ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 8. ТЕМА 3.2. ОБЪЕДИНЕНИЕ КОМПЬЮТЕРОВ В ЛОКАЛЬНУЮ СЕТЬ. ОРГАНИЗАЦИЯ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

1. Понятие локальной вычислительной сети

Локальная вычислительная сеть (ЛВС, англ. Local Area Network, LAN) — это система взаимосвязанных компьютеров и периферийных устройств, размещённых на ограниченной территории (помещение, здание, группа зданий, предприятие) и объединённых каналами связи для совместного использования ресурсов: файлов, программ, принтеров, дисковых накопителей и доступа в глобальные сети.

ЛВС прошли значительный путь эволюции: первые коммерческие сетевые технологии (Ethernet в его оригинальном виде, ARCNET) появились в 1980-е годы, базировались на шинной топологии и методе случайного доступа к общей среде передачи. Современные ЛВС строятся преимущественно на технологии Gigabit Ethernet (стандарт IEEE 802.3ab, скорости 1 Гбит/с) и всё шире внедряется 10 Gigabit Ethernet (стандарт IEEE 802.3ae). Классическая шинная топология с коаксиальным кабелем (стандарт 10Base2, 10Base5) считается устаревшей и на практике не применяется; основной тип физической топологии в современных сетях — «звезда» на базе неэкранированной витой пары (стандарты TIA/EIA-568-B).

Ключевое свойство ЛВС, отличающее её от распределённых вычислительных систем глобального масштаба, — низкая стоимость передачи данных, высокие скорости обмена и относительно низкий уровень ошибок в каналах связи. Именно это делает целесообразным выделение в рамках организации единого сетевого периметра с общими сервисами.

2. Оборудование локальной сети и принципы её построения

2.1. Сетевое оборудование

Основными элементами аппаратной инфраструктуры ЛВС являются:

• **Сетевой адаптер (сетевая карта, Network Interface Card, NIC)** — устройство, обеспечивающее физическое и канальное взаимодействие компьютера со средой передачи. Различают встроенные адаптеры (интегрированные в материнскую плату) и внешние (PCIe-платы, USB-адаптеры), проводные (Ethernet) и беспроводные (Wi-Fi, IEEE 802.11).

• **Коммутатор (сетевой коммутатор, свитч)** — активное оборудование, осуществляющее коммутацию кадров Ethernet на канальном уровне модели OSI. В отличие от концентратора (хаба), работавшего по принципу широковещательной передачи на все порты, коммутатор передаёт кадр только на порт получателя, что существенно повышает пропускную способность и снижает коллизии. Коммутаторы классифицируются по уровню: неуправляемые (для малых сетей), управляемые второго уровня (L2), управляемые третьего уровня (L3).

• **Маршрутизатор (роутер)** — устройство сетевого (третьего) уровня, осуществляющее маршрутизацию пакетов между IP-подсетями и соединяющее ЛВС с внешними сетями (например, с сетью Интернет).

• **Точка беспроводного доступа (Wireless Access Point)** — оборудование организации беспроводного сегмента сети по стандартам IEEE 802.11 (актуальное поколение — Wi-Fi 6, стандарт 802.11ax).

• **Модем** — устройство преобразования цифровых сигналов компьютера в форму, пригодную для передачи по физической среде (телефонная линия, оптоволокно, коаксиальный кабель).

2.2. Среда передачи

Передающая среда современных ЛВС — преимущественно неэкранированная витая пара категории 5e и выше (стандарты 100Base-TX, 1000Base-T) либо одномодовое/многомодовое оптическое волокно для магистральных линий и соединения

между зданиями. Волоконно-оптические линии связи (ВОЛС) обладают существенно более высокой пропускной способностью и устойчивостью к электромагнитным помехам, однако их развёртывание дороже, а монтаж требует специализированного оборудования и квалифицированного персонала.

2.3. Топология и модели организации сети

Физическая топология «звезда» является доминирующей: все рабочие станции подключаются к центральному коммутатору. На логическом уровне для организации связи между рабочими станциями и серверами применяются клиент-серверная и одноранговая модели.

Одноранговая сеть (peer-to-peer) — все компьютеры равноправны, каждый может выступать и в роли клиента, и в роли сервера. Достоинства: простота и низкая стоимость развёртывания, отсутствие необходимости в выделенном сервере. Недостатки: ограниченная масштабируемость (как правило, до 10–15 узлов), сложность централизованного администрирования, распределённое хранение критичных данных, повышенные риски безопасности.

Клиент-серверная сеть — выделяются серверы, предоставляющие централизованные сервисы (файловый сервер, сервер баз данных, контроллер домена, сервер печати), и клиенты, запрашивающие эти сервисы. Сервер представляет собой высокопроизводительный компьютер, работающий в непрерывном режиме. Достоинства: централизованное администрирование, единая политика безопасности, масштабируемость, надёжное резервное копирование. Недостатки: высокая стоимость оборудования и постоянные расходы на администрирование.

3. Организация работы пользователей в локальных компьютерных сетях

3.1. Идентификация и аутентификация пользователей

Ключевым механизмом организации работы пользователей в сети является система централизованной аутентификации. Каждому пользователю присваивается уникальная учётная запись (логин), ассоциированная с паролем и набором прав доступа. Процесс доступа к сетевым ресурсам реализуется в три этапа:

1. **Идентификация** — пользователь сообщает системе свой уникальный идентификатор (логин).
2. **Аутентификация** — проверка подлинности идентификатора (ввод пароля, PIN-кода, подтверждение биометрическими данными, смарт-картой или другим аутентификатором).
3. **Авторизация** — предоставление пользователям прав на выполнение определённых действий над ресурсами сети в соответствии с назначенной ролью.

В среде Microsoft Windows механизмом централизованной аутентификации служит служба каталогов **Active Directory** (AD): все пользователи, компьютеры и группы учётных записей объединяются в домен, контролируемый сервером-контроллером домена. При входе в систему пользователь авторизуется на контроллере домена, и ему автоматически применяются назначенные групповые политики (Group Policy), определяющие права доступа, параметры рабочего стола, ограничения на запуск приложений и сетевые настройки.

В POSIX-совместимых системах (Linux, Unix) учётные записи хранятся в файлах /etc/passwd и /etc/shadow, а централизованная аутентификация в корпоративных сетях реализуется с использованием протокола **LDAP** (Lightweight Directory Access Protocol) — например, через серверы OpenLDAP, Samba DC (совместимые с AD) или через систему FreeIPA. Альтернативой локальным учётным записям является единый каталог LDAP, подключаемый как источник данных для всех рабочих станций и сервисов сети.

3.2. Общее дисковое пространство в локальной сети

Одним из центральных сервисов ЛВС является организация **общего сетевого диска** — централизованного хранилища файлов, доступного всем (или уполномоченным) пользователям сети.

В Windows-средах общий доступ реализуется с помощью протокола **SMB/CIFS** (Server Message Block / Common Internet File System): папка на сервере или рабочей станции «расшаривается», назначаются разрешения на уровне разделяемого ресурса и на уровне файловой системы NTFS (ACL — списки контроля доступа). На клиенте общий ресурс подключается как сетевой диск с присвоением буквы диска (например, Z:). Администратор имеет возможность гибко настраивать права: чтение, запись, изменение, полный доступ — отдельно для каждого пользователя или группы.

В Linux/Unix-средах аналогичные функции выполняют сервер **NFS** (Network File System) и демоны Samba (позволяющие предоставлять Linux-ресурсы для Windows-клиентов по протоколу SMB). Сетевое дисковое пространство может быть организовано на базе выделенного файлового сервера, сетевого хранилища **NAS** (Network Attached Storage) или кластерной файловой системы (Ceph, GlusterFS, OCFS2) для отказоустойчивости.

Перспективным направлением является облачная модель организации общего дискового пространства (Nextcloud, ownCloud, коммерческие сервисы облачного хранения), при которой доступ к данным реализуется через веб-интерфейс или протоколы WebDAV, а синхронизация файлов поддерживается и за пределами локального периметра. Существуют также системы виртуальных защищённых сетей (VPN), обеспечивающие безопасный доступ к общим ресурсам ЛВС для удалённых сотрудников.

3.3. Разграничение прав доступа в сети

Разграничение доступа — совокупность механизмов, определяющих, какие действия над информационными ресурсами разрешены каждому пользователю и процессу. В теории компьютерной безопасности выделяют основные модели:

- **Дискреционное разграничение доступа (DAC, Discretionary Access Control)** — владелец ресурса сам определяет права доступа к нему (списки ACL в файловых системах NTFS, ext4, права chmod в Unix). Модель гибкая, но не гарантирует защиты от непреднамеренного распространения привилегий.
- **Мандатное разграничение доступа (MAC, Mandatory Access Control)** — права доступа определяются centrally установленной политикой и уровнями конфиденциальности объектов и субъектов. Пример реализации — модель безопасности SELinux (Security-Enhanced Linux) в Linux и Windows Integrity Levels.
- **Ролевое разграничение доступа (RBAC, Role-Based Access Control)** — права назначаются не отдельным пользователям, а ролям, к которым приписываются пользователи. Данная модель считается оптимальной для крупных организаций, поскольку минимизирует административные издержки и упрощает аудит.

В практике администрирования ЛВС разграничение доступа реализуется на нескольких уровнях:

1. **На уровне учётных записей** — создание групп пользователей (администраторы, бухгалтерия, отдел кадров, «все пользователи») и назначение прав группам, а не отдельным пользователям. Это позволяет управлять доступом декларативно и избежать ошибок ручного назначения.
2. **На уровне ресурсов** — права доступа к файлам и папкам (чтение, запись, изменение, удаление, полный доступ) задаются ACL на файловых серверах и сетевых хранилищах.
3. **На уровне сервисов** — права администратора домена, оператора баз данных, оператора системы печати и т. д.

4. **На уровне сети** — сегментация сети с помощью виртуальных локальных сетей (VLAN), настроенных на коммутаторах, и межсетевое экранирование (firewall) с фильтрацией трафика между сегментами.

Важным принципом проектирования политики доступа является **принцип наименьших привилегий** (least privilege): каждому пользователю должны предоставляться только те права, которые необходимы для выполнения его служебных обязанностей. Также применяются механизмы аудита (журналирование действий пользователей, инспекция безопасности), периодический пересмотр прав доступа (например, ежеквартальная аттестация учётных записей) и немедленное блокирование учётных записей уволенных сотрудников.

3.4. Сетевые сервисы для совместной работы пользователей

Организация работы пользователей в ЛВС не ограничивается доступом к общему диску. Для эффективного совместного труда используются следующие сервисы:

• **Служба каталогов** (Active Directory, LDAP) — единая база учётных записей, групп, компьютеров и ресурсов, обеспечивающая сквозную аутентификацию.

• **DNS** (Domain Name System) — разрешение имён узлов (например, fileserver.company.local) в IP-адреса; в корпоративной среде используется внутренний DNS-сервер.

• **DHCP** (Dynamic Host Configuration Protocol) — автоматическое назначение IP-адресов и сетевых параметров рабочим станциям. Службы DHCP и DNS обычно совмещены на контроллере домена или выделенном сервере.

• **Служба печати** — централизованная организация доступа к принтерам (в Windows — Print Server, пул принтеров).

• **Серверы приложений** — терминальные серверы (RDS в Windows), системы виртуализации (VMware vSphere, Microsoft Hyper-V, KVM, Proxmox), контейнерные платформы (Docker, Kubernetes).

• **Корпоративные мессенджеры и средства совместной работы** — корпоративная почта (Exchange, Postfix/Dovecot), системы электронного документооборота, CRM/ERP-системы.

• **Система резервного копирования** — регулярное создание резервных копий критичных данных на выделенное хранилище (как правило, по расписанию), с политиками хранения и восстановления.

4. Администрирование локальной сети

4.1. Задачи системного администрирования

Администрирование ЛВС — это комплекс организационных, технических и программных мер, направленных на поддержание работоспособности, безопасности и эффективности сетевой инфраструктуры. К числу основных задач администрирования относятся:

1. **Планирование и проектирование сети.** Разработка топологии, выбор оборудования и операционных систем, планирование IP-адресации (подсети, диапазоны, резерв), документирование инфраструктуры.

2. **Развертывание и настройка.** Установка и настройка серверного оборудования и операционных систем серверов (Windows Server, Linux-дистрибутивы), настройка коммутаторов, маршрутизаторов, точек доступа.

3. **Управление учётными записями и правами доступа.** Создание, изменение и блокирование учётных записей, назначение прав, управление группами, применение групповых политик.

4. **Мониторинг.** Непрерывный контроль состояния серверов, коммутаторов, каналов связи, загрузки процессора, памяти, дискового пространства. Применяются

системы мониторинга Zabbix, Nagios, Prometheus, Grafana; протокол SNMP (Simple Network Management Protocol) используется для опроса состояния сетевого оборудования.

5. **Обеспечение безопасности.** Настройка межсетевых экранов, антивирусной защиты, системы обнаружения и предотвращения вторжений (IDS/IPS), своевременное обновление ПО (управление патчами), контроль за соблюдением политики безопасности.

6. **Резервное копирование и восстановление.** Организация регулярного резервного копирования (полное, инкрементальное, дифференциальное), проверка восстановления, хранение резервных копий отдельно от основных данных (правило 3-2-1: три копии, на двух разных типах носителей, одна — за пределами площадки).

7. **Управление конфигурацией.** Ведение актуальной документации по инфраструктуре, схемам подключения, паролям (в защищённом виде), версии ПО; автоматизация развёртывания (Ansible, Puppet, PowerShell DSC).

8. **Поддержка пользователей.** Служба технической поддержки (helpdesk), регистрация заявок, обучение пользователей правилам работы и информационной безопасности.

4.2. Инструменты администрирования

В среде Windows основным средством централизованного управления является **групповая политика (Group Policy)**, применяемая через объекты групповой политики (GPO) к пользователям и компьютерам домена; administration реализуется средствами утилит Active Directory Users and Computers (dsa.msc), Group Policy Management Console (GPMC), PowerShell-модулей для AD. Инструменты удалённого администрирования: Remote Desktop (RDP), Windows Admin Center, System Center Configuration Manager (SCCM), а также распределённые системы управления конфигурациями (Intune для гибридных сред).

В Linux-средах администрирование осуществляется через **SSH** (Secure Shell) — защищённый протокол удалённого управления, консольные утилиты, конфигурационные файлы в /etc, системы управления пакетами (apt, yum/dnf, zypper), автоматизацию Ansible. Для управления виртуализацией — libvirt, Proxmox VE, oVirt/RHV.

4.3. Журналирование и аудит

Важнейшей частью администрирования является централизованный сбор журналов (логов). В Unix-системах применяется подсистема **syslog** (демон syslogd, протокол syslog, RFC 5424) с централизованными коллекторами (rsyslog, syslog-ng), а также journald в systemd-дистрибутивах. В Windows используется журнал событий (Event Log), централизованно собираемый службой Windows Event Forwarding или через SIEM-системы. Анализ журналов позволяет выявлять попытки несанкционированного доступа, отслеживать изменение конфигураций, проводить расследование инцидентов и обеспечивать соответствие требованиям регуляторов.

4.4. Обеспечение безопасности сети

Современный ландшафт угроз требует комплексного подхода к безопасности ЛВС:

• **Сегментация сети.** Разделение сети на подсети/VLAN по функциональному признаку (пользователи, серверы, гостевой Wi-Fi, промышленный контур) с контролем трафика между сегментами на межсетевом экране. Практикуется выделение демилитаризованной зоны (DMZ) для общедоступных сервисов (веб-серверы, почтовые шлюзы).

• **Межсетевое экранирование.** Фильтрация трафика на границе сети и между сегментами по адресам, портам и протоколам; современные решения (NGFW) выполняют глубокий анализ пакетов (DPI) и инспекцию содержимого.

• **Защита от вредоносного ПО** — централизованные антивирусные системы (управление с единой консоли), механизмы ограничения приложений (AppLocker, Application Control), контроль запуска неподписанного кода.

• **Управление уязвимостями** — регулярное сканирование инфраструктуры (Nessus, OpenVAS/GVM, Qualys), своевременная установка обновлений безопасности.

• **Контроль сетевого доступа (NAC, Network Access Control)** — проверка соответствия устройства политикам безопасности перед допуском в сеть (стандарт IEEE 802.1X, аутентификация через RADIUS-сервер).

• **Шифрование.** Защита каналов связи (VPN для удалённых сотрудников и межсетевого шлюза, шифрование трафика Wi-Fi по стандарту WPA3), шифрование данных на дисках (BitLocker, LUKS, dm-crypt).

• **Обучение персонала** — регулярные инструктажи по информационной безопасности, модель осведомлённости о фишинге и социальной инженерии.

5. Организационные аспекты администрирования

5.1. Правовые основы

Администрирование сети и обработка данных пользователей регулируются законодательством. В Российской Федерации ключевым документом является **Федеральный закон № 152-ФЗ «О персональных данных»** от 27.07.2006, определяющий требования к обработке персональных данных, обязанности оператора и меры по обеспечению безопасности. Применительно к государственным информационным системам и объектам критической информационной инфраструктуры действуют требования ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и подзаконные акты, регламентирующие защиту информации.

5.2. Организационные меры

Помимо технических мер, администрирование включает организационные мероприятия:

• разработку и утверждение внутренних регламентов и политик информационной безопасности (политика паролей, политика использования ИТ-ресурсов, политика резервного копирования);

• определение ответственных за отдельные сегменты и сервисы;

• регулярные внутренние аудиты и тестирование восстановления из резервных копий;

• документирование аварийных сценариев и плана реагирования на инциденты (Incident Response Plan).

6. Тенденции развития сетевых технологий

Развитие локальных сетей определяется несколькими устойчивыми направлениями:

• **Повышение пропускной способности.** Массовый переход на 2.5G/5G/10G Ethernet на уровне доступа и 25G/40G/100G на магистралях; внедрение оптических технологий (SFP+, QSFP+).

• **Конвергенция проводных и беспроводных сетей.** Wi-Fi 6/6E и приближающийся Wi-Fi 7 (802.11be) обеспечивают скорости, сопоставимые с проводным Gigabit Ethernet, что меняет модель подключения пользователей.

• **Виртуализация и контейнеризация.** Сети всё чаще строятся поверх виртуализированных центров обработки данных (SDN — программно-определяемые сети), при этом администрирование выполняется в автоматизированном режиме.

• **Облачные сервисы и гибридная инфраструктура.** Организации совмещают локальные серверы (on-premises) с облачными сервисами (гибридная модель), что требует единого управления идентификацией и доступом.

• **Zero Trust и микросегментация.** Парадигма «нулевой доверенной сети» (Zero Trust) предполагает, что доверие не предоставляется по факту нахождения в локальном периметре: каждый запрос на доступ аутентифицируется и авторизуется независимо от источника [5].

• **Автоматизация.** Инструменты автоматизации (Ansible, Terraform, Nornir) снижают стоимость администрирования, минимизируют человеческий фактор и обеспечивают воспроизводимость конфигураций.

Локальная вычислительная сеть является фундаментальной инфраструктурой организации, обеспечивающей совместное использование информационных и аппаратных ресурсов. Организация работы пользователей строится на основе централизованной аутентификации и службы каталогов, а разграничение доступа реализуется многоуровневыми механизмами — от прав файловой системы до сегментации сети и политик безопасности. Администрирование ЛВС требует комплексного подхода: сочетания технических средств мониторинга, резервного копирования, защиты от угроз и организационных мер, включая регламенты и обучение персонала. Современные тенденции — автоматизация, виртуализация, Zero Trust-подход и гибридные облачные модели — формируют новую архитектуру корпоративных сетей, в которой границы локального периметра становятся динамическими, а безопасность — сквозной, непрерывной и контекстно-зависимой.