1. Потенциальные цели и назначение крупных сегментов сети

1.1. Enterprise Zone

Цель: обеспечение работы офисных приложений, доступа к корпоративным ресурсам и сервисов для сотрудников.

Назначение:

- поддержка клиентских ПК (Enterprise Client PCs);
- размещение критически важных корпоративных серверов (Enterprise Servers);
- обеспечение защищённого доступа к публично доступным сервисам (Publicly Facing Services) через DMZ;
- интеграция с WAN и Интернет через Edge Router.

1.2. Demilitarized Zone

Цель: создание буферной зоны между Интернетом и внутренней корпоративной сетью для защиты критически важных ресурсов.

Назначение:

- размещение публично доступных сервисов (веб-серверов, почтовых серверов);
- фильтрация и контроль трафика между Интернетом и Enterprise Core с помощью Enterprise DMZ Firewalls.

1.3. Industrial Demilitarized Zone

Цель: обеспечение безопасного обмена данными между корпоративной и промышленной зонами, минимизация рисков атак на промышленную инфраструктуру.

Назначение:

- буферизация трафика между Enterprise Zone и Industrial Zone;
- защита промышленных приложений и данных с помощью Industrial DMZ Firewalls;
- поддержка брокерских сервисов (Broker Services) для интеграции данных.

1.4. Industrial Zone

Цель: управление и контроль над промышленным оборудованием и процессами.

Назначение:

- управление производственными линиями (Line 1, Line 2);
- контроль над утилитами и безопасностью (Utilities, Safety IO);
- поддержка распределённых промышленных сетей (Industrial Distribution);
- обеспечение работы PLC (программируемых логических контроллеров) и IO (входов/выходов) для автоматизации процессов.

2. Риски ИБ для каждого из крупных сегментов сети

2.1.Enterprise Zone

- утечка конфиденциальных данных (фишинг, вредоносное ПО, атаки на почтовые серверы);
- DDoS-атаки на публично доступные сервисы в DMZ;
- несанкционированный доступ к корпоративным ресурсам через уязвимости в ПО или слабые пароли;
- атаки на маршрутизаторы и брандмауэры (например, через эксплойты);
- вредоносное ПО, распространяемое через корпоративные сети (вирусы, трояны, ransomware);
- классические МСЭ на границе WAN → Edge Router и в DMZ могут оперировать только IP-адресами и портами TCP/UDP, не анализируя содержимое пакетов. Это оставляет лазейки для продвинутых атак (например, эксплойтов на уровне приложений);
- МСЭ может не поддерживать фильтрацию специфических промышленных протоколов (Modbus, Profibus, ControlNet), используемых в Industrial Zone;
- нет механизмов проверки целостности трафика, направленного к PLC и IO устройствам — злоумышленник может имитировать легитимные команды.

2.2.Industrial Demilitarized Zone

- компрометация брокерских сервисов, приводящая к утечке данных или нарушению работы промышленных систем;
- атаки на межсетевые экраны (Industrial DMZ Firewalls) с целью проникновения в промышленную зону;

- недостаточная фильтрация трафика, позволяющая злоумышленникам получить доступ к критическим системам;
- MITM-атаки (Man-in-the-Middle) на обмен данными между зонами.

2.3.Industrial Zone

- атаки на PLC и контроллеры, приводящие к остановке или нарушению производственных процессов (например, Stuxnet);
- уязвимости в промышленных протоколах (Modbus, Profibus, ControlNet);
- физический доступ к устройствам (кража или повреждение оборудования);
- недостаточный мониторинг событий безопасности, затрудняющий обнаружение атак;
- угрозы от инсайдеров (несанкционированные изменения настроек оборудования).

3. Отсутствующие, компоненты ИС

Для повышения надёжности и безопасности системы рекомендуется добавить:

1 системы резервного копирования и восстановления данных для всех сегментов сети;

2 системы обнаружения и предотвращения вторжений (IDS/IPS) в каждой зоне (особенно в DMZ и IDMZ);

3 средства криптографической защиты (VPN, TLS/SSL) для шифрования трафика между сегментами;

4 системы управления конфигурацией (CMDB) для контроля изменений в инфраструктуре;

5 средства контроля доступа (AAA — Authentication, Authorization, Accounting) для всех устройств и сервисов;

6 системы мониторинга производительности (Zabbix, Prometheus) для раннего обнаружения аномалий;

7 антивирусное ПО и системы защиты от вредоносного ПО для всех рабочих станций и серверов;

8 системы управления патчами для своевременного обновления ПО.

4. Компоненты архитектуры ИБ (идентификация, управление, контроль, анализ, мониторинг, автоматизация)

4.1. Идентификация

Внедрить систему управления идентификацией и доступом (IAM — Identity and Access Management) между Enterprise Client PCs и Enterprise Core, а также между Broker Services (IDMZ) и Industrial Core.

Добавить серверы аутентификации (например, Active Directory, LDAP) в Enterprise Zone и Industrial Demilitarized Zone (IDMZ).

Внедрить многофакторную аутентификацию (MFA) для административного доступа к Enterprise Servers и Industrial PLCs.

4.2. Управление

Централизовать управление политиками безопасности через SIEM-систему (Security Information and Event Management), подключённую к:

- Enterprise DMZ Firewalls;
- Industrial DMZ Firewalls;
- Industrial Distribution (для контроля доступа к PLC).

Добавить консоль управления конфигурациями (например, Ansible, Puppet) для синхронизации настроек безопасности на всех узлах (серверах, маршрутизаторах, брандмауэрах).

Включить управление жизненным циклом ключей и сертификатов для защищённого обмена данными между зонами (например, через HSM — Hardware Security Module).

4.3. Контроль

Внедрить межсетевые экраны нового поколения (NGFW) на границах:

- WAN → Edge Router;
- Enterprise DMZ → Enterprise Core;
- IDMZ → Industrial Core.

Добавить системы контроля доступа на уровне приложений (например, WAF — Web Application Firewall) для Publicly Facing Services.

Внедрить политики Zero Trust для всех соединений между Enterprise Zone и Industrial Zone.

Использовать списки контроля доступа (ACL) на всех коммутаторах и маршрутизаторах.

4.4. Анализ

Интегрировать SIEM-систему для анализа логов с:

- серверов (Enterprise Servers, Broker Services);
- брандмауэров (Enterprise DMZ Firewalls, Industrial DMZ Firewalls);
- промышленных контроллеров (PLC, IO).

Добавить систему анализа угроз (Threat Intelligence), подключённую к внешним базам данных (например, VirusTotal, MITRE ATT&CK).

Внедрить анализаторы трафика (IDS/IPS — Intrusion Detection/Prevention System) на границах зон:

- между Internet → Edge Router;
- между IDMZ → Industrial Core.

4.5. Мониторинг

Развертывание системы мониторинга в реальном времени (NMS — Network Management System) с визуализацией состояния:

- сетевых устройств (маршрутизаторы, коммутаторы);
- серверов и рабочих станций;
- промышленных устройств (PLC, IO).

Добавить датчики аномального поведения (например, для обнаружения DDoS-атак на Publicly Facing Services).

Внедрить автоматические уведомления о критических событиях (например, через Slack, SMS, email) для администраторов ИБ.

Использовать системы логирования (Log Management) с ротацией и шифрованием журналов.

4.6. Автоматизация

Внедрить SOAR-систему (Security Orchestration, Automation and Response) для:

- автоматического реагирования на инциденты (изоляция заражённых узлов, блокировка IP-адресов);
- автоматизации патчей и обновлений ПО на всех узлах;
- синхронизации политик безопасности между зонами.

Использовать скрипты для автоматического развёртывания защитных мер (например, блокировка портов при обнаружении атаки).

Использовать оркестратор (например, Kubernetes для контейнеризированных сервисов) в Enterprise Servers для автоматизированного развертывания обновлений.

Интегрировать API SIEM и NMS для обмена данными и автоматизации процессов (например, автоматическое отключение доступа при компрометации учётной записи).