Приложение 4

Организационные и технические меры по повышению защищенности внешнего периметра органа (организации)

1. Работы по администрированию, управлению конфигурацией и эксплуатации сетевых (пограничных) устройств.

1.1. Обеспечить выполнение работ по настройке (администрированию) сетевых (пограничных) устройств с отдельных автоматизированных рабочих мест, изолированных от сети «Интернет», предназначенных только для администрирования указанного оборудования. Осуществлять настройку сетевых (пограничных) устройств в соответствии с эксплуатационной документацией производителя.

1.2. Обеспечить настройку сетевых (пограничных) устройств, используя авторизацию по сертификатам. В случае отсутствия возможности реализовать подобным образом авторизацию, учитывать следующие требования к сложности пароля:

длина пароля должна быть не менее 15 символов;

пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (например, !, », №, %, *, /);

в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов);

1.3. Для каждого сетевого (пограничного) устройства использовать отличные друг от друга пароли.

1.4. Организовать контроль конфигураций сетевых (пограничных) устройств с использованием организационных и технических мер (например, средства управления привилегированным доступом (PAM), служба централизованных каталогов учетных записей (LDAP-каталоги), обеспечивающих разграничение административного доступа, регламентирование процессов изменения конфигурации, контроль целостности конфигураций, регистрацию и анализ событий, а также возможность установления причин и ответственных лиц в случае выявления несанкционированных изменений.

1.5. Выявить перечень сервисов (служб), функционирующих в информационной инфраструктуре органа (организации), которые в перечне публичных (внешних) IP-адресов доступны из сети «Интернет». Определить легитимность доступных по открытым портам сервисов, IP-адресов, сетевых служб, доступ к которым возможен за периметром информационной инфраструктуры органа (организации). В случае невозможности отнесения их к легитимным осуществить их блокировку.

1.6. Обеспечить учет сетевых (пограничных) устройств, размещенных на сетевом периметре информационной инфраструктуры, с указанием их назначения, конфигурации, версий программного обеспечения, сроков эксплуатации и сроков технической поддержки со стороны производителей.

1.7. Обеспечить управление жизненным циклом сетевых (пограничных) устройств, срок эксплуатации (технической поддержки) которых приближается к окончанию и не подлежащих исключению из эксплуатации. Организовать принятие компенсирующих мер по защите информации, учитывая невозможность устранения выявляемых в них уязвимостей программного обеспечения.

1.8. Исключить удаленное администрирование сетевых (пограничных) устройств, в том числе публикацию интерфейсов удаленного управления (SSH, RDP, VNC) на сетевом периметре или в демилитаризованной зоне сетевой инфраструктуры органа (организации).

1.9. Обеспечить обязательное согласование с ответственными за информационную безопасность лицами в органе (организации) вносимых изменений в конфигурацию сетевых (пограничных) устройств. К изменениям конфигурации сетевых (пограничных) устройств, подлежащим обязательному согласованию относятся любые изменения, способные повлиять на разграничение доступа, сегментацию сети, реализацию функций средств защиты информации, регистрацию событий безопасности, параметры аутентификации и управление сетевым периметром информационной инфраструктуры.

1.10. Обеспечить использование безопасных протоколов для мониторинга сетевых (пограничных) устройств (HTTPS, SNMP v3), с отключением небезопасных протоколов и сервисов (HTTP, SNMP v1/v2).

2. Меры по защите информации для повышения устойчивости сетевой инфраструктуры к атакам, направленным на «отказ в обслуживании» (DDoS-атакам).

2.1. Обеспечить настройку правил межсетевого экранирования для блокировки неразрешенного входящего и исходящего сетевого трафика.

2.2. Обеспечить фильтрацию сетевого трафика прикладного уровня с использованием межсетевого экрана уровня веб-приложений (WAF), установленного в режим противодействия атакам.

2.3. Обеспечить активацию функций защиты от атак, направленных на «отказ в обслуживании» (DDoS-атак), на межсетевых экранах и других средствах защиты информации.

2.4. Обеспечить ограничение количества подключений с одного IP-адреса (например, с использованием параметра rate-limit).

2.5. Организовать взаимодействие с оператором связи (провайдером услуг связи) в части применения мер противодействия атакам, направленным на «отказ в обслуживании» (DDoS-атакам), в соответствии с условиями договора и планом реагирования на такие атаки.

3. Сегментирование сети и внедрение средств контроля и управления доступом для предотвращения компрометации основных сегментов сети.

3.1. Осуществить сегментацию сети с применением технологий VLAN на сетевом оборудовании (логическая сегментация), на уровне управления

виртуальной инфраструктурой (логическая сегментация), а также путем создания локальной вычислительной сети для ключевых сегментов.

3.2. Организовать управление и контроль сетевого трафика между сегментами сети посредством внедрения списков контроля доступа (ACL) с учетом обрабатываемой в таких сегментах категорий информации (служебная, персональные данные).

3.3. Настроить доступ к сети по модели нулевого доверия (ZTNA).

3.4. Обеспечить невозможность администрирования устройств уровня ядра сети со стороны пользовательских, серверных и внешних сегментов информационной инфраструктуры при сохранении основных функций ядра сети.

3.5. Организовать создание демилитаризованной зоны (DMZ) для внешних сетевых взаимодействий. Обеспечить отсутствие прямого доступа из демилитаризованной зоны (DMZ) к внутренним сегментам инфраструктуры, за исключением регламентированных взаимодействий.

4. Резервное копирование конфигурационных файлов.

4.1. Регламентировать процесс резервного копирования конфигураций сетевых (пограничных) устройств в органе (организации), в рамках которого определить ответственное лицо (подразделение) в органе (организации) и его обязанности по выполнению мероприятий по регулярному резервному копированию конфигурационных файлов сетевых (пограничных) устройств органа (организации).

4.2. Определить место, способ хранения конфигурационных файлов сетевого оборудования и частоту снятия резервных копий. В этих целях необходимо руководствоваться следующими принципами:

создавать и хранить не менее трех резервных копий конфигурационных файлов – одну основную и две резервные;

использовать для хранения резервных копий не менее двух разных типов носителей информации (например, внешние жесткие диски и систему хранения данных);

хранить одну из резервных копий в отдельном (обособленном) от иных резервных копий месте.

4.3. Производить резервное копирование конфигурационных файлов сетевого оборудования не реже одного раза в месяц.

4.4. Определить перечень учетных записей, имеющих права осуществлять резервное копирование.

4.5. Обеспечить резервное копирование следующих конфигураций сетевых (периметровых) устройств, критичных для обеспечения безопасности информации и устойчивости функционирования информационной инфраструктуры:

правила межсетевого экранирования (ACL, firewall rules);

параметры сегментации сети (конфигурации VLAN);

настройки трансляции сетевых адресов (NAT);

списки пользователей, ролей и прав доступа.

4.6. Обеспечить контроль возможности восстановления конфигураций сетевых (пограничных) устройств из резервных копий не реже одного раза в три месяца.

5. Управление уязвимостями сетевого (пограничного) оборудования.

5.1. Обеспечить реализацию процессов управления уязвимостями в соответствии с Методикой анализа защищенности информационных систем, утвержденной ФСТЭК России 25.11.2025, и Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным ФСТЭК России 17.05.2023 (https://fstec.ru/dokumenty/vse-dokumenty/).

5.2. Обеспечить установку обновлений безопасности на устройствах, расположенных на сетевом периметре в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022, а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025 (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

6. Аутентификация и управление доступом пользователей и администраторов.

6.1. Обеспечить централизованный контроль доступа к сети с использованием межсетевых экранов и системы централизованного контроля доступа пользователей и администраторов к сетевым устройствам (NAC).

6.2. Обеспечить применение многофакторной аутентификации при осуществлении административного доступа к инфраструктуре, из которой осуществляется доступ к сетевым (пограничным) устройствам.

6.3. Обеспечить разграничение ролей администрирования с предоставлением минимально необходимых привилегий для каждой роли (администратор безопасности, администратор сети, оператор).

7. Регистрация событий информационной безопасности и их анализ.

7.1. Обеспечить сбор событий безопасности информации с использованием системы мониторинга и управления событиями информационной безопасности (SIEM-систем), обеспечивающих автоматизированную обработку событий, выявление аномалий и признаков нарушений безопасности информации, формирование уведомлений (оповещений), а также поддержку расследования инцидентов информационной безопасности.

7.2. Обеспечить централизованный сбор, хранение и анализ журналов регистрации событий безопасности информации с установлением максимально детализированного уровня журналирования, достаточного для выявления и расследования инцидентов информационной безопасности, а также с установленными временными метками (с использованием средств синхронизации времени в информационной инфраструктуре (NTP-сервер)). Сбору, хранению и анализу подлежат:

успешные и неуспешные попытки авторизации, включая имя пользователя, используемый им метод (многофакторная аутентификация,

SSH-ключ, сертификат или иной способ), IP-адрес, время, имя хоста, а также соответствующие идентификаторы сеанса;

журналы сервисов и приложений (HTTP/HTTPS-запросы и ответы, сеансы интерактивной командной строки (CLI) и аналогичные сервисы, включая IP-адреса, методы запросов, используемые URI, версии протоколов, пользовательские агенты, идентификаторы сеансов, коды состояния ответов и объем переданных данных);

создание процессов, путь к исполняемому файлу, имя пользователя, передаваемые и получаемые аргументы;

коды завершения процессов и причины их завершения;

загрузка и выгрузка модулей и библиотек, включая имя модуля или библиотеки, версию, путь к файлу, идентификатор связанного процесса и пользовательский контекст;

создание, изменение и удаление файлов в файловой системе, включая корневой веб-каталог, каталоги конфигурации и системные бинарные файлы;

выполненные DNS-запросы, включая такие типы записей как A, AAAA, TXT, SOA, NS, MX и PTR;

обновления программного обеспечения, включая успешные и неудачные попытки, номера текущей и целевой версий, источники обновления (например, URL-адрес или репозиторий), подтвержденные цифровые подписи или контрольные суммы, пользователя или процесс, инициировавшего обновление, а также сообщения об ошибках;

изменения в конфигурации устройств;

изменения параметров ведения журнала, предыдущие и новые значения, пользователя или процесс, внесший изменения, способ внесения изменений;

резервное копирование конфигурации, экспорт и (или) загрузка;

журнал попыток очистки, ротации или изменения файлов журнала событий.

7.3. Обеспечить реализацию механизмов оповещения администраторов информационной безопасности о фактах успешной аутентификации с административными привилегиями, множественных неуспешных попыток аутентификации, смены способа аутентификации (попытки обойти MFA), внесении изменений в конфигурацию программных и программно-аппаратных средств, изменение параметров ведения журнала, попыток очистки, ротации или изменения журналов событий, обновления программного обеспечения из непредусмотренных источников, экспорта, загрузки или восстановления конфигурации.

8. Проводить регулярные учения по реагированию на инциденты информационной безопасности для подтверждения их эффективности и способности органа (организации) обеспечивать выявление, локализацию, устранение инцидентов и восстановление работоспособности информационной инфраструктуры.