получения сведений о целевой системе без активного вмешательства.

Теоретическая часть:
Сбор предварительной информации (reconnaissance, или разведка) — один из ключевых этапов анализа защищённости информационной системы. Этот этап часто предшествует активным действиям и позволяет сформировать общее представление о целевой сети, её структуре, уязвимостях и потенциальных точках входа для атаки.

Сбор информации делится на два основных типа:
1. Пассивная разведка — получение сведений без прямого взаимодействия с целевой системой. Это может включать анализ открытых источников (OSINT), доменных записей, сетевых диаграмм, соцсетей, утечек данных, WHOIS, Shodan и других.
2. Активная разведка — взаимодействие с системой (например, через пинг, сканирование портов, определение версий сервисов), что может быть замечено средствами защиты и спровоцировать ответную реакцию.

Инструменты и методы пассивной разведки:
– WHOIS-запросы для получения регистрационных данных доменов и IP-адресов
– DNS-запросы (nslookup, dig)
– Поиск утечек данных через HaveIBeenPwned, BreachDirectory и др.
– Поиск информации через Google dorking
– Анализ сервисов Shodan и Censys
– Изучение метаданных файлов (например, PDF, DOCX)
– Анализ соцсетей, форумов, блогов

Инструменты и методы активной разведки:
– Сканеры портов: Nmap
– Определение версий сервисов и операционных систем
– Сканеры уязвимостей: Nikto, Nessus (в рамках белого тестирования)
– Анализ открытых портов, баннеров и служб

Практические задания

Задание 1. WHOIS и анализ доменов
– Используйте утилиты whois и nslookup для получения сведений о целевом домене (например, testdomain.com).
– Определите IP-адреса, используемые DNS-сервера, срок регистрации домена,

контактные данные администратора.
– Составьте краткий отчёт о доменной информации.

Задание 2. Использование Shodan для анализа инфраструктуры
– Зарегистрируйтесь на Shodan.io.
– Выполните поиск по IP-адресу, домену или по фильтрам (например, port:22, country:RU).
– Выявите используемые сервисы, их версии и потенциальные уязвимости.
– Зафиксируйте результаты анализа в отчёте.

Задание 3. Поиск уязвимых файлов и метаданных
– Скачайте несколько документов из открытых источников (например, PDF-файлы с сайта компании).
– Используйте утилиты `exiftool` или `strings` для анализа метаданных.
– Определите, можно ли извлечь из файлов имена пользователей, версии программного обеспечения, пути к файлам и т.д.

Задание 4. Выполнение Google Dorking
– Примените специальные поисковые запросы Google для поиска конфиденциальной информации (например, `filetype:xls site:example.com`).
– Найдите незащищённые директории, документы с паролями, конфигурационные файлы и прочие ценные сведения.

Задание 5. Подготовка отчёта
– Обобщите собранную информацию.
– Определите потенциальные векторы атак.
– Сформулируйте предварительные выводы о степени защищённости инфраструктуры.

Вопросы и задания

1. В чём заключается разница между пассивной и активной разведкой?
2. Какие данные можно получить с помощью WHOIS и зачем они нужны?
3. Какие риски могут возникать при публикации метаданных файлов в открытом доступе?
4. Что такое Google Dorking? Приведите 3 примера поисковых запросов.
5. Как можно использовать Shodan в процессе сбора предварительной информации?
6. Почему важно соблюдать законность при проведении разведки?
7. Какие методы защиты от разведки вы бы рекомендовали организациям?

Вывод:
Сбор предварительной информации — необходимый этап как для атакующих, так и для специалистов по защите. Он позволяет выявить потенциальные уязвимости без непосредственного вмешательства в систему. Практическое владение инструментами пассивной и активной разведки помогает лучше понимать, какие данные могут быть доступны извне, и своевременно предпринимать меры по их защите.

ЛАБОРАТОРНАЯ РАБОТА №11
ИДЕНТИФИКАЦИЯ УЗЛОВ И ПОРТОВ СЕТЕВЫХ СЛУЖБ

Цель работы:
Изучить методы и инструменты для выявления сетевых узлов и открытых портов, определить активные сетевые службы и их характеристики, освоить принципы сканирования и идентификации, а также научиться анализировать результаты для оценки безопасности сети.

Теоретическая часть:
Идентификация узлов и портов — важнейшая задача при анализе сетевой инфраструктуры, особенно в рамках оценки защищённости или тестирования на проникновение. Узлы сети — это устройства, участвующие в коммуникациях (компьютеры, серверы, маршрутизаторы и т.д.). Порты — виртуальные точки подключения к службам, которые слушают сетевые запросы.

Каждый сетевой сервис работает на определённом порте (например, HTTP обычно на 80, HTTPS на 443, SSH на 22), и сканирование портов помогает определить, какие службы запущены на узлах. Это позволяет выявить потенциальные уязвимости и настроить защитные меры.

Основные понятия:
– **Порт** — числовой идентификатор интерфейса транспортного уровня, используемый для взаимодействия приложений.
– **Открытый порт** — порт, который принимает входящие соединения, значит, на нём работает сервис.
– **Закрытый порт** — порт, который не принимает соединения.
– **Фильтрованный порт** — порт, доступ к которому ограничен брандмауэром или другим механизмом фильтрации.

Сканирование портов бывает нескольких типов:
– **TCP SYN scan** (half-open) — отправляет SYN-пакет и ждёт ответа; если приходит SYN-ACK, порт открыт.
– **TCP Connect scan** — устанавливает полное соединение, более заметен для системы.
– **UDP scan** — сложнее, так как UDP не гарантирует подтверждения, часто требует дополнительных методов.
– **Сканирование версий сервисов** — определение типа и версии программного обеспечения, работающего на порте.

Инструменты для идентификации узлов и портов:
– **Nmap** — один из самых популярных и мощных сканеров. Поддерживает множество режимов сканирования, позволяет определять версии сервисов и ОС.
– **Netcat** — утилита для проверки доступности портов и взаимодействия с ними.
– **Masscan** — высокоскоростной сканер портов, полезен для больших сетей.
– **Zenmap** — графический интерфейс для Nmap.

Помимо портов, важна идентификация самих узлов: это можно сделать с помощью анализа IP-адресов, MAC-адресов, трассировки маршрута (traceroute), и определения операционных систем (OS fingerprinting).

Идентификация узлов и портов играет ключевую роль в обеспечении безопасности, так как позволяет определить, какие сервисы доступны извне, какие версии программного обеспечения работают, и каким образом можно усилить защиту.

Практические задания

Задание 1. Сканирование сети на наличие активных узлов
– С помощью утилиты Nmap выполните сканирование локальной сети для определения активных устройств.
– Зафиксируйте список IP-адресов обнаруженных узлов.

Задание 2. Определение открытых портов и работающих сервисов
– Для каждого активного узла выполните сканирование портов с помощью Nmap. Используйте опцию `-sS` (TCP SYN scan) и `-sV` (определение версий).
– Составьте таблицу с перечислением узлов, открытых портов и обнаруженных сервисов.

Задание 3. Анализ закрытых и фильтрованных портов
– Используйте Nmap с опцией `-sA` (ACK scan) для определения фильтрованных портов.
– Определите, какие порты заблокированы и предположите возможные причины.

Задание 4. Использование Netcat для проверки портов
– На одном из узлов выполните команду Netcat для проверки доступности конкретного порта.
– Попробуйте подключиться к открытому порту, отправьте простой запрос (например, HTTP GET) и проанализируйте ответ.

Задание 5. Идентификация операционной системы
– Используйте Nmap с опцией `-O` для определения операционных систем на активных узлах.
– Сопоставьте полученные результаты с известной информацией об устройствах.

Вопросы и задания

1. В чём разница между открытым, закрытым и фильтрованным портом?
2. Какие методы сканирования портов существуют и чем они отличаются?
3. Какую информацию можно получить, определяя версии сервисов и операционные системы?
4. Какие риски связаны с наличием открытых портов на сервере?
5. Почему сканирование портов иногда может быть обнаружено средствами защиты?
6. Как можно защитить сеть от несанкционированного сканирования?
7. Опишите процедуру проверки доступности порта с помощью Netcat.

Вывод:
Идентификация узлов и портов является основой для понимания структуры сети и оценки её безопасности. Практическое использование инструментов сканирования позволяет выявить активные сервисы и потенциальные уязвимости. Правильный анализ и

интерпретация данных помогут своевременно выявить риски и принять меры для усиления защиты сетевой инфраструктуры.

ЛАБОРАТОРНАЯ РАБОТА №12
ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ СЕТЕВЫХ ПРИЛОЖЕНИЙ ПО КОСВЕННЫМ ПРИЗНАКАМ

Цель работы:
Освоить методы обнаружения уязвимостей сетевых приложений на основе анализа косвенных признаков, таких как поведение сервисов, нестандартные ответы, ошибки и особенности протоколов. Научиться использовать инструменты для сбора и интерпретации такой информации в целях оценки безопасности.

Теоретическая часть:
Идентификация уязвимостей сетевых приложений — важный этап обеспечения информационной безопасности. Помимо классического поиска уязвимых версий ПО и открытых портов, существуют косвенные признаки, которые позволяют выявить слабые места даже при отсутствии прямых данных.

Косвенные признаки могут включать:

- **Аномалии в поведении приложений:** например, нестандартные ответы на запросы, ошибки, задержки.
- **Особенности протоколов:** некоторые реализации протоколов могут иметь известные баги, и по поведению сервиса можно понять, какая версия используется.
- **Ошибки в заголовках HTTP или других протоколов:** они могут выдавать информацию о сервере, системе управления контентом (CMS), языках программирования и используемых библиотеках.
- **Формат и содержание ошибок:** раскрывают детали внутренней структуры и позволяют выявить потенциальные уязвимости, например, раскрытие путей к файлам, конфигурационных данных, сведений о базе данных.
- **Таймингговые атаки:** анализ времени отклика может выявлять утечки информации.

Основные методы и инструменты:

- **Сканеры уязвимостей (например, Nikto, OpenVAS, Nessus):** часто анализируют сервисы по косвенным признакам.
- **Инструменты для анализа HTTP-заголовков (например, curl, Burp Suite, OWASP ZAP):** позволяют выявить излишне информативные заголовки или ошибки.
- **Фингерпринтинг приложений:** выявление программных продуктов и их версий по косвенным признакам.
- **Анализ логов и сетевого трафика:** выявление подозрительных шаблонов.

Косвенная идентификация позволяет обнаруживать уязвимости, которые не видны при простом сканировании портов или проверке версий, что значительно расширяет возможности для оценки защищённости.

Практические задания

Задание 1. Анализ HTTP-заголовков

- С помощью утилиты curl или браузерных плагинов сделайте запрос к тестовому веб-серверу.
- Проанализируйте заголовки ответа, определите наличие избыточной информации, которая может помочь злоумышленнику.
- Определите, какие заголовки могут указывать на используемые технологии.

Задание 2. Идентификация приложений по ошибкам

- Вызовите на сервере разные ошибочные состояния (например, 404, 500).
- Проанализируйте содержимое страниц ошибок, найдите сведения, раскрывающие детали о сервере или приложении.

Задание 3. Фингерпринтинг веб-приложений

- Используя специализированные инструменты (например, Wappalyzer, WhatWeb), определите тип и версии веб-сервисов по косвенным признакам.
- Сопоставьте результаты с официальной документацией по уязвимостям.

Задание 4. Тайминговый анализ

- Проведите серию запросов к сетевому приложению с разными параметрами.
- Зафиксируйте время отклика и выявите аномалии, которые могут свидетельствовать о проблемах безопасности.

Задание 5. Использование сканеров уязвимостей

- Запустите сканирование тестового сервера с помощью Nikto или OpenVAS.
- Проанализируйте отчёт, обратите внимание на выявленные уязвимости, основанные на косвенных признаках.

Вопросы и задания

1. Что такое косвенные признаки уязвимостей сетевых приложений и почему они важны?
2. Как ошибки и заголовки HTTP могут раскрывать информацию о сервере?
3. В чём заключается методика таймингового анализа?
4. Какие инструменты используются для фингерпринтинга веб-приложений?
5. Почему идентификация уязвимостей по косвенным признакам может быть более эффективна, чем прямое сканирование?

6. Какие меры можно принять для минимизации утечек информации через косвенные признаки?

Вывод:
Идентификация уязвимостей по косвенным признакам расширяет возможности оценки безопасности сетевых приложений, позволяя выявлять потенциальные угрозы, скрытые от стандартных методов сканирования. Освоение этих методов повышает качество анализа и способствует своевременному выявлению и устранению уязвимостей, что критически важно для защиты информационных систем.

ЛАБОРАТОРНАЯ РАБОТА №13
ЗАЩИТА БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (ЛВС)

Цель работы:
Изучить основные угрозы безопасности беспроводных локальных вычислительных сетей и методы их защиты. Ознакомиться с механизмами аутентификации, шифрования и контроля доступа в беспроводных сетях. Научиться настраивать средства защиты в типичной беспроводной сети.

Теоретическая часть:
Беспроводные локальные вычислительные сети (Wi-Fi сети) обладают высокой степенью удобства, обеспечивая мобильность и гибкость доступа к ресурсам. Однако, открытая природа беспроводной среды делает такие сети уязвимыми для разнообразных угроз, среди которых подслушивание трафика, несанкционированный доступ, атаки «человек посередине» (MITM), и внедрение вредоносных устройств.

Основные угрозы безопасности беспроводных ЛВС включают:

- **Перехват данных:** беспроводной трафик легко перехватить, если он не зашифрован.
- **Неавторизованный доступ:** злоумышленники могут подключиться к сети, используя слабые пароли или уязвимости в протоколах.
- **Атаки отказа в обслуживании (DoS):** создание помех или перегрузка сети.
- **Фальсификация точки доступа:** злоумышленник создает ложную точку доступа для сбора данных пользователей.
- **Распространение вредоносного ПО:** через беспроводные каналы возможно распространение вирусов и троянов.

Для защиты беспроводных ЛВС применяются следующие методы:

- **Аутентификация пользователей и устройств:** применение WPA2/WPA3 с сильной паролизацией, использование сертификатов и EAP-методов.
- **Шифрование трафика:** защищённые протоколы (WPA2-AES, WPA3), использование VPN поверх Wi-Fi.
- **Контроль доступа:** фильтрация MAC-адресов, создание гостевых сетей с ограниченными правами.

- **Мониторинг сети:** обнаружение подозрительных активностей, анализ логов и использование систем обнаружения вторжений (IDS).
- **Настройка точки доступа:** ограничение мощности передатчика, скрытие SSID, регулярное обновление прошивок.

Кроме того, важной частью является регулярное обучение пользователей, поскольку многие атаки основываются на социальной инженерии и человеческом факторе.

Практические задания

Задание 1. Анализ безопасности беспроводной сети

- Выполните сканирование Wi-Fi сетей с помощью инструментов (например, Kismet, Wireshark).
- Определите используемые стандарты шифрования и уровень защиты.
- Зафиксируйте видимые SSID, MAC-адреса точек доступа и уровень сигнала.

Задание 2. Настройка защищённой точки доступа

- Настройте точку доступа с использованием WPA2/WPA3.
- Установите сложный пароль и активируйте фильтрацию по MAC-адресам.
- Спрячьте SSID и ограничьте максимальное количество подключений.

Задание 3. Проведение аутентификации пользователей

- Настройте метод EAP (например, PEAP или TLS) для аутентификации в беспроводной сети.
- Проверьте подключение клиентских устройств с использованием данного метода.

Задание 4. Анализ уязвимостей и атак

- Смоделируйте атаку типа «фальшивая точка доступа» и исследуйте, каким образом устройства реагируют.
- Определите, как можно предотвратить подобные атаки.

Задание 5. Мониторинг и аудит беспроводной сети

- Используйте средства мониторинга для отслеживания активности в сети.
- Проанализируйте логи и выявите подозрительные подключения или попытки доступа.

Вопросы и задания

1. Какие основные угрозы характерны для беспроводных локальных сетей?
2. Как работает шифрование WPA2 и в чём преимущества WPA3?
3. Какие методы аутентификации применяются в современных Wi-Fi сетях?

4. Какие меры помогают предотвратить несанкционированный доступ к беспроводной сети?
5. Почему важен мониторинг и аудит беспроводной сети?
6. Как социальная инженерия может использоваться для обхода технических мер безопасности?
7. Какие дополнительные меры можно рекомендовать для повышения безопасности в домашней беспроводной сети?

Вывод:
Безопасность беспроводных локальных сетей требует комплексного подхода, включающего технические меры защиты, постоянный мониторинг и осведомлённость пользователей. Правильная настройка аутентификации, шифрования и контроля доступа существенно снижает риски несанкционированного доступа и атак. Освоение данных методов является ключевым навыком для специалистов по безопасности сетей.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Безопасность сетей ЭВМ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем,
специализация Анализ безопасности информационных систем

Ставрополь
2025

ПРАКТИЧЕСКАЯ РАБОТА 1.

НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ CISCO

Цель: освоить базовые навыки настройки операционной системы Cisco, изучить основные команды и принципы конфигурации сетевых устройств.

Теоретическая часть
Операционная система Cisco IOS (Internetwork Operating System) является основой функционирования большинства маршрутизаторов и коммутаторов Cisco. Она предоставляет гибкую и мощную платформу для управления сетевыми устройствами, настройки маршрутизации, безопасности и коммутации.

В рамках данной практической работы рассматриваются базовые аспекты работы с Cisco IOS, включая доступ к устройству, режимы работы (пользовательский, привилегированный, режим конфигурации), базовые команды конфигурации интерфейсов, настройку протоколов маршрутизации и основных параметров безопасности.

Особое внимание уделяется структуре конфигурационных файлов, сохранению настроек и восстановлению конфигурации. Понимание принципов работы Cisco IOS необходимо для эффективного администрирования и защиты сетевой инфраструктуры.

Вопросы и задания

1. Что такое Cisco IOS и какие основные функции она выполняет?
2. Какие режимы работы существуют в Cisco IOS и чем они отличаются?
3. Как получить доступ к устройству Cisco?
4. Какие команды используются для базовой настройки интерфейсов?
5. Как сохранить и восстановить конфигурацию устройства?
6. Что такое файл конфигурации и какова его структура?
7. Каковы основные принципы безопасности при настройке Cisco IOS?

Практические задания

Задание 1. Подключитесь к маршрутизатору Cisco через консольный порт и выполните вход в привилегированный режим.
Задание 2. Выполните базовую настройку интерфейса Ethernet, задав IP-адрес и маску подсети.
Задание 3. Настройте и активируйте протокол маршрутизации RIP или OSPF.
Задание 4. Сохраните текущую конфигурацию в файл и проверьте её содержание.
Задание 5. Настройте базовую безопасность устройства, задав пароль на доступ в привилегированный режим.
Задание 6. Выполните перезагрузку устройства и восстановите сохранённую конфигурацию.
Задание 7. Составьте отчет с описанием выполненных действий, командами и результатами.

ПРАКТИЧЕСКАЯ РАБОТА 2.

ЗАЩИТА ИНФРАСТРУКТУРЫ МАРШРУТИЗАЦИИ

Цель: изучить основные методы и инструменты защиты инфраструктуры маршрутизации, научиться настраивать меры безопасности для предотвращения атак и несанкционированного доступа.

Теоретическая часть
Инфраструктура маршрутизации является критически важной частью сетевой архитектуры, обеспечивающей передачу данных между различными сетевыми сегментами. Защита маршрутизаторов и протоколов маршрутизации необходима для предотвращения различных угроз, включая подделку маршрутов, атаки типа «Man-in-the-Middle», DoS-атаки и внедрение вредоносных изменений в маршруты.

Для обеспечения безопасности маршрутизации применяются различные методы: аутентификация протоколов маршрутизации (например, с помощью MD5), фильтрация маршрутов, настройка списков контроля доступа (ACL), использование защищённых туннелей (VPN), мониторинг и логирование событий.

В рамках практической работы студенты научатся применять эти методы, анализировать уязвимости и внедрять защитные меры в конфигурации маршрутизаторов Cisco.

Вопросы и задания

1. Какие угрозы существуют для инфраструктуры маршрутизации?
2. Какие протоколы маршрутизации наиболее уязвимы и почему?
3. Что такое аутентификация протоколов маршрутизации и какие методы она включает?
4. Как работают списки контроля доступа (ACL) в контексте маршрутизации?
5. Какие способы защиты от DoS-атак применяются на маршрутизаторах?
6. Что такое фильтрация маршрутов и как она реализуется?
7. Как настроить мониторинг и логирование событий маршрутизатора для повышения безопасности?

Практические задания

Задание 1. Настройте аутентификацию MD5 для протокола OSPF на двух маршрутизаторах. Проверьте успешность обмена маршрутами.
Задание 2. Создайте и примените списки контроля доступа для ограничения входящего и исходящего трафика на интерфейсах маршрутизатора.
Задание 3. Настройте фильтрацию маршрутов, запретив получение нежелательных маршрутов из определённой сети.
Задание 4. Включите логирование событий безопасности маршрутизатора и настройте отправку уведомлений на syslog-сервер.
Задание 5. Смоделируйте попытку атаки типа DoS и примените базовые методы защиты.

Задание 6. Составьте отчет с описанием всех проведённых настроек, приведите примеры команд и результаты тестирования.

ПРАКТИЧЕСКАЯ РАБОТА 3. ЗАЩИТА ИНФРАСТРУКТУРЫ КОММУТАЦИИ

Цель: изучить основные методы обеспечения безопасности коммутационной инфраструктуры локальных сетей, освоить настройки защиты коммутаторов и предотвращения атак на канальном уровне.

Теоретическая часть
Коммутационная инфраструктура является фундаментом локальных сетей, обеспечивая передачу данных между конечными устройствами и распределение трафика внутри сети. Защита коммутаторов необходима для предотвращения множества угроз, включая атаки типа MAC-спуфинг, петли в сети, подделку адресов, а также для ограничения доступа к сетевым ресурсам.

Основные методы защиты включают в себя использование протоколов управления петлями (например, STP), фильтрацию MAC-адресов, настройку портовой безопасности (port security), использование VLAN для сегментации сети, а также внедрение систем обнаружения атак и мониторинга.

Особое внимание уделяется предотвращению петель на канальном уровне, которые могут привести к деградации сети и отказу в обслуживании. Методики защиты включают конфигурацию Rapid Spanning Tree Protocol (RSTP), настройку BPDU Guard и Root Guard.

В рамках практической работы студенты познакомятся с этими методами, научатся конфигурировать основные функции безопасности на коммутаторах Cisco, а также анализировать и устранять проблемы безопасности на канальном уровне.

Вопросы и задания

1. Какие угрозы характерны для коммутационной инфраструктуры в локальных сетях?
2. Что такое петля на канальном уровне и почему она опасна?
3. Как работает протокол Spanning Tree и его расширенные версии?
4. Какие методы портовой безопасности существуют и как они применяются?
5. В чем назначение VLAN с точки зрения безопасности?
6. Как реализуются механизмы BPDU Guard и Root Guard?
7. Какие меры можно принять для предотвращения MAC-спуфинга?
8. Как мониторить состояние сети и выявлять атаки на канальном уровне?

Практические задания

Задание 1. Настройте протокол Rapid Spanning Tree Protocol (RSTP) на коммутаторе и проверьте его работу в тестовой сети с петлей.
Задание 2. Включите и настройте портовую безопасность (port security) на выбранных портах, ограничив количество разрешённых MAC-адресов и определив действия при

нарушении политики.
Задание 3. Создайте VLAN для сегментации сети и настройте меж-VLAN маршрутизацию с применением правил доступа.
Задание 4. Включите BPDU Guard и Root Guard на портах доступа и транка для защиты от неправильной топологии.
Задание 5. Проведите мониторинг активности MAC-адресов и проанализируйте журналы безопасности.
Задание 6. Составьте подробный отчёт с описанием выполненных настроек, приведите примеры команд и результаты тестирования безопасности.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Безопасность сетей ЭВМ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем,
специализация Анализ безопасности информационных систем

Ставрополь
2025

ВВЕДЕНИЕ

Настоящие рекомендации предназначены для студентов всех форм обучения при выполнении курсовых работ, для руководителей курсовых работ с целью формирования единых требований при разработке и защите работ. Рекомендации содержат предложения по структуре курсовой работы (далее - работа), объему, содержанию, оформлению, процедуре допуска к защите и порядку защиты работ.

Целями выполнения курсовой работы являются:

- обогащение знаний студентов,
- обучение методам теоретического анализа явлений и закономерностей науки,
- выработка навыков применения теоретических знаний к комплексному решению профессиональных задач, использования справочной литературы, методов математической обработки экспериментальных данных, компьютерных технологий.

Системой курсовых работ (проектов) студент подготавливается к выполнению выпускной квалификационной работы.

Перед прочтением Методических указаний ознакомьтесь с основными ошибками, которые допускают студенты, приступая к написанию курсовой работы. Возможно, это мотивирует на более внимательное отношение к требованиям по написанию курсовой работы.

1. Выбрав тему, студент выходит в сеть Интернет и через поисковую систему (Yandex, Google и т.д. – зависит от предпочтений) находит курсовую работу по данной теме, меняет реквизиты, Ф.И.О. автора и сдаёт преподавателю. В результате получает рецензию: «Плагиат. На переработку».
2. Аналогичные действия п.1, но студент подходит к решению проблемы творчески и находит несколько курсовых работ по данной теме. Компонует материал по своему усмотрению и сдает преподавателю под своим авторством. В результате получает рецензию: «Плагиат. На переработку». Почему дана такая рецензия? По трем основным причинам: во-первых, написание курсовых работ – распространённый бизнес в Интернете и качественный материал бесплатно не выкладывают в сети, таким образом, компоновать приходится из «третьесортного сырья»; во-вторых, курсовая уже написана и защищена ранее, то есть она уже устарела и не отражает современных реалий, в-третьих, такие работы редко соответствуют требованиям, предъявляемым кафедрой к курсовым работам.
3. Студент принимает постороннюю помощь в написании работы. Здесь есть несколько аспектов, но следует обратить внимание на два основных. Во-первых, помощь исходит, как правило, от одного физического или юридического лица для группы студентов. В результате преподаватель получает на проверку несколько работ на разные темы, написанные «одной рукой». Формальных причин для отрицательной рецензии у преподавателя нет, особенно если работа выполнена в строгом соответствии с требованиями, но, как показывает практика, защита таких работ проходит безуспешно. Во-вторых, студент, не приложивший усилий к данной работе, как правило, очень плохо в ней ориентируется, особенно, когда преподаватель уточняет аспекты рассматриваемой темы. Но так как Вы уже вышли на защиту, то получаете заслуженную оценку «неудовлетворительно».
4. Вы самостоятельно осуществляете работу, но так же самостоятельно

выбираете требования к курсовой работе. Если Вам они нравятся и понятны, то исполняете, а если не нравятся, пропускаете. Это очень распространённая ошибка. Выполнять надо все без исключения требования к курсовой работе. Если в процессе работы возникли вопросы, следует по ним получить консультацию у научного руководителя.

Это краткий перечень основных ошибок, которые недопустимо совершать после прочтения данных Методических указаний.

1. ОРГАНИЗАЦИЯ ВЫПОЛНЕНИЯ И ЗАЩИТЫ КУРСОВОЙ РАБОТЫ

Виды работ по этапам выполнения курсовой работы:

а) Предварительный этап:

- выбор темы курсовой работы и оценка возможности раскрытия данной темы;
- подача заявления на закрепление темы;

б) Основной этап:

- сбор материала;
- оформление курсовой работы;

в) Заключительный этап:

- рецензирование работы руководителем и допуск к защите;
- защита работы.

1.1 Предварительный этап

Темы курсовых работ определяются выпускающей кафедрой. Студенту предоставлено право выбора темы курсовой работы. Задание к выбранной теме выдается руководителем работы (проекта) и регистрируется в кафедральном журнале.

1.2 Основной этап

Составление плана курсовой работы

План курсовой работы представляет собой составленный в определенном порядке перечень глав и развернутый перечень вопросов, которые должны быть освещены. Правильно составленный план работы помогает систематизировать материал, обеспечивает последовательность его изложения. План работы составляется самостоятельно, с учетом замысла и индивидуального подхода. План работы рекомендуется **согласовать с руководителем курсовой работы**. В процессе работы план работы может уточняться.

Подбор литературы

Курсовая работа выполняется на основе глубокого изучения литературных источников. Литература по теме работы может быть подобрана студентом при помощи предметных и алфавитных каталогов библиотек. Для этих целей могут быть использованы каталоги книг, указатели журнальных статей, специальные библиографические справочники, тематические сборники литературы, периодически выпускаемые отдельными издательствами, интернет-сайты официальных организаций.

Проработка источников сопровождается выписками, конспектированием. Выписки из текста делают обычно в виде цитаты. После каждой цитаты приводится ссылка на автора и источник. Поэтому при выписке цитат и конспектировании следует делать ссылки: автор, название издания, место издания, издательство, год издания, номер страницы. Конспект может содержать в себе факты, доказательства, примеры, основные положения и выводы автора, а также личное отношение студента к изученному материалу.

Рациональной и эффективной организации исследовательской деятельности способствует составление студентом собственной картотеки проработанных по теме и смежным вопросам литературных источников. Картотека не только помогает получить представление о степени изученности данной проблемы, но и позволяет работать с литературой более целеустремленно.

Оформление курсовой работы

Оформление проекта или работы осуществляется в соответствии с требованиями положения о выполнении и защите курсовых о выполнении и защите курсовых работ (проектов).

Содержание и структура курсовых работ

Курсовая работа должна содержать элементы новизны, наряду с фундаментальным аспектом должен быть проведен анализ современного состояния изучаемой проблемы, а также отражены региональные особенности. Задание по курсовой работе необходимо индивидуализировать с учетом интересов и способностей студентов.

Курсовая работа должна состоять из введения, теоретической части, эмпирической (практической, расчетно-графической) части, заключения, списка литературы и приложения. В отдельных случаях, в соответствии с тематикой работы, эмпирическая часть может отсутствовать.

Во введении обосновывается актуальность выбранной темы исследования, задачи, цели, новизна, теоретическая и практическая значимость исследования.

Теоретическая часть должна содержать анализ состояния изучаемой проблемы на основе обзора научной, научно-информационной, справочной литературы. Представленный материал должен быть логически связан с целью исследования. В параграфах теоретической части необходимо отражать отдельные компоненты проблемы и завершать их выводами.

Эмпирическая (практическая, расчетно-графическая) часть (при наличии) включает описание системы экспериментального исследования, обоснование методов исследования, анализ результатов экспериментального исследования, схемы, графические и математические способы интерпретации полученных данных, выводы.

Заключение содержит выводы, подтверждающие или опровергающие первоначальные предположения (гипотезы), перспективы дальнейшего изучения проблемы, связь с практикой, анализ реализации целей и задач исследования.

Список литературы должен быть составлен в соответствии с требованиями к оформлению библиографий.

Приложение содержит весь фактический материал экспериментальных исследований (анкеты, опросники, схемы, чертежи, расчетные материалы, карты, рисунки, ответы респондентов и т.д.).

Содержание курсовой работы (проекта) рекомендуется представлять в объеме 20-30 страниц печатного текста. Текст работы должен быть напечатан через 1,5 интервала на одной стороне стандартного листа белой бумаги (А - 4). Текст и другие отпечатанные элементы работы должны быть черными, контуры букв и знаков – четкими, без ореола и затенения. Шрифт TimesNewRoman, кегель 14. Курсив и подчеркивание в работе не допускаются. Названия глав и параграфов выделяются полужирным шрифтом. Лист с текстом должен иметь поля: слева – 30 мм, справа – 10 мм, сверху – 20 мм, снизу – 20 мм. Нумерация страниц текста делается в правом нижнем углу листа. Проставлять номер страницы необходимо со страницы, где печатается "Введение", на которой ставится цифра "3". После этого нумеруются все страницы, включая приложения.

Между названием главы и названием параграфа этой главы ставится пробел равный двум интервалам, а название параграфа не должно отделяться от текста этого параграфа пробелом. Названия параграфов отделяются от текста предыдущего параграфа пробелом, равным двум интервалам. Каждая глава, а также введение, выводы, предложения и список использованной литературы начинаются с новой страницы. Слово "Глава" не пишется. Главы имеют порядковые номера в пределах всей работы, обозначаемые арабскими цифрами (например: 1,2,3), после которых ставится точка. Слово "параграф" или значок параграфа в названии не ставятся. Параграфы имеют порядковые номера в пределах глав, обозначаемые арабскими цифрами (например: 1.1. и 1.2.). Заголовки глав и параграфов в тексте работы должны располагаться по центру, точку в конце названия главы и параграфа не ставят. Не допускается переносить часть слова в заголовке.

Нумерация таблиц и рисунков может быть сквозной или соотноситься с номером главы и параграфа. Например, если таблица или рисунок включены в текст первого параграфа второй главы, нумерация следующая: Таблица 2.1.1., рис. 2.1.1. Последняя цифра означает порядковый номер таблицы (или рисунка) в данном параграфе. Таблица помещается в качестве следующей страницы после первого упоминания о ней в тексте.

В рамках отведенного для руководства курсовыми работами времени регулярно проводятся индивидуальные консультации. Руководитель работы осуществляет предварительный просмотр выполненных заданий. После проверки выполнения студентом одного этапа работы, руководитель работы разрешает студенту перейти к следующему.

1.3 Заключительный этап

Работа сдается руководителю. Если работа удовлетворяет требованиям, предъявляемым к курсовым работам, она допускается к защите.

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на заседании кафедры, научно-методического семинара кафедры, научной проблемной группы при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ могут быть доложены на научных конференциях.

Защита состоит в коротком докладе студента по выполненной работе и в ответах на вопросы присутствующих на защите.

Результаты защиты курсовой работы, согласно действующему Положению о текущем контроле и промежуточной аттестации, оцениваются дифференцированной отметкой по пятибалльной системе.

Студент, не представивший в установленный срок работу, получивший неудовлетворительную оценку на защите или не явившийся на защиту по неуважительной причине, считается имеющим академическую задолженность.

Для ликвидации академической задолженности студент обязан в установленные сроки представить курсовую работу руководителю и защитить её перед комиссией.

Допуск к защите курсовой работы

Допуск к защите осуществляет научный руководитель курсовой работы.

Работа не допускается к защите, если она не носит самостоятельного характера, списана из литературных источников или у других авторов, если основные вопросы не раскрыты, изложены схематично, фрагментарно, в тексте содержатся ошибки, научный аппарат оформлен неправильно, текст написан небрежно.

Неудовлетворительно выполненная работа подлежит переработке в соответствии с замечаниями преподавателя, содержащимися в отзыве.

При получении допуска к защите студент вправе получить дополнительную

консультацию по предстоящей защите.

Курсовая работа, студенту не возвращается и хранится на кафедре в течение 2-х лет.

После получения допуска к защите, студент самостоятельно готовится к защите: составляет текст доклада, реагирует на замечания руководителя.

Подготовка к защите курсовой работы включает устранение ошибок и недостатков, изучение дополнительных источников, готовность объяснить любые приведенные в работе положения.

В ходе защиты курсовой работы задача студента - показать углубленное понимание вопросов конкретной темы, хорошее владение материалом по теме.

Защита работы производится в соответствии с планом приёма защит курсовых работ. С ним можно ознакомиться на стенде кафедры или непосредственно уточнить у научного руководителя время и место защиты.

По результатам защиты курсовой работы в зачётную ведомость (для защиты курсовой работы) выставляется оценка.

Критерии оценки курсовой работы:

- «**отлично**» выставляется студенту, показавшему глубокие знания, которые применяются при самостоятельном исследовании избранной темы, умение обобщать практический материал и делать на основе анализа выводы. Курсовая работа с оценкой «отлично» может быть рекомендована на конкурс студенческих работ, использована в качестве доклада на научно-студенческой конференции.
- «**хорошо**» выставляется студенту, показавшему в работе и при её защите полное знание материала, всесторонне осветившему вопросы темы, но не полной мере проявившему самостоятельность в исследовании.
- **«удовлетворительно»** выставляется студенту, раскрывшему в работе основные вопросы избранной темы, но не проявившему самостоятельности в анализе или допустившему отдельные неточности содержания работы.
- «**неудовлетворительно»** выставляется студенту, не раскрывшему основные положения избранной темы и допустившему грубые ошибки в содержании работы.

2. СОДЕРЖАНИЕ КУРСОВОЙ РАБОТЫ

2.1 Структурные элементы курсовой работы

Структурными элементами курсовой работы являются:

1) титульный лист,
2) оглавление,
5) введение;
6) основная часть;
7) заключение;
8) список использованных источников;
9) приложения.

Титульный лист является первой страницей курсовой работы.

Оглавление включает введение, наименование всех глав и параграфов, заключение, список использованных источников и приложения с указанием номеров страниц, с которых начинаются эти элементы работы. Следует обратить внимание, что через оглавление прослеживается структура всей работы. Желательно основную часть работы уместить в 2

главы, каждая из которых разбивается на 2-3 параграфа. Глава не может содержать один параграф. Наличие в главе более трех параграфов говорит о поверхностном представлении данных вопросов, так как к работе предъявляются жесткие требования по объему работы.

Введение. Во введении обосновывается **актуальность темы**, **формулируются цель** курсовой работы **и комплекс взаимосвязанных задач**, подлежащих решению в процессе работы, а также представляется **теоретическая и методологическая база.**

Актуальность темы отражает степень важности её раскрытия на данный момент, то есть, почему читателю будет интересно, важно или просто необходимо познакомиться с Вашей работой. Это 2-3 предложения, которые анонсируют Вашу работу. Важно во введении**,** раскрывая актуальность темы, не уйти в раскрытие заявленной проблемы. Не следует писать фразы типа: «Мне эта тема очень интересна, поэтому она актуальна». Здесь необходимо заинтересовать читателя предметно и содержательно, а не своим примером.

Цель работы – это результат, к которому Вы желаете прийти и путь к нему. Цель работы одна. Формулируем её с использованием неопределённой формы глагола: изучить, исследовать, проанализировать, рассмотреть и т.д. Цель вашей курсовой работы скрыта в названии работы.

Задачи работы отражают шаги, делая которые, Вы достигаете цели. Вы должны поставить 6 - 7 задач. Они фактически связаны с параграфами Вашей работы. Задачи формулируются аналогично цели с использованием неопределенной формы глагола: изучить, исследовать, проанализировать, рассмотреть, оценить, выявить и т.д.

Теоретическая и методологическая база подразумевает краткое описание использованных источников с указанием основных авторов. Это «поклон» в адрес людей, чьими трудами Вы воспользовались, а также возможность для специалиста с первого взгляда понять, о чем написана работа и какого подхода к данной проблеме придерживаетесь Вы.

Объем этой части работы 1 лист.

Так как введение – это та часть работы, которая подразумевает 100% самостоятельное изложение, важно не перейти на «ты» в общении с подразумеваемым читателем, то есть **всё изложение материала должно осуществляется в неопределенной форме глагола**. Нельзя употреблять местоимение «я».

Основная часть. Требования к содержанию основной части работы даны ранее.

Заключение. В заключении формулируются краткие выводы, полученные в ходе выполнения поставленных задач и цели. Вы кратко излагаете то, что написали в работе, но это самое главное, что вы хотите донести до читателя, самый «сок» Вашего труда. В заключение можно вынести числовые данные в целях иллюстрации вывода. Они должны отражать цель и задачи исследования, и не быть «вырванными» из работы числами.

Список использованных источников должен содержать сведения об источниках, использованных при выполнении работы.

Приложения. В приложении рекомендуется включать материалы, связанные с выполненной работой, которые по каким-либо признакам не могут быть включены в основную часть.

2.2 Содержание основной части курсовой работы

Теоретический раздел

Раздел должен иметь наименование, отражающее теоретические аспекты темы курсовой работы. В общем случае в этом разделе должны быть отражены:

1) характеристика предмета исследования в соответствии темой курсовой

работы, в частности, должен присутствовать анализ понятийной базы по заявленной теме.

2) анализ состояния вопроса, являющегося темой работы, при необходимости – методы анализа.

3) основные подходы к решению проблемы, являющейся темой курсовой работы.

Теоретический раздел должен давать ответы на вопросы, что представляет собой проблема, являющаяся темой курсовой работы.

Объем раздела – 10 - 12 с. В разделе должно быть **не менее двух и не более трех подразделов**.

Аналитический раздел

Наименование данного раздела должно быть связано с анализом состояния предмета исследования, являющегося темой курсовой работы.

Исследование проблемы должно быть целевым и глубоким.

В аналитическом разделе используются различные приемы анализа, указываются источники информации, приводятся аналитические таблицы и расчеты, графические способы отражения результатов анализа, делаются выводы.

В данном разделе обязательно использование не только статистического материала, но и результатов анализа, проведенного специалистами по данному вопросу, которые изложены в источниках периодической печати.

Объем аналитического раздела курсовой работы не должен превышать 10-12 страниц.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Перечень основной литературы:

1. Галатенко В.А. Основы информационной безопасности. – М.: Интернет-Университет Информационных Технологий, 2020.
2. Петраков А.В. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2021.
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: ДМК Пресс, 2019.
4. Лопатин В.Н. Информационная безопасность России. – СПб.: Юридический центр Пресс, 2018.
5. Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2020.

Перечень дополнительной литературы:

6. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
7. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".
8. Федеральный закон от 26.12.1995 № 208-ФЗ "О безопасности".
9. Приказы ФСТЭК России
10. ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения".
11. ГОСТ Р 57580.1-2017 "Безопасность финансовых организаций".