**Тема лекции: Средства защиты информации в локальных вычислительных сетях при межсетевом взаимодействии**

**Учебные вопросы:**

1. Требования к межсетевым экранам.
2. Правила межсетевого экранирования.

**В.1.** Межсетевой экран (МСЭ) — это устройство (программный или программно-аппаратный элемент компьютерной сети) обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

Требования к межсетевым экранам определены приказом ФСТЭК России от 9 февраля 2016 г. №9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный № 41564 для служебного пользования). Требования к межсетевым экранам выпущены на замену Руководящему документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД МЭ), утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

В целях разъяснения позиции ФСТЭК России в связи с утверждением Требований к межсетевым экранам было выпущено Информационное сообщение по вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации от 24 марта 2017 г. №240/24/1382.

Допускается применение межсетевых экранов, сертифицированных на соответствие РД МЭ (при условии наличия действующих сертификатов соответствия требованиям по безопасности информации) в информационных (автоматизированных) системах, созданных до вступления в силу соответствующих изменений в Требования о защите информации, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17, Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21.

Согласно Требований 2016 года устанавливается 5 типов межсетевых экранов:

• Типа А - уровня сети;

• Типа Б – уровня логических границ сети;

• Типа В – уровня узла;

• Типа Г – уровня веб-сервера;

• Типа Д – уровня промышленной сети (АСУ ТП).

**Типы межсетевых экранов**

«А» – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы. Межсетевые экраны типа «А» могут иметь только программно-техническое исполнение;

«Б» – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы. Межсетевые экраны типа «Б» могут иметь программное или программно-техническое исполнение;

«В» – межсетевой экран, применяемый на узле (хосте) информационной системы. Межсетевые экраны типа «В» могут иметь только программное исполнение и устанавливаются на мобильных или стационарных технических средствах конкретного узла информационной системы;

«Г» – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;

«Д» – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных.

**Межсетевые экраны типа «А»**

Согласно Профилям МЭ должен противодействовать следующим угрозам безопасности информации:

• Несанкционированный доступ к информации, содержащейся в информационной системе;

• Отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

• Несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

• Несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

• Несанкционированное получение сведений о сети информационной системы (автоматизированной системы управления), а также об ее узлах.

Должны быть реализованы следующие функции безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Класс 6** | **Класс 5** | **Класс 4** |
| контроль и фильтрация | + | + | + |
| идентификация и аутентификация | + | + | + |
| регистрация событий безопасности (аудит) | + | + | + |
| обеспечение бесперебойного функционирования и восстановление | + | + | + |
| тестирование и контроль целостности |  | + | + |
| преобразование сетевых адресов |  |  | + |
| маскирование |  |  | + |
| приоритизация информационных потоков |  |  | + |
| управление (администрирование) | + | + | + |
| взаимодействие с другими средствами защиты информации |  |  | + |

В среде должны быть реализованы следующие функции безопасности среды:

• исключение каналов связи в обход правил фильтрации;

• обеспечение доверенного канала;

• обеспечение доверенного маршрута;

• физическая защита;

• обеспечение безопасного функционирования;

• обеспечение взаимодействия с сертифицированными средствами защиты информации.

**Межсетевые экраны типа «Б»**

Согласно Профилям МЭ должен противодействовать следующим угрозам безопасности информации:

• Несанкционированный доступ к информации, содержащейся в информационной системе;

• Отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

• Несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

• Несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

• Несанкционированное получение сведений о сети информационной системы (автоматизированной системы управления), а также об ее узлах.

Должны быть реализованы следующие функции безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Класс 6** | **Класс 5** | **Класс 4** |
| контроль и фильтрация | + | + | + |
| идентификация и аутентификация | + | + | + |
| регистрация событий безопасности (аудит) | + | + | + |
| обеспечение бесперебойного функционирования и восстановление | + | + | + |
| тестирование и контроль целостности |  | + | + |
| преобразование сетевых адресов |  |  | + |
| маскирование |  |  | + |
| приоритизация информационных потоков |  |  | + |
| управление (администрирование) | + | + | + |
| взаимодействие с другими средствами защиты информации |  |  | + |

В среде должны быть реализованы следующие функции безопасности среды:

• исключение каналов связи в обход правил фильтрации;

• обеспечение доверенного канала;

• обеспечение доверенного маршрута;

• физическая защита;

• обеспечение безопасного функционирования;

• тестирование и контроль целостности

• обеспечение взаимодействия с сертифицированными средствами защиты информации.

**Межсетевые экраны типа «В»**

Согласно Профилям МЭ должен противодействовать следующим угрозам безопасности информации:

• Несанкционированный доступ к информации, содержащейся в информационной системе;

• Отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

• Несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

• Несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

Должны быть реализованы следующие функции безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Класс 6** | **Класс 5** | **Класс 4** |
| контроль и фильтрация | + | + | + |
| идентификация и аутентификация |  |  | + |
| регистрация событий безопасности (аудит) | + | + | + |
| обеспечение бесперебойного функционирования и восстановление | + | + | + |
| тестирование и контроль целостности | + | + | + |
| преобразование сетевых адресов |  |  |  |
| маскирование |  |  |  |
| приоритизация информационных потоков |  |  |  |
| управление (администрирование) | + | + | + |
| взаимодействие с другими средствами защиты информации |  |  | + |

В среде должны быть реализованы следующие функции безопасности среды:

• исключение каналов связи в обход правил фильтрации;

• обеспечение доверенного канала;

• обеспечение доверенного маршрута;

• физическая защита;

• обеспечение безопасного функционирования;

• тестирование и контроль целостности

• обеспечение взаимодействия с сертифицированными средствами защиты информации.

**Межсетевые экраны типа «Г»**

Согласно Профилям МЭ должен противодействовать следующим угрозам безопасности информации:

• Несанкционированный доступ к информации веб-сервера;

• Отказ в обслуживании сервера, обслуживающего сайты, веб-службы и веб-приложения;

• Несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

Должны быть реализованы следующие функции безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Класс 6** | **Класс 5** | **Класс 4** |
| контроль и фильтрация | + | + | + |
| идентификация и аутентификация | + | + | + |
| регистрация событий безопасности (аудит) | + | + | + |
| обеспечение бесперебойного функционирования и восстановление | + | + | + |
| тестирование и контроль целостности | + | + | + |
| преобразование сетевых адресов |  |  |  |
| маскирование |  |  |  |
| приоритизация информационных потоков |  |  |  |
| управление (администрирование) | + | + | + |
| взаимодействие с другими средствами защиты информации | + | + | + |

В среде должны быть реализованы следующие функции безопасности среды:

• исключение каналов связи в обход правил фильтрации;

• обеспечение доверенного канала;

• обеспечение доверенного маршрута;

• физическая защита;

• обеспечение безопасного функционирования;

• тестирование и контроль целостности

• обеспечение взаимодействия с сертифицированными средствами защиты информации;

• контроль шифрованного потока.

**Межсетевые экраны типа «Д»**

Согласно Профилям МЭ должен противодействовать следующим угрозам безопасности информации:

• Несанкционированный доступ к информации, содержащейся в автоматизированной системе управления;

• Отказ в обслуживании автоматизированной системы управления и (или) ее отдельных компонентов;

• несанкционированная передача информации из автоматизированной системы управления в информационно-телекоммуникационные сети или иные информационные системы;

• Несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности.

Должны быть реализованы следующие функции безопасности:

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Класс 6** | **Класс 5** | **Класс 4** |
| контроль и фильтрация | + | + | + |
| идентификация и аутентификация | + | + | + |
| регистрация событий безопасности (аудит) | + | + | + |
| обеспечение бесперебойного функционирования и восстановление | + | + | + |
| тестирование и контроль целостности |  | + | + |
| преобразование сетевых адресов |  |  |  |
| маскирование |  |  |  |
| приоритизация информационных потоков |  |  |  |
| управление (администрирование) | + | + | + |
| взаимодействие с другими средствами защиты информации |  |  |  |

В среде должны быть реализованы следующие функции безопасности среды:

• исключение каналов связи в обход правил фильтрации;

• обеспечение доверенного канала;

• обеспечение доверенного маршрута;

• физическая защита;

• обеспечение безопасного функционирования;

• обеспечение взаимодействия с сертифицированными средствами защиты информации.

**В.2. Правила межсетевого экранирования**

1. Наличие правила, используемого для доступа с сервера управления и компьютера администратора к шлюзу безопасности. Остальным доступ должен быть запрещен.

2. Наличие правила, используемого для блокирования любой попытки доступа к самому шлюзу, что делает его “невидимым” и исключает возможность несанкционированного доступа. Следует обратить внимание, что данное правило должно иметь более низки приоритет чем указанное в пункте 1.

3. Отсутствуют правила разрешающие весь трафик.

4. Запрещен входящий интернет-трафик для отдельных сегментов (например для определенных отделов).

5. Запрещен FTP-трафик из сети интернет в демилитаризованную зону.

6. Отсутствуют неиспользуемые правила. Если последнее использование правила было более чем шесть месяцев назад, то рекомендуется удалить данное правило, дабы не перегружать общий список.

7. Запись в журнал (лог) всех важных событий, исключая широковещательный трафик. При необходимости можно вести запись и широковещательного трафика, но это может перегружать журнал.

8. Для всех правил должно быть указано смысловое имя и присутствует комментарий, поясняющий назначение этого правила.

9. На всех шлюзах должно быть включено логирование.

10. На всех шлюзах настроен резервный лог-сервер. Это позволит сохранить важные сообщения в случае отказа основного лог-сервера.

11. На всех шлюзах включена функция локального хранения логов. Это позволит сохранить информацию о событиях в случае недоступности лог-сервера.

12. На всех шлюзах настроено создание нового лог-файла при достижении определенного размера старого. Это значительно ускорит обработку логов (отображение, поиск). Вернуться к более старым логам можно будет, переключив Лог-файл.

13. На всех шлюзах настроены уведомления сигнализирующие о заканчивающемся дисковом пространстве. Уровень срабатывания выбирается в зависимости от общего объема жесткого диска.

14. На всех шлюзах настроено удаление старых лог-файлов при заканчивающемся дисковом пространстве. Уровень срабатывания выбирается в зависимости от общего объема жесткого диска.

15. На всех шлюзах настроено автоматическое резервное копирование, которое выполняется перед удалением старых лог-файлов (при необходимости).

16. На всех шлюзах включено средство Anti-Spoofing против подделки исходящих IP-адресов для всех интерфейсов.

17. Проверьте значения временных интервалов настроенных по умолчанию и измените их в случае необходимости в соответствии с требованиями вашей сети.

18. В настройках оптимизации шлюза укажите максимальное количество конкурентных сессий для предотвращения его перегрузки.

19. Пароли учетных записей пользователей и администраторов истекают не позднее чем через 180 дней (в зависимости от локальной парольной политики организации или учреждения).Также должно быть настроено оповещение об истекающем пароле.

20. При интеграции с Active Directory настроена смена пароля.

21. Активирована блокировка Администраторов. Учетная запись блокируется на определенный промежуток времени в случае трех неудачных попыток входа. Настроено уведомление о блокировке и сброс сессии управления, неактивной в течение определенного времени.

22. В свойствах шлюзов выставлена опция (правило), позволяющая блокировать запрещенные соединения сразу после установки новой политики и не ждать окончания сессии.

23. Настроена синхронизация времени (NTP) Это позволяет видеть актуальную дату и время для всех событий (логов).

**Написание правил межсетевого экранирования**

1. Не следует разрешать то, что и так не запрещено. Использование таких правил приводит к бесполезному расходу ресурсов.

2. Лучше не использовать нормально открытый межсетевой экран, то есть такой, в котором по умолчанию разрешено все. Это приводит к большому количеству запретительных правил, через которые проходит пакет, что увеличивает нагрузку на процессор устройства.

3. Неверный порядок правил. В межсетевом экране правила обрабатываются по порядку и порядок правил имеет значение. Возможна ситуация, когда запрещающее правило не работает потому, что выше есть правило, которое разрешает этот трафик, либо что разрешено не работает, так как выше есть запрещающее правило.

4. Запрет BOGON–адресов. BOGON–адреса – это IP-адреса, которые не должны встречаться в таблицах маршрутизации в Интернет. Этим термином описываются частные и зарезервированные диапазоны адресов. При их запрете вначале правил маршрутизации делается их список, а затем запрещают его для входящего интерфейса.

**Защита информации в локальных вычислительных сетях**

Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

Средства защиты информации должны располагаться на каждом узле ЛВС вне зависимости от того, обрабатывается ли на нем конфиденциальная информация. Каждый администратор и пользователь ЛВС должен иметь уникальный пароль, идентификатор и, в случае использования криптографических средств защиты, ключ шифрования.

Класс защищенности ЛВС определяется в соответствии с классификацией АС.

Состав пользователей ЛВС должен утверждаться руководителем организации и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде межсетевого экрана (МЭ). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли.

Абонентский пункт (АП) с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

Коммуникационное оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.) и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны. При конфигурировании коммуникационного оборудования) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

При подключении ЛВС к АС с другим классом защищенности необходимо использовать межсетевой экран в соответствии с НПА.

Если каналы связи выходят за пределы контролируемой зоны, необходимо использование защищенных каналов связи либо сертифицированных криптографических средств защиты.

Вопросы?