positive technologies

Харденинг сетевой инфраструктуры

Москва, 2024

Дата редакции документа: 27.01.2025

Содержание

1. Введение

Документ предназначен для сетевых инженеров и сетевых администраторов, отвечающих за проектирование, внедрение и эксплуатацию сетей передачи данных. Документ описывает комплексный подход к харденингу ЛВС, который поможет минимизировать риски и повысить уровень безопасности сети. Документ содержит рекомендации по выбору оптимальных практик и конфигураций сетевого оборудования.

Харденинг — это процесс повышения безопасности системы за счет изменения ее конфигурации с целью уменьшения количества доступных атакующему точек проникновения, повышения сложности проникновения и увеличения заметности действий атакующего.

Документ состоит из следующих разделов:

- общие рекомендации. Базовые рекомендации по безопасности ЛВС.
- сегментация сети. Рекомендации по разделению сети на логически изолированные зоны, которые позволят ограничить распространение вредоносных программ, защитить критически важные сервисы и усложнить для атакующего продвижение к цели атаки.
- защита оборудования. Инструкции по настройке сетевого оборудования для обеспечения максимального использования встроенных механизмов безопасности оборудования и применяемых технологий.
- чек-лист для проверки ЛВС. Список вопросов, которые помогут проверить уровень защищенности сети и выявить потенциальные уязвимости.

Использование рекомендаций, представленных в этом документе, позволит:

- повысить защищенность ЛВС от внешних и внутренних угроз;
- снизить риски несанкционированного доступа;
- обеспечить устойчивую работу сети в случае возникновения инцидентов информационной безопасности;
- упростить расследование инцидентов информационной безопасности и сократить время расследования.

2. Перечень сокращений

Таблица 1. Список сокращений документа

Сокращение	Расшифровка
БД	База данных
БЛВС	Беспроводная локальная вычислительная сеть
ИБ	Информационная безопасность
ЛВС	Локальная вычислительная сеть
МСЭ	Межсетевой экран
СКЗИ	Средство криптографической защиты информации
ЦОД	Центр обработки данных
AAA	Authentication, authorization, accounting
ACL	Access control list
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BPDU	Bridge protocol data unit
BUM	Broadcast, unknown-unicast and multicast
CA	Certificate authority
CDP	Cisco Discovery Protocol
CoPP	Control Plane Policing
CRL	Certificate revocation list
DACL	Downloadable access list
DH	Diffie–Hellman
DHCP	Dynamic Host Configuration Protocol

Сокращение	Расшифровка
DMZ	Demilitarized zone
DoS	Denial of service
EAP-TLS	Extensible Authentication Protocol–Transport Layer Security
ESP	Encapsulating Security Payload
FHRP	First Hop Redundancy Protocols
FTP	File Transfer Protocol
FVRF	Front-door virtual routing and forwarding
FW	Firewall
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
iACL	Infrastructure access control list
IDS	Intrusion detection system
IGP	Interior Gateway Protocol
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPS	Intrusion prevention system
ISP	Internet service provider
LEAP	Lightweight Extensible Authentication Protocol
LLDP	Link Layer Discovery Protocol
MAB	Mac Authentication Bypass
MAC	Media access control
MFA	Multi-factor authentication

Сокращение	Расшифровка
MITM	Man-in-the-middle
MOP	Maintenance Operation Protocol
NGFW	Next-generation firewall
NTA	Network traffic analyzer
NTP	Network Time Protocol
OOB	Out-of-band management
PFS	Perfect forward secrecy
PSK	Pre-shared key
RA VPN	Remote access virtual private network
RADIUS	Remote Authentication Dial-In User Service
SCP	Secure copy
SHA	Secure Hash Algorithm
SIEM	Security information and event management
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
tACL	Transit access control list
TACACS	Terminal Access Controller Access-Control System
TAP	Test access point
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

Сокращение	Расшифровка
TTL	Time to live
UDP	User Datagram Protocol
URL	Uniform resource locator
uRPF	Unicast reverse path forwarding
VLAN	Virtual local area network
VPN	Virtual private network
VRF	Virtual routing and forwarding
VTP	VLAN Trunking Protocol
WAF	Web application firewall
WAN	Wide area network
WEP	Wired Equivalent Privacy
WIPS	Wireless intrusion prevention system
WPA	Wi-Fi protected access

3. Общие рекомендации

В разделе представлены базовые принципы и даны основные рекомендации. В нем рассматриваются ключевые аспекты информационной безопасности и описываются эффективные практики, которые помогут повысить уровень защищенности вашей сети.

В этом разделе

3.1. Основные принципы

Основные принципы харденинга сетевой инфраструктуры:

- телекоммуникационное оборудование должно размещаться таким образом, чтобы максимально затруднить физический доступ к нему неавторизованных лиц.
- для телекоммуникационного оборудования, в отношении которого возможен контроль физического доступа (например, серверные стойки, шкафы или устройства в охраняемых помещениях), необходимо вести журнал регистрации посещений и действий с указанием времени, личности и цели доступа.
- для ограничения доступа к информационным ресурсам компании должны применяться принципы «по умолчанию запрещено» и «принцип наименьших привилегий».
- на сетевом оборудовании необходимо использовать ПО актуальных версий, рекомендованное производителем оборудования, что позволит закрыть известные уязвимости ПО.
- все учетные записи, предустановленные производителем оборудования, должны быть удалены на оборудовании.
- для повышения уровня защиты от несанкционированного доступа к системам управления ЛВС и оборудованием ЛВС рекомендуется использовать многофакторную аутентификацию.
- доступ к управлению оборудованием через любой из интерфейсов (console, aux и т.д.) должен использовать аутентификацию.

- Необходимо осуществлять регулярное резервное копирование конфигурационных файлов сетевых устройств. Копирование должно осуществляться с использованием протоколов, использующих шифрование данных при передаче. Учитывая вероятность компрометации систем хранения данных, также рекомендуется хранить резервные копии на офлайн-носителях в зашифрованном виде.

- Необходимо использовать только оборудование корпоративного уровня, поддерживаемое производителем.

- Необходимо проводить периодические регламентные работы с целью проверки консистентности конфигурационных файлов.

- Отключать неиспользуемую версию проктокола IP (IPv4/IPv6).

3.2. Архитектурные рекомендации

- Доступ пользователей к интернету должен осуществляться через веб-прокси или PT NGFW с использованием следующих функций: URL-фильтрация, репутационные фильтры, потоковый антивирус, контроль приложений, анализ файлов в песочнице.

- Доступность оборудования ЛВС и систем управления из интернета должна быть полностью исключена либо строго ограничена.

- Прямое подключение оборудования ЛВС к интернету должно быть исключено (за исключением пограничных устройств — маршрутизаторов, МСЭ).

3.3. Настройка оборудования

- Все неиспользуемые сетевые службы, протоколы или устаревшие сервисы (например, MOP на Cisco) должны быть отключены.

- Пароли и ключи в конфигурационных файлах должны храниться только в зашифрованном виде, шифрование должно осуществляться с использованием надежных алгоритмов шифрования.

- На оборудовании должно быть настроено журналирование событий не ниже уровня INFO с обязательной отправкой журналов в SIEM-систему. Дополнительно должно быть настроено журналирование ключевых событий, в том числе:

    - вход и выход пользователей;
    - выполнение конфигурационных команд;
    - события, связанные с VPN;
    - создание и удаление NAT-трансляций.

- На оборудовании необходимо настроить локальную парольную политику (если поддерживается производителем оборудования):

  - длина пароля — не менее 15 символов;
  - пароль должен содержать строчные и заглавные буквы, спецсимволы и цифры;
  - пароль не должен содержать обычных слов, как русских, так и английских, или он должен удовлетворять парольной политике компании;
  - должно быть установлено время жизни пароля — не более 90 дней;
  - перерыв между неуспешными попытками подключения — не менее 1 секунды;
  - учетная запись должна блокироваться на 5 минут после трех неуспешных попыток авторизации.

4. Сегментация сети

В современной сетевой инфраструктуре необходимо разделять сеть на логически изолированные сегменты или модули по функциональным признакам. Такой подход не только облегчит построение и масштабирование сети, но и позволит повысить безопасность сети, ограничить распространение вредоносных программ и обеспечить стабильную работу критически важных сервисов. Ниже описаны типичные модули сети:

- ЦОД (центр обработки данных) — централизованный комплекс, где размещается серверное оборудование, системы хранения данных и другие критически важные элементы инфраструктуры. Предназначен для обеспечения работы и доступности сервисов, хранения данных, обработки информации, выполнения сложных вычислений. Характеризуется высокой плотностью оборудования и сетевых подключений, необходимостью обеспечивать высокую доступность сервисов и отказоустойчивостью систем.

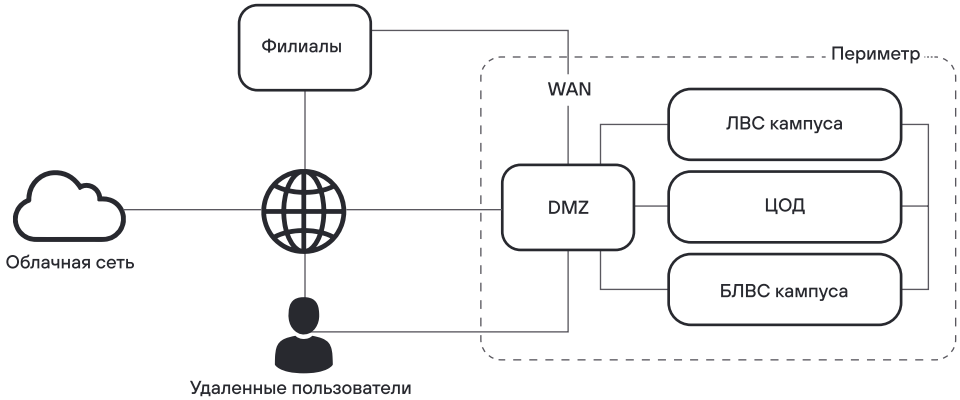
- Периметр сети — представляет собой совокупность оборудования и систем, отделяющих внутреннюю сеть от внешнего мира (интернета). Служит для обеспечения взаимодействия с внешним миром. Безопасность взаимодействия обеспечивается средствами предотвращения несанкционированного доступа к ресурсам внутренней сети, фильтрации трафика и контроля доступа. Основные элементы периметра — межсетевые экраны, системы обнаружения и предотвращения вторжений, прокси-серверы, песочницы, VPN-серверы и т. д.

- WAN — сеть, которая охватывает географически распределенные объекты (офисы, филиалы, центры обработки данных). Обеспечивает связь между удаленными объектами, передачу данных между различными подразделениями, доступ к интернет-ресурсам.

- ЛВС кампуса или офиса объединяет компьютеры, принтеры, серверы и другие устройства в пределах одного здания или территории. Обеспечивает обмен данными между пользователями, доступ к локальным сервисам и ресурсам, подключение к глобальной сети.

- Беспроводная ЛВС кампуса или офиса обеспечивает доступ к ресурсам ЛВС при помощи беспроводных точек доступа и мобильность пользователей внутри офиса.

Рисунок 1.
Сетевая инфраструктура



В каждом модуле применяется свой набор мер защиты информации.

Для повышения сетевой безопасности принято выделять сети с различным уровнем защиты:

- **Сеть с повышенной безопасностью.** Сегмент внутренней сети, требующий более высокой степени защиты. Доступ к такой сети осуществляется только изнутри (внутренняя сеть) и ограничивается за счет ис пользования МСЭ, VPN. Такой сегмент сети не общедоступен, доступ к нему есть только у ограниченного количества сотрудников. Доступ согласовывается со службой ИБ. Пример: серверы «1С», бюджет.

- **Доверенная (общедоступная) сеть.** Такой сегмент охватывает большую часть внутренней сети. Сеть доступна для всех авторизованных пользователей. Пример: домашний портал, справочный портал.

- **Сеть DMZ.** Сеть, предназначенная для размещения сервисов, доступных для внешних сетей, в частности для интернета. Взаимодействие с внешними и внутренними (доверенными) сетями ограничено с использованием МСЭ и устройств IDS/IPS. Пример: веб-серверы, почта.

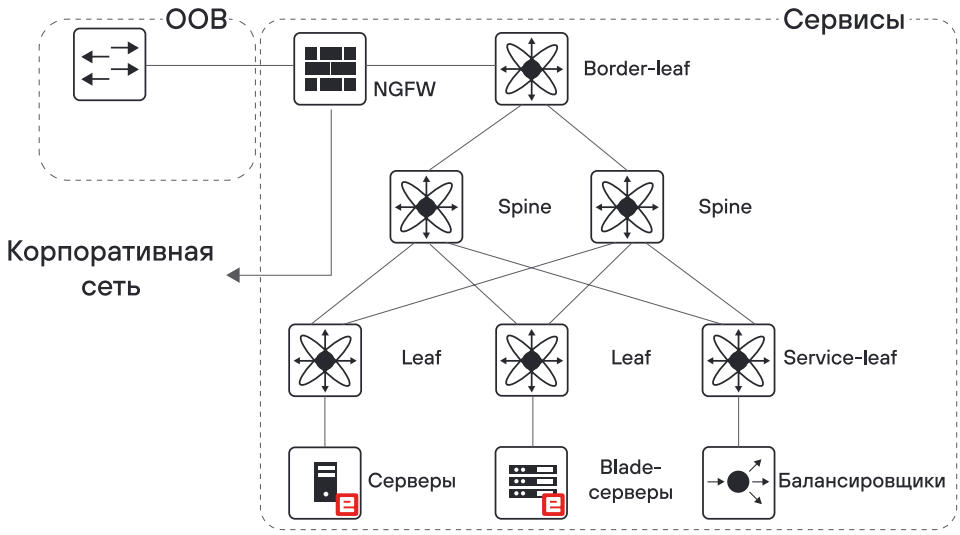
- **Гостевая сеть.** Сеть для использования посетителями при выходе в интернет. Из гостевой сети не должно быть доступа во внутреннюю доверенную сеть. Обязательный сбор метаданных. Пример: гостевой Wi-Fi.

В этом разделе

- Сегмент ЦОД (см. раздел 4.1)
- Периметр сети (см. раздел 4.2)
- Сегмент WAN (см. раздел 4.3)
- ЛВС кампуса или офиса (см. раздел 4.4)
- Беспроводная ЛВС кампуса или офиса (см. раздел 4.5)

4.1. Сегмент ЦОД

Рисунок 2. Сегмент ЦОД



Центры обработки данных характеризуются передачей больших объемов трафика на высоких скоростях. Трафик в ЦОД можно разделить на два типа:

- Горизонтальный («запад — восток») — обмен данными происходит между серверами и размещенными на них сервисами в пределах одного ЦОД.
- Вертикальный («север — юг») — обмен данными происходит между внешними пользователями/сервисами и сервисами, расположенными в ЦОД.

Рекомендуемой практикой является сегментирование сети ЦОД по сервисам. Каждый сервис изолируется в отдельном виртуальном маршрутизируемом сегменте (VRF). Трафик между VRF контролируется межсетевым экраном по принципу наименьших привилегий: разрешен только явно определенный трафик.

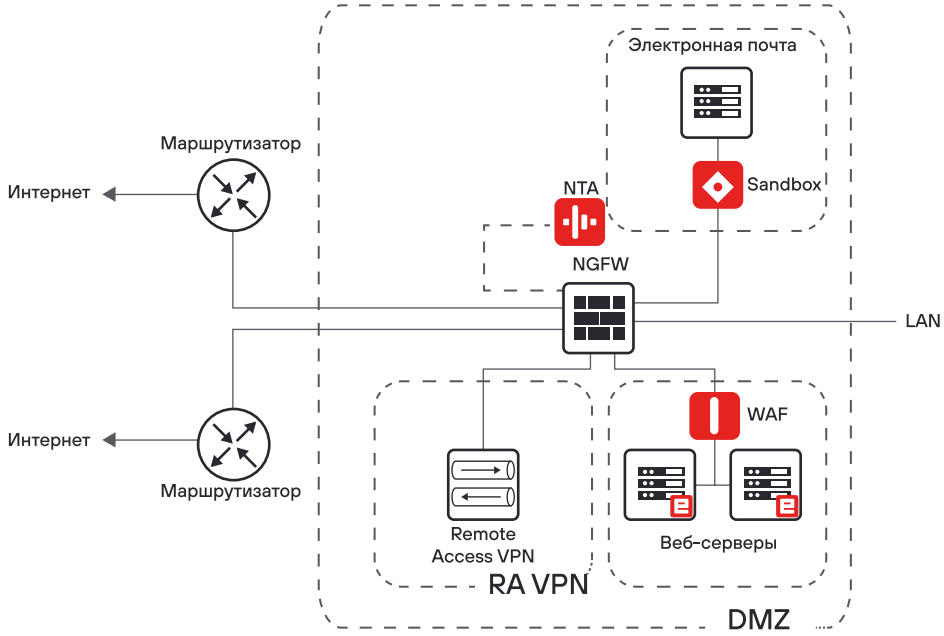
В виртуальной среде трафик приложений может оставаться в пределах физического сервера, становясь невидимым для сетевого оборудования. Для контроля такого трафика рекомендуется использовать межсетевые экраны на конечных точках либо использовать встроенные средства фильтрации среды виртуализации (при технической возможности).

Для управления оборудованием, расположенным в ЦОД, необходимо иметь выделенную сеть управления оборудованием (OOB). Доступ к этой сети должен быть разрешен только для администраторов: как минимум ограничен IP-адресами рабочих станций администраторов либо их учетными записями (если средство фильтрации умеет работать с identity), как максимум доступ должен предоставляться при помощи PAM-серверов, использующих двухфакторную аутентификацию, а также журналирование действий администраторов и запись экрана.

4.2. Периметр сети

Этот модуль включает в себя несколько зон безопасности, таких как VPN, RA VPN, доступ пользователей в интернет, публикация сервисов.

Рисунок 3. Периметр сети



RA VPN

Рекомендуется использовать выделенное оборудование под задачи RA VPN.

Необходимо использовать аутентификацию на основе сертификатов для максимальной защиты. При невозможности использования сертификатов необходимо применять многофакторную аутентификацию (MFA). При использовании MFA необходимо обеспечить должный уровень информирования пользователей по работе с этим приложением во избежание случаев выдачи необоснованных разрешений на подключение. Пользователи должны подтверждать только собственные подключения и уметь правильно их идентифицировать.

Необходимо использовать протокол TLS версии не ниже 1.3 с наборами шифров. В зависимости от сетевой инфраструктуры рекомендуется проверять корпоративные подключаемые устройства на предмет актуальности БД антивируса, наличие подключенных сторонних устройств, флеш-накопителей.

Каждая туннельная группа должна иметь ограниченный доступ к сети. Необходимо использовать полное туннелирование трафика (full tunneling). Права и доступы должны ограничиваться согласно уровню привилегий пользователя. Должны быть установлены таймауты бездействия пользователя.

Доступ к VPN-серверам должен быть ограничен необходимыми для работы портами (например, TCP/443). Сервисы управления на внешних интерфейсах должны быть выключены.

Site-to-Site VPN

Рекомендуется использовать выделенное оборудование под задачи Site-to-Site VPN.

Необходимо использовать наиболее стойкие алгоритмы шифрования. Для авторизации рекомендуется использовать сертификаты, подписанные корпоративным центром сертификации. Если необходимо авторизовываться по ключам, следует выбирать наиболее стойкие алгоритмы обмена ключами, доступные на используемом оборудовании. Только эти алгоритмы должны быть включены в список на VPN-концентраторе. В стеке протоколов IPsec должны использоваться только IKEv2 и PFS либо алгоритмы шифрования ГОСТ.

Доступ к VPN-серверам должен быть ограничен необходимыми для работы портами (например, 500/UDP, 4500/UDP и ESP). Сервисы управления на внешних интерфейсах должны быть выключены.

Публикация внешних сервисов

При публикации ресурсов должен предоставляться только минимально необходимый доступ.

Для защиты веб-порталов необходимо использовать WAF. WAF (web application firewall) — это система, которая фильтрует HTTP/HTTPS-трафик, защищая веб-приложения от атак. WAF должен дополнительно интегрироваться с другими системами безопасности, такими как SIEM и IDS/IPS, для улучшения защиты.

Доступ публикуемых ресурсов к внутренней сети должен быть максимально ограничен. Если доступ необходим, правило должно описывать взаимодействие на уровне определенных узлов и приложений или протоколов.

Общие рекомендации

Необходимо использовать инфраструктурные листы доступа, ограничивающие трафик, направленный непосредственно на сетевое устройство, по принципу наименьших привилегий. Например, чтобы запретить обращение к маршрутизаторам из интернета, за исключением необходимых взаимодействий (BGP-пиринг, Site-to-Site VPN, RA VPN и т. д.).

Весь периметральный трафик должен дублироваться на IDS/NTA-системы для дальнейшего анализа.

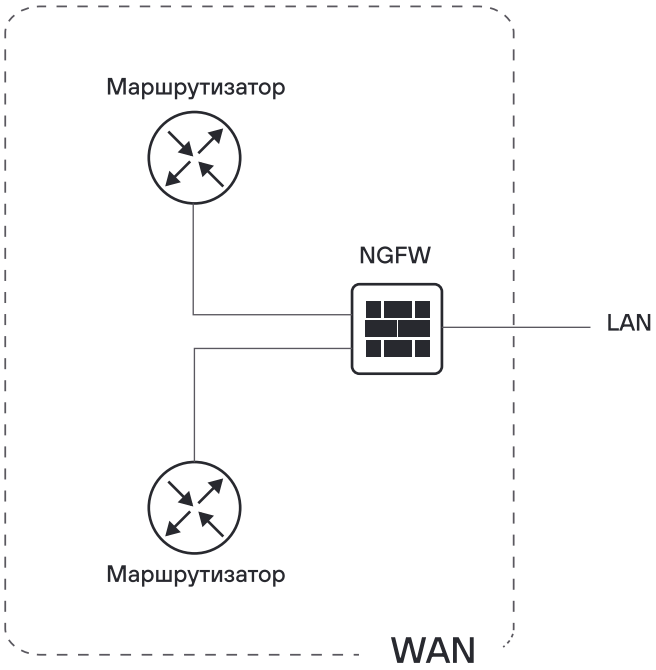
Для защиты от DDoS-атак рекомендуется использовать как решения on-premise (WAF, NGFW), так и облачные anti-DDoS-продукты.

Должно быть предусмотрено техническое решение, позволяющее безопасно и оперативно подключиться к инфраструктуре при возникновении аварии (в том числе связанной с кибератакой) на оборудовании периметра (например, резервный канал и выделенный VPN-сервер для подключения администраторов сети).

Доступ к управлению периметральным оборудованием должен осуществляться только из сети управления.

4.3. Сегмент WAN

Рисунок 4. Сегмент WAN



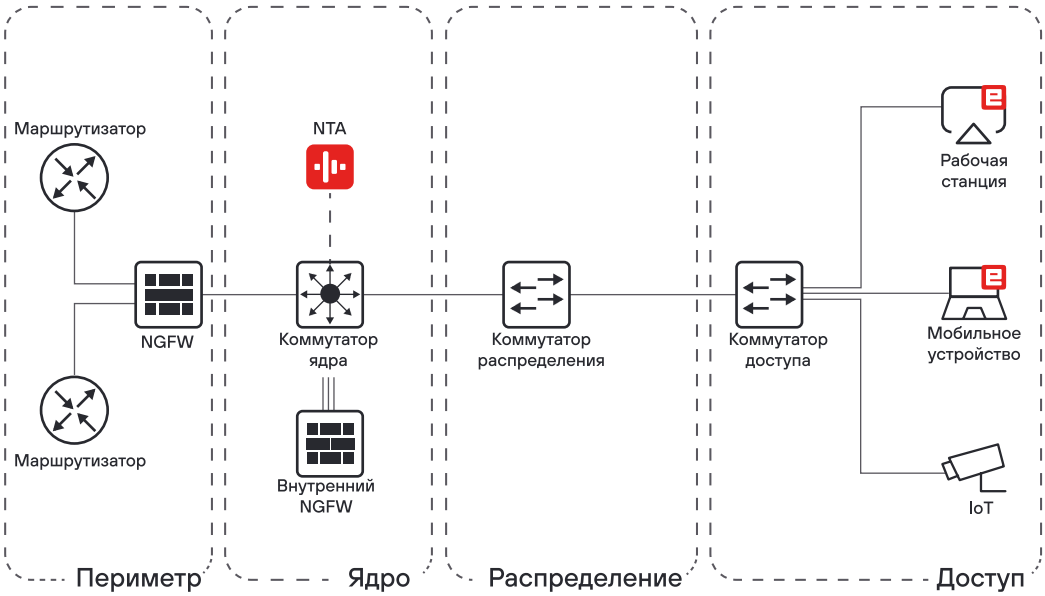
Весь трафик, передаваемый по WAN-каналам, должен быть зашифрован. Для этих задач рекомендуется использовать выделенные СКЗИ. В случае их отсутствия допускается использование маршрутизаторов распределенной сети (WAN) для построения VPN-каналов, при этом маршрутизаторы должны обеспечивать стойкое шифрование VPN-каналов по стеку технологий IPsec или ГОСТ. Если не требуется использовать отечественные алгоритмы шифрования при выборе общеизвестных «зарубежных» алгоритмов необходимо стремиться использовать наиболее криптостойкие алгоритмы.

В случае IPsec аутентификация должна проходить с использованием сертификатов, выданных собственным центром сертификации (CA). Использование самоподписанных сертификатов не допускается. Во время аутентификации концентраторы VPN-каналов должны проверять список отозванных сертификатов CRL CA. В случае компрометации устройства сертификат должен быть отозван. Передача сертификатов на удаленные устройства должна осуществляться либо физическим перемещением, либо по зашифрованным каналам связи. В случае крайней необходимости сертификат можно передать удаленному устройству через специально установленный для этих целей IPsec-туннель с аутентификацией по PSK. Для построения туннелей рекомендуется использовать FVRF.

Альтернативным вариантом шифрования WAN-каналов на основе L2 является WAN MACsec.

4.4. ЛВС кампуса или офиса

Рисунок 5. ЛВС кампуса



На коммутаторах неактивные порты должны быть административно выключены.

Для портов доступа конечных пользователей должен использоваться один из двух подходов:

- минимальный вариант — на портах должен быть закреплен соответствующий access VLAN. Должны быть настроены базовые технологии защиты, такие как port security (если за портом более одного устройства, необходимо вручную ограничивать количество MAC-адресов).

- целевой вариант — с использованием протоколов 802.1x и MAB. После прохождения аутентификации рекомендуется передать dACL на данный порт. В случае неуспешной аутентификации пользовательское устройство должно попадать в карантинный VLAN без доступа к ресурсам ЛВС.

Для защиты от несанкционированного трафика, приводящего к атакам типа MITM, внутри сетевого сегмента необходимо дополнительно настроить технологию DHCP snooping с дополнительными функциями безопасности dynamic ARP inspection и IP source guard.

Если в организации используется статическая адресация конечных узлов, формирование базы DHCP snooping необходимо прописывать вручную.

Uplink-порты должны быть настроены в жестком режиме trunk с ограниченным пропуском тегов нужных VLAN. Нетегированный трафик должен относиться к отдельному выделенному native VLAN, отличному от значения по умолчанию.

Для оборудования Cisco необходимо перевести режим протокола VTP в transparent.

Обязательно необходимо использовать функцию storm control для ограничения BUM-трафика. Значения подбираются исходя из нормальной работы порта.

Не допускается настройка портов в access default VLAN.

Для STP необходимо в явном виде назначить корневой коммутатор (root switch) для всех VLAN. Кроме того, необходимо использовать технологию root guard для предотвращения получения лучшего BPDU. BPDU guard должен быть прописан на всех портах PortFast.

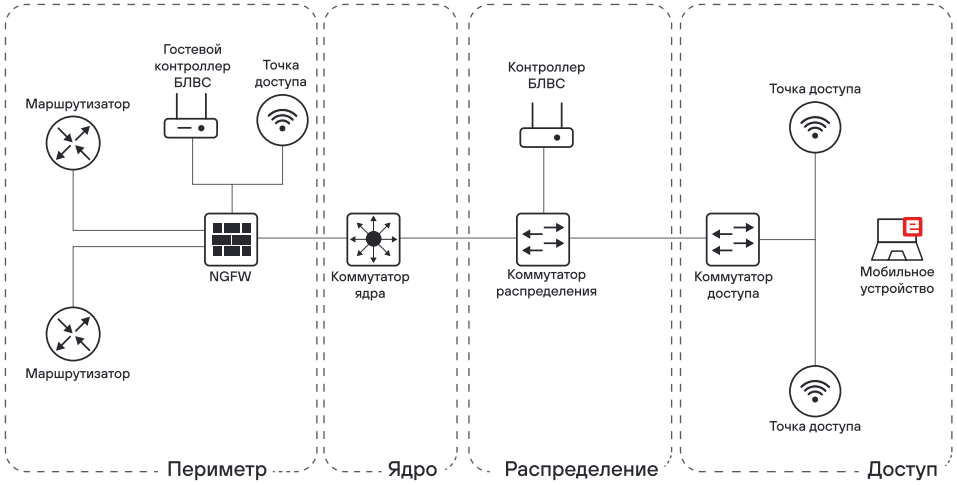
Для изоляции узла от других узлов в рамках одного широковещательного домена рекомендуется использовать private VLAN.

Рекомендуется использовать uRPF (проверка обратного пути пакета, антиспуфинг) как минимум в режиме loose (проверяется, есть ли в таблице маршрутизации обратный маршрут к источнику пакета) или в режиме strict (помимо проверки loose, также проверяется, что интерфейсы, куда пришел пакет и куда смотрит обратный маршрут до источника, совпадают). uRPF необходимо использовать с осторожностью, так как эта технология подходит не под все реализации сети, особенно с асимметричной маршрутизацией.

Пользовательский трафик может не выходить из сети кампуса — таким образом этот трафик становится невидимым для средств межсетевого экранирования. Для контроля трафика рекомендуется использовать межсетевые экраны на конечных точках и PT NAD.

4.5. Беспроводная ЛВС кампуса или офиса

Рисунок 6. Беспроводная ЛВС кампуса



В этом разделе

- Корпоративная сеть (см. раздел 4.5.1)
- Гостевой доступ (см. раздел 4.5.2)

4.5.1. Корпоративная сеть

В инфраструктуре предприятия необходимо использовать WPA3-Enterprise-192 и аутентификацию по стандарту 802.1x через RADIUS-сервер. Максимальной защиты можно добиться, используя EAP-TLS. Этот метод подразумевает использование сертификатов как на стороне сервера, так и на супликанте.

Для каждого пользователя необходимо сгенерировать сертификат и установить его на устройство пользователя. В случае увольнения сотрудника или потери супликанта сертификат пользователя отзывается.

Для обеспечения максимальной защиты управление точками доступа должно осуществляться централизованно. Если управление точками доступа или контроллерами предусматривает управление через интернет, необходимо использовать только HTTPS с усиленными криптографическими шифрами (устаревшие методы необходимо

исключить или удалить). Необходимо отключить управление через беспроводную сеть. Адреса управления должны быть доступны только администраторам БЛВС.

В случае невозможности использования WPA3 допускается применять WPA2-Enterprise, при этом необходимо обеспечить аутентификацию по сертификатам.

После аутентификации необходимо авторизовать пользователя в соответствии с его привилегиями и изолировать его от пользователей в той же подсети.

Необходимо использовать функциональность WIPS и средства обнаружения и подавления сторонних точек доступа.

Необходимо регулярно проводить радиоразведку на предмет помех, фейковых точек доступа в подконтрольном помещении (желательно в автоматическом режиме). Кроме того, нужно внимательно относиться к трафику в нерабочее время пользователей.

При гостевом доступе пользователь, подключенный по 802.11a/b/g, может намеренно ухудшать или замедлять производительность сети (подключившись с data rate 1, 2, 5,5), занимая больше эфирного времени для передачи данных. Рекомендуется отключить legacy data rate 1, 2, 5,5 Мбит/с.

Необходимо закрыть доступ из подсетей пользователей к точкам доступа. Должны быть отключены устаревшие методы, такие как LEAP, wireless uplink. В корпоративной сети не должно быть открытых WEP/WPA/TKIP, использующих PSK. Время ожидания EAP должно быть не более 30 секунд, повторные попытки — не более 2.

4.5.2. Гостевой доступ

Эта сеть не должна пересекаться с корпоративной сетью.

Для гостевых устройств при подключении к беспроводной сети весь трафик должен перенаправляться на гостевой портал, и, пока пользователь не авторизуется, весь остальной трафик необходимо блокировать. Пользователь должен пройти аутентификацию с помощью одноразового пароля и подписать пользовательское соглашение для использования беспроводной сети. Пользователю выдается доступ в интернет на ограниченное время, не более 8 часов. После этого сессия пользователя блокируется. Пользователи в этой подсети должны быть изолированы друг от друга.

При гостевом доступе пользователь, подключенный по 802.11a/b/g, может намеренно ухудшать или замедлять производительность сети (подключившись с data rate 1, 2, 5,5), занимая больше эфирного времени для передачи данных. Рекомендуется отключить legacy data rate 1, 2, 5,5 Мбит/с.

5. Защита оборудования

В работе сетевого устройства можно выделить три абстракции — Management Plane, Control Plane и Data Plane — которые необходимо защищать.

- Management Plane — обрабатывает трафик, который отправляется непосредственно на устройство для управления или контроля состояния этого устройства.
- Control Plane — отвечает за логику работы сетевого устройства для обеспечения возможности передачи пакетов в дальнейшем (заполнение таблиц маршрутизации, ARP-таблиц, отработку служебных протоколов семейства STP и т. д.).
- Data Plane — отвечает непосредственно за передачу трафика через сетевое устройство.

В этом разделе

- Защита Management Plane (см. раздел 5.1)
- Защита Control Plane (см. раздел 5.2)
- Защита Data Plane (см. раздел 5.3)

5.1. Защита Management Plane

В организации рекомендуется иметь сеть управления с ограниченным доступом к ее ресурсам. Администрирование сетевых устройств должно осуществляться только с выделенной сети или узлов. На сетевом оборудовании необходимо выделить отдельный порт, предусмотренный вендором, а при отсутствии такового нужно выделить VRF, отделенный от обычной корпоративной сети; доступ к оборудованию должен быть ограничен только этим интерфейсом.

Управление оборудованием должно осуществляться только через защищенные протоколы (SSHv2, SSL). Открытых каналов управления, таких как Telnet или HTTP, быть не должно. Кроме того, доступ к оборудованию должен быть ограничен политиками ACL, позволяющими подключаться к оборудованию только с выделенных узлов.

Необходимо использовать механизм поддержки TCP-сессий администратора устройства. Этот механизм позволяет удостовериться в том, что сессия активна, в противном случае сессия будет разорвана со стороны устройства.

Необходимо защитить конфигурацию устройства, чтобы усложнить эксфильтрацию ключей из файла конфигурации.

Пароли доступа к устройству необходимо зашифровать стойкими алгоритмами, они не должны храниться в текстовом виде в файле конфигурации.

Предустановленные производителем учетные записи должны быть удалены. Учетные записи для доступа и управления оборудованием должны быть персонифицированы. Доступ к устройству необходимо осуществлять с использованием модели AAA (серверы TACACS, RADIUS). Рекомендуем использовать протокол TACACS+ с параметрами авторизации команд и аккаунтинга, это позволит более гранулярно и безопасно настроить доступ для администраторов и технологических учетных записей и журналировать действия на устройствах. Кроме того, необходимо ограничивать количество неудачных попыток входа на оборудование как на сервере авторизации, так и локально на оборудовании (рекомендованные значения приведены в разделе Настройка оборудования (см. раздел 3.3)).

Роли учетных записей должны быть настроены на серверах учета согласно профилю и компетенциям владельцев учетных записей. Доступ к оборудованию должен быть ограничен политиками ACL, необходимо использовать тайм-ауты бездействия сеанса равные 5–10 минутам.

На устройстве должны быть только локальные учетные записи, необходимые для обеспечения доступа в аварийных режимах работы (например, отказ серверов AAA). Эти учетные записи не должны совпадать с предустановленной производителем административной УЗ (эта УЗ должна быть удалена), они должны быть персонифицированными, и их перечень должен актуализироваться при кадровых изменениях в административном составе.

Должен быть разработан и исполняться регламент работы с локальными учетными записями, включающий порядок смены паролей по истечении времени (или в случае компрометации).

Доступ по протоколу SNMP должен быть только с определенных адресов (ограничен при помощи листов доступа — ACL), должен использоваться защищенный протокол SNMPv3 с аутентификацией и шифрованием данных.

В целях обеспечения безопасности необходимо отключить любые ненужные и неиспользуемые службы.

Для своевременного обнаружения и расследования инцидентов ИБ необходимо использовать решения SIEM и NTA.

В момент расследования необходимо иметь точное доверенное время, не искаженное извне, поэтому рекомендуется использовать аутентификацию при настройке NTP (в случае технической поддержки со стороны сетевого оборудования и NTP-сервера).

Необходимо собирать syslog-сообщения со всего сетевого оборудования. Так как syslog отправляет данные в открытом виде, необходимо разрешать передачу этого типа только до места назначения либо использовать сеть управления (она не должна пересекаться с пользовательскими данными или сервисами) для передачи syslog-данных.

Необходимо настроить уведомления о превышении пороговых значений ЦПУ и памяти сетевых устройств. Значения подбираются исходя из показаний, полученных на основе ежедневного мониторинга оборудования.

Рекомендуется собирать и хранить метаданные NetFlow. Хорошей практикой считается настройка сбора метаданных как можно ближе к контролируемому источнику.

Протоколы управления, не поддерживающие шифрование передаваемых данных, необходимо исключить из использования.

Следует отключать протоколы обнаружения устройств (CDP, LLDP) на недоверенных портах (например, портах для внешних подключений, пользовательских портах, на которых не требуется работа этих протоколов).

Для контроля прямого взаимодействия с сетевыми устройствами необходимо использовать инфраструктурные списки доступа. При помощи iACL трафик, предназначенный для сетевых устройств (например, BGP-соединения, SNMP- и SSH-обращения), ограничивается узлами, с которых возможны эти обращения. Остальной трафик для этих соединений явно запрещается, и так же явно разрешается транзитный трафик.

5.2. Защита Control Plane

Для каждого сетевого устройства необходимо настроить защиту центрального процессора в соответствии с рекомендациями вендора (CoPP).

Как минимум необходимо настроить классификацию трафика Control Plane с выделением достаточной полосы. Это позволит зарезервировать ресурсы оборудования для критически важных классов трафика. Параметры для каждого класса нужно определять с учетом специфики сети компании. Пока параметры не определены, рекомендуется перевести violate-action drop в violate-action transmit.

На интерфейсах необходимо отключить отправку ICMP unreachables, кроме сегментов сети, где это действительно нужно.

Proxy ARP следует использовать только в случае крайней необходимости; во всех остальных случаях эта функция должна быть отключена. Proxy ARP может быть отключена как на интерфейсе, так и глобально.

Следует отключить возможность маршрутизации на основе параметров пакета.

По умолчанию сетевые устройства отправляют информацию о маршрутизации своим соседям и получают такую же информацию от них в открытом виде, что делает эту информацию видимой для всех заинтересованных сторон. Исходя из этого, должна быть настроена аутентификация динамических протоколов маршрутизации; в противном случае злоумышленник получит возможность участия в обмене маршрутной информацией, что позволит ему проводить как MITM-, так и DDoS-атаки.

При использовании BGP рекомендуется использовать технологию TTL security. Необходимо использовать фильтрацию маршрутной информации как по префиксам, так и с использованием автономных систем. Не рекомендуется использовать автоматическое обнаружение соседей в BGP. Для внешних подключений рекомендуется использовать ACL с фильтрацией соседств.

IGP-протоколы маршрутизации должны быть защищены от формирования соседства с несанкционированными маршрутизирующими устройствами путем выключения отправки hello-пакетов на интерфейсах (passive-interface). Там, где это возможно, необходимо использовать связки ключей (key chains). При использовании протоколов динамической маршрутизации необходимо ограничить объем получаемой маршрутной информации. Кроме того, необходимо фильтровать вводимую и объявляемую маршрутную информацию.

При использовании технологий FHRP необходимо настроить аутентификацию каждого устройства, участвующего в работе этих протоколов, и обязательно назначить главному максимальный приоритет.

5.3. Защита Data Plane

Необходимо отключить возможность маршрутизации по источнику, а также запретить использование опций IP.

На интерфейсах необходимо отключить отправку перенаправлений ICMP (ICMP redirects) и направленного широковещательного трафика (directed broadcast), кроме сегментов сети, где это действительно нужно.

В случае технической поддержки телекоммуникационным оборудованием необходимо использовать технологии защиты уровня L2 и L3, перечисленные в разделе ЛВС кампуса или офиса (см. раздел 4.4), например защиту от спуфинга (IP Source Guard), защиту от атак на DHCP-сервер (DHCP snooping), защиту от атак на ARP-таблицу сетевого устройства (DAI).

При сетевых инцидентах может потребоваться быстро идентифицировать и отследить сетевой трафик. Для этой задачи рекомендуется использовать NetFlow. Протокол обеспечивает видимость всего трафика в сети. NetFlow может использоваться с коллекторами, которые предоставляют анализ трафика и его исторические данные.

6. Чек-лист для проверки ЛВС

Администраторам ЛВС рекомендуется проверить параметры усиления безопасности ЛВС в соответствии с таблицей ниже. Если рекомендация не выполнена (результат «Нет»), необходимо запланировать работы, которые устранят данный пробел в безопасности ЛВС. Для каждой рекомендации установлен приоритет выполнения от 1 до 5, где 5 — рекомендация, которую необходимо выполнить в первую очередь, 1 — в последнюю.

Таблица 2. Чек-лист для проверки ЛВС

Рекомендация	Результат	Приоритет
Физический доступ к оборудованию закрыт	☐ Да ☐ Нет	4
Версии ПО и установленных обновлений оборудования со-ответствуют рекомендованным производителем оборудо-вания	☐ Да ☐ Нет	4
Настроена политика для локальных учетных записей: ■ длина пароля — не менее 15 символов; ■ пароль должен содержать строчные и заглавные буквы, спецсимволы и цифры; ■ пароль не должен содержать обычных слов, как русских, так и английских, или он должен удовлетворять парольной политике компании; ■ должно быть установлено время жизни пароля — не более года; ■ перерыв между попытками подключения — не менее 1 секунды; ■ блокировка учетной записи на 5 минут после трех неверных попыток авторизации	☐ Да ☐ Нет	5

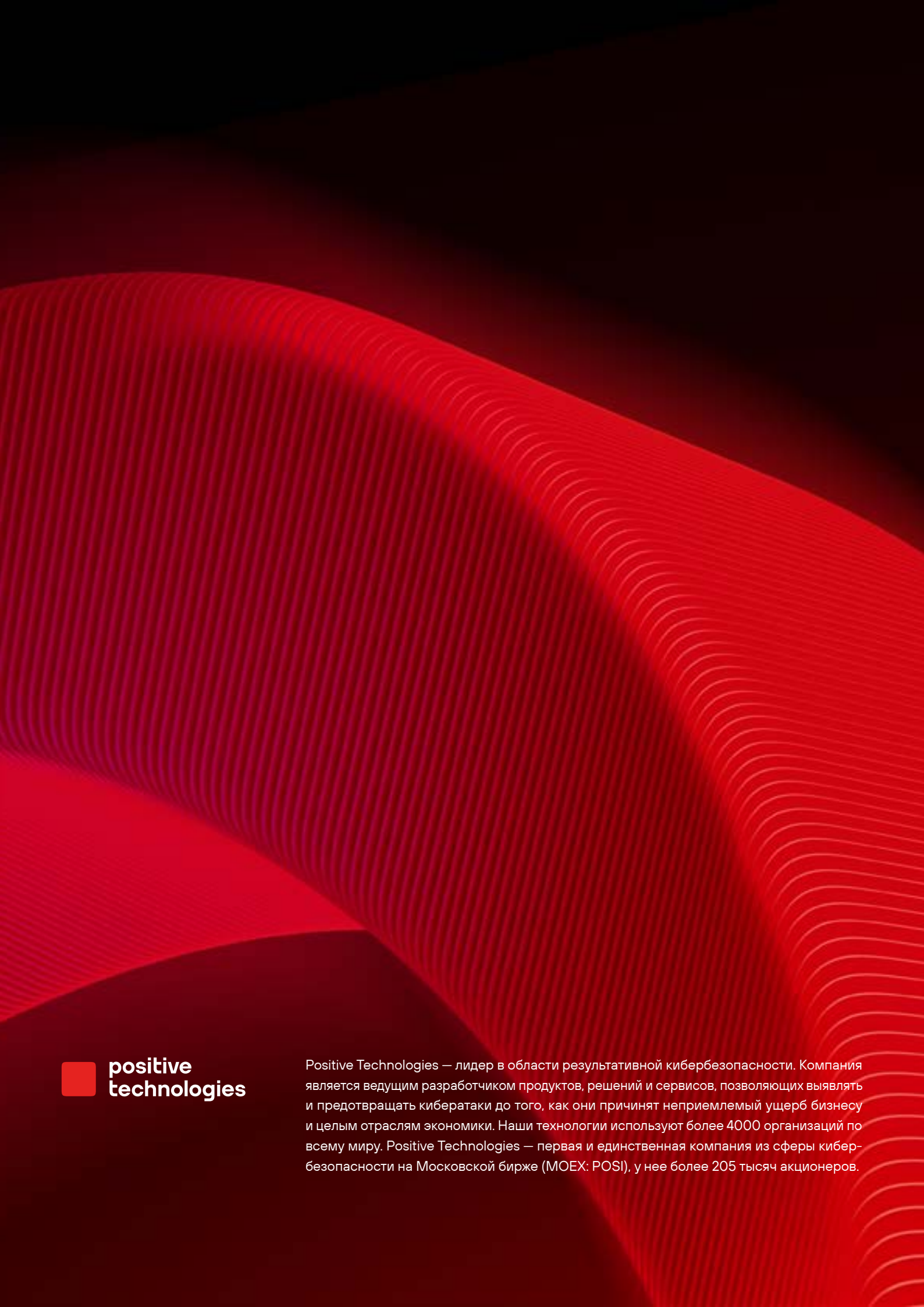
Рекомендация	Результат	Приоритет
Настроен механизм журналирования	☐ Да ☐ Нет	5
Используется подход AAA	☐ Да ☐ Нет	5
Используется SIEM сбора журналов	☐ Да ☐ Нет	3
Используется SSH/SCP	☐ Да ☐ Нет	5
Используется NetFlow	☐ Да ☐ Нет	2
Есть система управления файлами конфигураций	☐ Да ☐ Нет	3
Настроена защита протокола STP	☐ Да ☐ Нет	4
Telnet отключен	☐ Да ☐ Нет	5
Служба HTTP отключена	☐ Да ☐ Нет	5
На всех ненадежных интерфейсах CDP отключен	☐ Да ☐ Нет	3

Рекомендация	Результат	Приоритет
На всех ненадежных интерфейсах LLDP отключен	☐ Да ☐ Нет	3
Используется механизм поддержки TCP-сессий администратора	☐ Да ☐ Нет	4
Используется выделенный интерфейс для управления оборудованием	☐ Да ☐ Нет	4
Используется port-security	☐ Да ☐ Нет	2
Для подключения пользователей используется 802.1x	☐ Да ☐ Нет	3
Используется механизм защиты DHCP-сервера (DHCP snooping)	☐ Да ☐ Нет	2
Используется механизм защиты ARP-таблиц (DAI)	☐ Да ☐ Нет	2
Используется IP Source Guard	☐ Да ☐ Нет	2
Используется uRPF	☐ Да ☐ Нет	2
На L3-интерфейсах выключен ICMP unreachables	☐ Да ☐ Нет	3
На оборудовании выключен Proxy ARP	☐ Да ☐ Нет	3

Рекомендация	Результат	Приоритет
На оборудовании выключен ICMP redirects	☐ Да ☐ Нет	3
На оборудовании выключен directed broadcast	☐ Да ☐ Нет	3
Для протоколов динамической маршрутизации используется аутентификация	☐ Да ☐ Нет	4
Для протоколов динамической маршрутизации используется фильтрация маршрутной информации	☐ Да ☐ Нет	3
Для протоколов динамической маршрутизации используется настройка passive-interface, кроме интерфейсов, участвующих в обмене маршрутной информацией	☐ Да ☐ Нет	4
Для протоколов FHRP настроена аутентификация	☐ Да ☐ Нет	3
Для протоколов FHRP задан мастер с максимальным прио-ритетом	☐ Да ☐ Нет	3
VLAN 1 (default) не используется в сети	☐ Да ☐ Нет	4
Все L2-соединения настроены либо как access, либо как trunk с обязательным указанием разрешенных VLAN	☐ Да ☐ Нет	3
Настроен контроль BUM-трафика	☐ Да ☐ Нет	2

Рекомендация	Результат	Приоритет
На оборудовании настроен протокол NTP с аутентификацией	☐ Да ☐ Нет	3
Для мониторинга оборудования настроен SNMPv3 с аутен-тификацией и шифрованием данных	☐ Да ☐ Нет	4
При построении VPN-туннелей для трафика, выходящего за пределы контролируемой зоны, используются криптографи-ческие алгоритмы DH 19, AES-256, SHA-256 или более стой-кие	☐ Да ☐ Нет	3
Для IPSEC-туннелей используются IKEv2 и PFS	☐ Да ☐ Нет	3
RA VPN использует MFA и (или) аутентификацию по серти-фикатам	☐ Да ☐ Нет	4
Для БЛВС используется WPA3-Enterprise-256 (если обору-дование его не поддерживает, то используется WPA2-Enterprise)	☐ Да ☐ Нет	3
На оборудовании настроены и используются iACL	☐ Да ☐ Нет	2
На оборудовании настроены и используются tACL	☐ Да ☐ Нет	2
На оборудовании настроен CoPP	☐ Да ☐ Нет	2

Рекомендация	Результат	Приоритет
Сеть сегментирована — выделены сегменты DMZ, сегменты критически значимых систем, сегменты ключевых пользователей, создана сеть управления	☐ Да ☐ Нет	4
Между сегментами используются средства фильтрации трафика	☐ Да ☐ Нет	4
Фильтрация трафика построена по принципу «наименьшего доверия» — запрещено все, что не разрешено	☐ Да ☐ Нет	4
Для контроля трафика используется NetFlow с коллекторами	☐ Да ☐ Нет	1
Периметральный трафик отправляется на NTA-оборудование	☐ Да ☐ Нет	1



positive technologies

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.