Методические рекомендации к практическому занятию №5

С.А. Краснов

УСТАНОВКА И НАСТРОЙКА СЗИ В ЛВС ПРИ МЕЖСЕТЕВОМ ВЗАИМОДЕЙСТВИИ

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 5

**УСТАНОВКА И НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ПРИ МЕЖСЕТЕВОМ ВЗАИМОДЕЙСТВИИ**

***Цель работы.*** Получить практические навыки настройки МЭ СЗИ НСД «Dallas Lock».

***Теоретические сведения.***

1. **Назначение и общие принципы работы** **межсетевого экрана:**

Межсетевой экран (МЭ) является модулем СЗИ НСД Dallas Lock 8.0 и предназначен для защиты рабочих станций и серверов от несанкционированного доступа посредством осуществления контроля и фильтрации, проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.

Для работы МЭ не требуется внесение изменений в структуру существующей сети.

## Возможности межсетевого экрана

Модуль МЭ осуществляет защиту как физических, так и виртуальных машин и поддерживает работу со всеми основными сетевыми протоколами.

Задавать ограничения можно по работе служебных и прикладных протоколов, сетевых интерфейсов, портов и т. д. А также распределять уровни доступа среди пользователей, компьютеров, групп пользователей. Функции МЭ осуществляются посредством контроля и фильтрации сетевых пакетов в соответствии с набором параметров, таких как параметры сетевых протоколов, профили, исключения, учётные записи пользователей, сетевые интерфейсы и приложения.

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность выполнить настройку правил МЭ для пользователей, работающих под различными уровнями доступа.

Работа МЭ осуществляется посредством:

 фильтрации сетевого трафика;

 работы правил исключения;

 разделения сетей на доверенные и не доверенные согласно профилям;

 контроля сетевых соединений;

 сбора и отображение статистической информации о функционировании МЭ;

 удалённого и централизованного управления.

Защита сетевых соединения осуществляется посредством проверки подлинности сетевых ресурсов, источника и приёмника данных, сообщений, проведения контроля доступа к ресурсам сети.

При помощи функций удалённого и централизованного управления Dallas Lock 8.0 реализована возможность выполнения всех необходимых операций по администрированию настроек МЭ с одного рабочего места. Возможно осуществлять такие операции как:

включение, выключение, установка и изменение правил для входящих/исходящих пакетов данных (соединений), просмотр журналов событий и статистики.

Сбор информации о работе сети ведётся на всех компьютерах системы, на которых установлен МЭ Dallas Lock 8.0.

Модули СОВ и МЭ не контролируют трафик, идущий внутри виртуальной сети VipNet.

***Практическая часть:***

## Эксплуатация

Управление настройками межсетевого экрана доступно пользователям, которым назначена возможность изменения настроек МЭ – администраторам ЗАРМ Dallas Lock (по умолчанию членам группы «Администраторы») и происходит из оболочки администратора во вкладке «Межсетевой экран».

## Адреса

В данной категории отображается список локальных адресов компьютера, посредством которых к нему можно обратиться.

## Сетевые профили

Механизм «Сетевых профилей» позволяет применять правила МЭ и фильтрации не безусловно, а в зависимости от параметров сети, через которую получен сетевой пакет.

Возможно применение правил МЭ или фильтрации не безусловно, а только для определённых сетей, определяющихся профилем. Доступно семь возможных сетевых профилей сетей, определяемых по адресам и используемым сетевым адаптерам. В случае, если для сетевого пакета не подходит ни один из активных сетевых профилей ‒ пакет будет считаться принадлежащем к сети, определённой сетевым профилем «По умолчанию». Для редактирования сетевого профиля нужно выбрать его на информационной панели и нажать кнопку «Свойства» на панели «Действия». Появится окно «Свойства сетевого профиля», в котором возможно задать IP-адрес или подсеть, выбрать сетевой интерфейс и ввести название сетевого профиля

### Свойства сетевого профиля

***Пример 1.***

Администратор хочет разрешить использование сети Интернет только из доверенной (корпоративной) сети.

1. Администратор задал подсеть компании и сетевой адаптер для сетевого профиля «Доверенная сеть».

2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сетевой профиль «Доверенная сеть» (см. раздел «Правила МЭ», руководства по администрированию).

3. Администратор отключил параметр «Глобальное правило ‒ пропускать пакеты по умолчанию».

В результате пользователь сможет пользоваться сетью Интернет на ЗАРМ только подключившись к подсети компании через заданный сетевой адаптер.

***Пример 2.***

Администратор хочет разрешить использование сети Интернет только через доверенную (корпоративную) сеть для надёжной антивирусной проверки трафика и принудительной защиты всего трафика от перехвата.

1. Администратор задал подсеть компании для сетевого профиля «Доверенная сеть».

2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сетевой профиль «Доверенная сеть» (см. раздел «Правила МЭ»).

3. Администратор создал разрешающее правило для VPN подключения и выбрал для него сетевой профиль «По умолчанию». Правило VPN подключения разрешит защищённое соединение с доверенной сетью из любых сетей. После установления соединения с доверенной сетью возможно использование сети Интернет при получении через VPN адреса из диапазона доверенной сети.

4. Администратор создал запрещающее правило для всех остальных подключений и выбрал для него сетевой профиль «По умолчанию». При этом необходимо, чтобы запрещающее правило было ниже по приоритету (проверялось после разрешающих правил).

В данной конфигурации для получения доступа к сети Интернет на ЗАРМ из неизвестной сети, пользователю необходимо сначала установить VPN соединение к доверенной сети (которое должно быть сконфигурировано таким образом, чтобы выдать пользователю IP-адрес из доверенной сети, и предоставить маршрутизацию через доверенную сеть в интернет).

## Соединения

В данной категории отображается список текущих сетевых соединений компьютера. В данном списке отображается детальная информация по каждому соединению с привязкой к процессам и ведением статистики.

Существует возможность запретить или разрешить соединение, создать запрещающее или разрешающее правило для соединения (см. раздел «Правила МЭ»), создать исключение для соединения (см. раздел «Исключения»), свернуть или развернуть список соединений, и обновить информационную панель. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

Активированное действие «Автообновление» позволяет автоматически обновлять список соединений раз в 5 секунд.

## Параметры

В данной категории для настройки доступны основные параметры МЭ. Управление параметрами осуществляется на панели «Действия» через нажатие кнопки «Свойства» при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню «свойства» интересующего пункта редактирования параметров безопасности.

Доступны следующие параметры.

Межсетевой экран - Параметр позволяет отключить или включить МЭ.

Доверенные правила МЭ - Данный параметр необходим для поддержания работы по умолчанию следующих протоколов:

 ARP;

 DNS;

 ICMP;

 DHCP;

 DL (трафик управления Dallas Lock). - Данный параметр создан для осуществления бесперебойной работы базовых сетевых функций ОС вне зависимости от заданных пользователем настроек. Наличие доверенных правил МЭ гарантирует возможность удалённого и централизованного управления по протоколам DL в случае ошибочного задания чрезмерных блокирующих правил. Отключение доверенных правил МЭ не рекомендуется.

Отключать GZIP для анализа HTTP трафика - Данный параметр отключает сжатие трафика в независимости от настроек браузеров. Сжатие трафика ускоряет загрузку веб-страниц, но при этом препятствует возможности анализа трафика механизмами фильтрации МЭ (и при анализе сигнатур трафика СОВ). Если деактивировать данную политику – возможна некорректная работа механизма фильтрации (при использовании сайтами сжатия трафика).

Глобальное правило – пропускать пакеты по умолчанию - Параметр задаёт политику по умолчанию, для тех сетевых пакетов, которые не попали ни под одно активное правило МЭ.

Разрешить использовать локальные правила МЭ - Параметр позволяет использовать локальные правила МЭ, которые не подчинены списку правил МЭ на СБ. Если на клиенте ДБ включён данный параметр, то при синхронизации локальные правила не будут удалены.

Режим обучения МЭ - Параметр позволяет включить и настроить режим обучения МЭ. Список разрешённых драйверов протоколов - Параметр позволяет задать разрешённые драйверы протоколов, предоставляющие возможность упрощённой настройки доступа для отдельных драйверов, которая может быть полезной при настройке таких приложений как «банк-клиент», работающих с ОС на низком уровне.

Протоколирование событий изменений конфигурации - Данный параметр позволяет выбрать регистрируемые события об изменении конфигурации МЭ (и СОВ, если модуль СОВ активен).

Периодичность проверки защищённости системы - Данный параметр позволяет настроить периодичность проверки защищённости системы с доступными интервалами от 10 мин до 1 дня. Доступна настройка (включение/выключение; определение временного интервала, если доступно) оповещения об отсутствии обновлений для следующих объектов:

 Обновление ОС;

 Обновление антивируса;

 Обновление сетевых сигнатур.

Также в окне свойств доступна информация о последнем обновлении объектов и времени проведения последней проверки.

Уведомление по событиям отсутствия антивируса и обновлений ОС и DL - Параметр позволяет настраивать (включение/выключение) способы уведомления по событиям отсутствия антивируса и обновлений ОС и DL. Доступны следующие способы уведомления:

 Уведомление в системный tray;

 Уведомление в СБ;

 Уведомление в журнал.

Отключать локальные правила МЭ при автопереключении профиля МЭ - С помощью данного параметра осуществляется настройка отключения локальных правил МЭ при автопереключении профиля МЭ. Значение по умолчанию «Да».

Порты сторонних программ - Параметр позволяет указывать множество портов (перечисление через запятую, указание диапазона портов через тире), которые не будут использоваться для перенаправления службой фильтрации. Перенаправления для настоек фильтрации МЭ создаются для всех портов, которые указаны в категории «МЭ» → «Фильтрация» → «Настройки» → «Список перехватываемых исходящих портов». Перенаправления для сигнатур трафика СОВ создаются только на ОС без механизма WFP (XP, Server 2003, Vista и Server 2008 SP1).

Служба берет диапазон портов от 10002 до 19999 и вычитает из него все порты, указанные в настройке «порты сторонних программ». Если пользователь укажет в ней слишком большое число портов, такое что после вычитания портов их не останется или будет меньше, чем необходимо для создания всех перенаправлений, то служба сообщит об этом пользователю через всплывающее окно, добавит запись в журнал политик и отправит уведомление на СБ.

## Режим обучения МЭ

Для автоматической настройки списка правил МЭ возможно использовать «Режим обучения МЭ». Данный режим позволяет автоматически создавать разрешающие правила МЭ для текущих соединений пользователя.

Чтобы выполнить настройку правил МЭ используя режим обучения МЭ, необходимо:

1. открыть категорию «МЭ» → «Параметры» и щёлкнуть два раза кнопкой мыши на параметр «Режим обучения МЭ». Появится окно подтверждения включения данного режима.

2. установить флаг «Включить режим обучения»;

3. выбрать режим работы МЭ после завершения режима обучения:

 пропускать пакеты ‒ устанавливает значение «Да» для параметра «Глобальное

правило – пропускать пакеты по умолчанию»;

 запрещать пакеты ‒ устанавливает значение «Нет» для параметра «Глобальное правило – пропускать пакеты по умолчанию».

4. установить дату и время окончания режима обучения. Возможно установить период времени: день, неделя и месяц;

5. для гибкой настройки правил возможно указать максимальное количество портов и IP-адресов в одном правиле;

6. осуществить вход на все те веб-ресурсы, с которыми пользователь имеет право работать (но, не открывать ничего лишнего).

Следует помнить, что не для всех веб-ресурсов является достаточным просто их открыть. Некоторые веб-ресурсы загружают не все данные, а только необходимое для работы конкретного веб-ресурса, остальное подгружается динамически, в процессе работы. Поэтому лучше выполнить все основные действия на веб-ресурсе для работы.

На этом этапе создаются автоматические локальные правила МЭ (Далее ‒ АЛП). В списке правил МЭ АЛП выделяются зелёным цветом.

Созданное АЛП может автоматически дополняться, до тех пор, пока не завершится режим обучения или пользователь не произведёт модификацию АЛП в момент работы режима обучения. Под модификацией АЛП понимается любое изменение данного правила.

Если в процессе обучения будет выявлена сетевая атака, приводящая к созданию огромного количества АЛП, то в «Журнал управления политик» регистрируется ошибка и работа режима обучения автоматически завершится. Также будет удалены все созданные АЛП.

Если в процессе обучения произойдёт выключение компьютера, то сохранятся только модифицированные пользователем АЛП.

7. после завершения режима обучения, созданные и модифицированные АЛП добавляются в конец списка правил МЭ (низший приоритет) и становятся локальными правилами.

Правила, созданные с помощью режима обучения МЭ выделяются синим цветом в списке правил МЭ.

Для ручного выключения режима обучения необходимо открыть категорию «МЭ» → «Параметры» и щёлкнуть два раза кнопкой мыши на параметр «Режим обучения МЭ». В появившемся окне снять флаг «Включить режим обучения».

## Правила МЭ

Данная категория настроек является основным инструментом управления функциями межсетевого экрана и позволяет настраивать его работу.

Для перехода к управлению правилами необходимо открыть вкладку «МЭ» и выбрать категорию «Правила МЭ». На информационной панели находится список правил и основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д.

При работе возможно наблюдать открытые порты 1000 и 1004, даже если создано запрещающее правило МЭ, но подключиться к этим портам невозможно, т.к. они используются службой DlIpsService.

На каждом клиенте присутствуют следующие правила МЭ:

 Правило по умолчанию (действие с пакетами, не попавшими ни под одно правило);

 Общие правили МЭ;

 Локальные правила МЭ (автоматические правила, создаваемые в режиме обучения по умолчанию являются локальными, для изменения типа правила нужно выполнить: выбрать редактируемое правило → «Редактировать» на панели «Действия» → вкладка «Общие» → изменить значение параметра «Локальное правило»).

Локальные правила являются индивидуальными для каждого клиента. На панели настройки правил МЭ локальные правила выделяются синим цветом.

Создать новое правило можно как с помощью копирования наиболее подходящего примера, так и создав новое правило.

Для того чтобы активировать готовый шаблон, нужно выбрать его на информационной панели и нажать кнопку «Свойства» на панели «Действия»

Существует возможность копирования имеющегося шаблона, его удаление, просмотра свойств и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

В появившемся меню «Настройки правила МЭ» можно осуществить несколько уровней настроек текущего шаблона.

В разделе «Информация» отображается сводная информация всех параметров правила.

Вносить какие-либо изменения в работу правила на данном этапе нельзя

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

В версии «С» раздел «Информация» дополнен параметром «Мандатный уровень», информирующий о том, для каких мандатных уровней применяется правило

В разделе «Общие» представлены основные настройки правила:

 описание правила;

 действие, которое должно выполняться согласно правилу: запретить/разрешить;

 расписание работы: настройка гибкого расписания;

 запустить приложение: указать путь к приложению, которое должно запуститься при срабатывании правила;

 применение правила только для указанных приложений: необходимо указать путь к приложению;

 параметры: необходимо указать все параметры (ключи), с которыми выполняется

приложение, при указании приложения с неполным перечнем параметров корректное выполнение правила не гарантируется.

Если был задан параметр «Запустить приложение», то при срабатывании правила, приложение запустится от имени ОС и не интерактивно.

Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе «Протоколы» можно задать детальные настройки отображаемой информации по принимаемым/отправляемым пакетам: направление передачи (входящие пакеты, исходящие пакеты, любое направление передачи, входящие соединения, исходящие соединения), вид протокола и его параметры. Возможно выбрать следующие направления передачи:

 входящие пакеты ‒ если правило разрешающее, то разрешаются все входящие пакеты;

 исходящие пакеты ‒ если правило разрешающее, то разрешаются все исходящие пакеты;

 любое направление передачи;

 входящие соединения ‒ если правило разрешающее, то при успешном входящем соединении разрешается обратное исходящее соединение. Если правило запрещающее, то запрещаются все входящие соединения;

 исходящие соединения ‒ если правило разрешающее, то при успешном исходящем соединение, разрешается обратное входящее соединение. Если правило запрещающее, то запрещаются все исходящие соединения.

Для фильтрации протоколов использующие различные и не и зафиксированные порты необходимо настроить правила МЭ таким образом, чтобы соединения (в том числе UDP) разрешались только для определённого списка портов, и все из этих портов включены в список перехватываемых исходящих портов. Таким образом фильтрация протоколов будет осуществляться на всем диапазоне возможных портов сетевого трафика.

Раздел «Пользователи» отображают список пользователей, к которым будет применено правило. Отметив пункт «Автоматический поиск пользователей /групп» при последующем нажатии кнопок «Пользователи» и «Группы» будет показан список всех возможных пользователей для последующего назначения прав. Далее в разделе «Мандатные уровни» каждому пользователю можно присвоить необходимый мандатный уровень.

При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки «Удалить»

Данный параметр доступен только для Dallas Lock 8.0 редакции «С». Реализована возможность назначения мандатных уровней отдельным пользователям или группам пользователям. В разделе «Дополнительно» существует возможность применения текущего правила МЭ только для определённых сетевых адаптеров и (или) сетевых профилей. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку «Добавить». Удаление производится выбором адаптера из списка и нажатием кнопки «Удалить». Для редактирования списка сетевых профилей правила МЭ необходимо отметить сетевые профили.

Задавать очерёдность исполняемых правил можно посредством назначения приоритетов. Правила с назначенным приоритетом выше, чем у других будут проверяться в первую очередь. После срабатывания правила, проверка правил останавливается.

Например, созданы ***два правила***.

***Правило 1*** запрещает отправку/приём почты по протоколам SMTP/POP3/IMAP.

***Правило 2*** разрешает пользоваться почтой по протоколам SMTP/POP3/IMAP для серверов mx.yandex.ru.

Рассмотрим случай, когда правила находятся в указанной последовательности. То есть «Правило 1» находится выше «Правила 2», соответственно приоритет первого правила выше. В данном случае приём/отправка почты по указанным протоколам осуществляться не будет.

В случае если приоритет «Правила 2» будет выше приоритета «Правила 1», то тогда работа по указанным протоколам будет осуществляться только через сервер mx.yandex.ru.

Процесс создания нового правила происходит по тем же настройкам, что и корректировка уже готового шаблона. Для создания нового правила нужно нажать правую клавишу мыши на информационной панели и выбрать «Добавить» в контекстном меню или нажать ту же кнопку на панели действий. Все последующие настройки аналогичны настройкам шаблонов.

Рассмотрим пример создания ***нового правила***.

Например, требуется создание правила для запрета передачи IM-Messaging (чат) трафика по протоколу ICQ.

Во вкладке «Межсетевой экран» выбрать категорию «Правила МЭ» и щёлкнув правой кнопкой мыши на информационном окне в выпадающем меню выбрать «Добавить».

В разделе «Общие» указывается описание правила и устанавливается действие для правила «Запретить».

Далее в разделе «Протоколы» в списке протоколов указывается нужный тип протокола «TCP […]». После нажатия кнопки «Добавить» в диалоговом окне необходимо отметить протокол «TCP […]» (ввиду того, что программа ICQ использует исключительно этот транспортный протокол). Нажать кнопку «ОК». Далее происходит настройка параметров выбранного протокола. Указывается внешний TCP порт «5190, 443», так как ICQ предусматривает работу с серверами по порту 5190 и, в случае безопасного подключения, по порту 443. Для того чтобы правило не распространялось для HTTPS (SSL) трафика, требуются уточнения. В разделе «Протоколы» дополнительно добавляется протокол IPv4 с указанием «Внешний IPv4» и соответствующий адрес (для того, чтобы получить IP-адрес DNS-имени login.icq.com можно через меню «Пуск» → «Выполнить» → «nslookup.exe.»).

Конкретизированное правило будет работать только при точном совпадении указанных настроек. Правило, конкретизированное для протокола ICQ, сервера login.icq.com и клиента Miranda – не будет работать при любом несовпадении. Например, в случае, если используется официальный клиент ICQ, либо какой-то нестандартный сервер или порт.

Конкретизированные правила удобны возможностью запретить всю работу по указанному протоколу, разрешая только определённый набор функций. Например, разрешить только работу с официальным сервером ICQ, только определённому пользователю и только с использованием определённого клиента. При создании такого разрешающего правила с детальными параметрами необходимо следующим правилом или правилом по умолчанию заблокировать трафик с отличными от указанных параметров.

IP-адреса, на которые ссылаются DNS-имена, могут изменяться. Также есть ситуации, когда для одного DNS-имени указываются несколько IP-адресов – в этом случае в графе «Внешний IPv4» необходимо указать диапазон адресов, или их перечисление через запятую, например, «217.69.139.70, 94.100.180.70» для DNS-имени www.mail.ru (на момент написания данного занятия).

Примечание. В случае одновременного задания нескольких параметров для одного протокола, например, одновременного задания пар «Локальный IPv4» и “Внешний IPv4” – для срабатывания правила должны выполниться оба условия. Это актуально и при указании пар «Локальный TCP порт» и «Внешний TCP порт» - при указанном локальном порте 1025 и удалённом 80 - правило работает для HTTP(80/TCP) трафика ТОЛЬКО в случае если локальный порт равен 1025.

«Логическое И» действует между параметрами одного протокола, например, в случае протокола IPv4 логическое «И» действует с «Локальным» и «Внешним» адресом, в случае указания портов (TCP или UDP) - точное соответствие локальных и внешних портов (TCP и отдельно между собой UDP соответственно) и т. д.

## Профили МЭ

Профиль МЭ представляет собой совокупность состояний правил МЭ (активировано/деактивировано) и значение для правила по умолчанию.

В профиль правил МЭ входят правила:

 правило по умолчанию;

 общие правила МЭ.

Для перехода к управлению правилами необходимо открыть вкладку «МЭ» и выбрать категорию «Профили МЭ».

На информационной панели находится список профилей, каждый из которых представляет из себя таблицу с полями:

 профиль («№\*Приоритет профиля\* \*Имя профиля\*» - для профилей с условием включения», «\*Имя профиля\*» - для ручных профилей);

 список условий включения профиля.

Для каждого профиля список правил МЭ одинаковый, но может быть индивидуально настроен. Чтобы посмотреть список правил МЭ с их настройками для конкретного профиля, нужно нажать на символ «+», находящийся слева от названия этого профиля. Список представляет из себя таблицу с полями:

 Статус правила МЭ (активно/деактивировано), управление которым осуществляется путём переключения чекбокса, либо кнопками «Активировать» / «Деактивировать» на панели «Действия»;

 № правила МЭ;

 Основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д.

Изменение параметров правил МЭ в режиме редактирования профилей МЭ невозможно. При выборе правила МЭ и нажатии кнопки «Свойства» на панели «Действия», доступна только информация о настроенных для правила МЭ параметрах.

Для выбора условий включения профиля, необходимо выбрать его в таблице, нажать кнопку «Свойства» на панели «Действия» и перейти на вкладку «Общие»

Доступны следующие условия включения профиля:

 Требуется обновление ОС;

 Отсутствует антивирус;

 Устарели сигнатуры антивируса;

 Устарели сигнатура СОВ;

 Нарушение целостности.

При выборе нескольких условий включения профиля действует правило «ИЛИ», т. е. при срабатывании любого из выбранных условий – активируется профиль.

Каждое условие включения может принадлежать нескольким профилям, но при одинаковых условиях у разных профилей, должен сработать профиль с наивысшим приоритетом.

Если для профиля не указаны условия включения, то данный профиль считается ручным и переключается только по команде администратора кнопкой «Переключить профиль» на панели «Действия». После переключения профиля необходимо нажать кнопку «Обновить» на панели «Действия».

Если ручному профилю задано хотя бы одно условие включения, ему присваивается самый низкий приоритет.

Для изменения приоритета профиля необходимо выбрать этот профиль и нажать кнопку «Увеличить приоритет» / «Уменьшить приоритет» на панели действия.

На панели «Действия» расположен параметр «Автовыбор профилей», предназначенный для автоматического включения профилей в соответствии приоритетам и условиям включения. По умолчанию параметр отключён.

При отключённом параметре «Автовыбор профилей» доступны любые изменения списков профилей МЭ и правил МЭ (кроме редактирования правила в категории «Профиля МЭ»), в том числе их статус.

При автоматическом переключении профиля МЭ на клиенте появляется всплывающее уведомление на панели задач.

При включённом параметре «СОВ» → «Параметры СОВ» → «Глобальные параметры» → «Маскирование датчика СОВ» → «Вкл.», всплывающее уведомление об автопереключении профиля на клиенте не появляется.

После нейтрализации условий включения профиля выполняется автоматическое переключение на профиль «По умолчанию».

При попытке смены профиля после его автоматического переключения появляется предупреждающее диалоговое окно о том, что для переключения необходимо отключить параметр «Автовыбор профилей» (рис. 210).

Название текущего профиля МЭ отображается на нижней части панели в категориях «Профили МЭ» и «Правила МЭ».

## Фильтрация

Посредством фильтрации возможно контролировать сетевой трафик по его содержимому (анализируется присутствие известных протоколов, рекламы, медиа-контента и мобильный код) во всем фильтруемом трафике.

При установленном антивирусе для работы механизма фильтрации необходимо добавить файл «C:\DLLOCK80\DlIpsService.exe» в список исключений антивируса.

## Настройки фильтрации

В данной категории доступны настройки фильтрации МЭ. Управление параметрами осуществляется на панели «Действия» через нажатие кнопки «Свойства» при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню «Свойства» интересующего пункта редактирования параметров безопасности.

Список перехватываемых исходящих портов Параметр позволяет задать список перехватываемых исходящих портов для фильтрации трафика. По умолчанию имеет значение: 80, 8080, 3128, 443. Анализ трафика ведётся только для соединений, проходящих по указанным портам.

Смена настроек, связанных с формированием списка перенаправлений (Сетевые профили МЭ, Параметры МЭ/СОВ, Фильтрация МЭ, Сигнатуры трафика СОВ), приводит к освобождению всех ресурсов занятых службой фильтрации, повторному созданию потоков и привязке портов для нового списка.

При возникновении ошибок в процессе формирования перенаправлений служба показывает всплывающее окно и добавляет запись в журнал политик.

Примечание. В ОС семейства Windows (начиная с Windows Server 2008 R2 и Windows 7) включается механизм WFP. В этом случае служба не создает список перенаправлений для сигнатур трафика, только для списка портов в настройках фильтрации МЭ.

Примечание. Список перехватываемых портов не должен превышать 1000. Если используется старая версия СБ с новой версией СЗИ, то ограничения на ввод портов на СБ не будет, и служба пользователей попытается построить все перенаправления по указанному списку.

## Режим работы

Данный параметр позволяет выбрать режим работы фильтрации относительно добавленных исключений. Доступно два режима:

 Фильтровать все, кроме исключений;

 Фильтрация активна только для хостов-исключений. Фильтрация будет применяться только к добавленным исключениям.

## Анализ SSL трафика

Включение данного параметра позволяет осуществлять фильтрацию в том числе для HTTPS (SSL) соединений. При включении данного параметра осуществляется внедрение в HTTPS трафик и анализ трафика прозрачно для пользователя путём подмены SSL сертификата.

При включении параметра «Анализ SSL трафика» возможно проявление конфликтов со сторонним ПО, детально проверяющим принадлежность своего SSL сертификата, например, возможна блокировка скачивания обновлений ОС. Для решения подобной проблемы необходимо добавить URL серверов обновлений ОС в список исключений (хосты из списка исключений не подвергаются подмене сертификата, при установленном режиме работы «Фильтровать все, кроме исключений»).

При включении параметра «Анализ SSL трафика» корректная работа гарантируется только через «Chrome». Работа с другими браузерами может быть ограничена.

## Максимальный размер http-заголовка

Данный параметр позволят реализовывать фильтрацию с целью выявления аномальности HTTP-заголовка по размеру. Доступны значения максимального размера HTTP-заголовка от 2048 символов до 16 384 символов. По умолчанию параметру присвоено значение 2048.

Включить уведомление в tray при блокировке соединения Параметр предназначен управления всплывающими уведомлениями при блокировке соединения. По умолчанию уведомления отключены.

## Фильтры

На информационной панели расположены фильтры, анализирующие присутствие известных сетевых протоколов и мобильного кода в фильтрующемся трафике.

Доступны следующие действия фильтрации для каждого отдельного фильтра:

 блокировать;

 вырезать;

 журналировать.

Для активации определённого фильтра нужно два раза щёлкнуть левой кнопкой мыши по фильтру на информационной панели, после чего появится окно «Свойства фильтра». Далее необходимо выбрать действие фильтра для всех профилей или действия для каждого профиля индивидуально, после чего нажать «ОК».

**Пример.**

Рассмотрим случай, когда требуется доверенный доступ к сайту «mail.ru», а для всех остальных необходимо вырезать ресурсы содержащие мобильный код, чтобы исключить известные и неизвестные уязвимости браузеров.

Открыв категорию «Фильтрация» → «Исключения» необходимо нажать правой кнопкой на информационной панели и в контекстном меню выбрать «Добавить». На информационной панели появится новое правило с пустым полем «URL», где нужно ввести IP-адреса или DNS-имя соответствующего хоста или сайта. В данном случае введя «mail.ru», поле «Адрес» автоматически заполнится всеми IP-адресами, принадлежащими DNS-имени «mail.ru» (и, при необходимости, другим доверенным адресами).

Далее, на вкладке «Фильтрация» → «Настройки» необходимо для параметра «Режим работы» выбрать режим «Фильтровать все, кроме исключений».

Для фильтрации мобильного кода для всех остальных сайтов необходимо на вкладке «Фильтрация» → «Фильтры» включить фильтры мобильного кода (ActiveX, Flash, JScript, VBScript) с действием фильтра «Вырезать».

При выполнении описанных настроек пользователю будет доступен хост «mail.ru» без ограничений, но для остального трафика фильтрация вырежет заданный мобильный код, значительно уменьшая возможность эксплуатирования уязвимостей браузеров.

Примечание. После загрузки страницы веб-сервиса, в кэш браузера помещаются загруженные объекты (html-страница, flash-файл и т. п.). При последующих загрузках данной страницы веб-сервиса, flash-файл больше не будет передаваться по сети, как и html-страница. Поэтому для корректной работы фильтров необходимо очистить кэш браузера.

## Веб-контроль

Принцип управления веб-контроля аналогичен принципу работы правил МЭ. Необходимо создать набор правил, которые могут быть запрещающими, разрешающими или информирующими. В правилах веб-контроля указывается на какие URL-адреса они действуют, к какому содержимому и для каких пользователей применяются. Правила проверяются в заданном порядке, после срабатывания правила, проверка прекращается.

Если ни одно из существующих правил не сработало, применяется правило по умолчанию.

После обработки правил веб-контроля возможны следующие события:

 доступ к запрошенной информации с сервера;

 уведомление пользователя о блокировке веб-ресурса;

 предупреждение о нежелательном доступе к запрошенному веб-ресурсу.

Для перехода к управлению правилами веб-контроля необходимо открыть подкатегорию «МЭ» → «Фильтрация» → «Веб-контроль».

На информационной панели находится список правил веб-контроля и основные данные по ресурсам и пользователям, для которых они назначены: расписание, приложения, сайты, типы данных, ключевые слова и т. д. (рис. 214).

Существует возможность создания правила и копирования уже имеющегося, удаления, просмотра свойств и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

При создании правила веб-контроля появится окно «Создание правила веб-контроля» в котором доступно 7 разделов.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

В версии «С» раздел «Информация» дополнен параметром «Мандатный уровень», информирующий о том, для каких мандатных уровней применяется правило

В разделе «Общие» представлены основные настройки правила веб-контроля. Если был задан параметр «Запустить приложение», то при срабатывании правила, приложение запустится от имени ОС и не интерактивно. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе «URL» можно задать URL-адреса веб-ресурсов, к которым будет применяться данное правило. Возможно указать маску, когда требуется применить правило для множества схожих URL-адресов веб-ресурсов, например, «mail.ru\*». Символ «\*» заменяет любую последовательность символов. Список URL-адресов возможно загрузить из файла, если предварительно он был составлен и сохранен.

Раздел «Контент» позволяет настроить контроль доступа пользователей к веб-ресурсам по типам данных и ключевым словам, предотвращая показ нежелательного содержимого.

При фильтрации по типу данных (видео, звуковые файлы и т. д.) правило применяется ко всем веб-ресурсам, которые содержат любой из выбранных типов.

При фильтрации по ключевым словам, правило применяется ко всем веб-ресурсам, которые содержат любое из введённых ключевых слов. Например, при наличии ключевых слов «открытые вакансии» и «калейдоскоп» для блокирования будет достаточно нахождения слова «калейдоскоп» или полного сочетания «открытые вакансии». Список ключевых слов возможно загрузить из файла, если предварительно он был составлен и сохранен. Возможна фильтрация ключевых слов без учёта регистра.

Раздел «Реклама» позволяет настроить блокировку рекламных изображений, основываясь на их размере, заданном в HTML-теге «A» (рис. 220). Если размер блокируемого объекта соответствует одному из заданных в списке, он заменяется текстом «[AD]» или отсутствующим изображением такого же размера с текстом «[AD]». Список возможно загрузить из файла, если предварительно он был составлен и сохранен.

Нажав на кнопку «По умолчанию» в список добавится несколько стандартных размеров рекламы. Для включения механизма удаления рекламы необходимо поставить флаг «Удаление включено».

Данная возможность позволяет вырезать картинки по указанным в списке размерам. Удаление картинок и рекламы в HTML-коде страниц может не осуществляться, если:

1. размеры изображения не указаны в атрибутах тега явно;

2. часть HTML-страницы, в которой находятся вырезаемые картинки, не передаётся в явном виде с сервера, а строится в браузере клиента во время исполнения скриптов.

Раздел «Пользователи» отображают список пользователей, к которым будет применено правило. Отметив пункт «Автоматический поиск пользователей /групп» при последующем нажатии кнопок «Пользователи» и «Группы» будет показан список всех возможных пользователей для последующего назначения прав. Далее в разделе «Мандатные уровни» каждому пользователю можно присвоить необходимый мандатный уровень. При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки «Удалить»

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность назначения мандатных уровней отдельным пользователям или группам пользователям.

В разделе «Дополнительно» существует возможность применения текущего правила МЭ только для определённых сетевых адаптеров и (или) сетевых профилей. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку «Добавить». Удаление производится выбором адаптера из списка и нажатием кнопки «Удалить». Для редактирования списка сетевых профилей правила МЭ необходимо отметить сетевые профили.

## Исключения

Исключения необходимы для работы с указанными хостами вне зависимости от настроенной фильтрации, при режиме работы «Фильтровать все, кроме исключений». При режиме работы «Фильтрация активна только для хостов исключений», фильтрация будет применяться только к указанным в исключениях хостам.

Для создания правила исключения, необходимо выбрать действие «Добавить», после чего на информационной панели появится новое правило с пустым полем, где необходимо ввести IP-адрес или DNS-имя. Для поддержания актуальных адресов хостов исключений, адреса исключений периодически обновляются.

Для того чтобы удалить исключения, нужно, выделив правило, щёлкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Удалить».

## Выключение фильтрации

Для временного прекращения фильтрации МЭ необходимо нажать кнопку «Выключить фильтрацию» на вкладке «Фильтрация» и в появившемся окне подтвердить действие

## Статистика МЭ

В категории «Статистика МЭ» содержится информация о принятом и отправленном трафике за указанный период. Полученные данные можно обновить и сбросить посредством нажатия соответствующих кнопок на панели «Действия». Справа от панели находится диаграмма, отображающая статистику всего входящего и исходящего трафика с указанием количества информации и времени, когда она была получена.

### Весь трафик

Параметр «Весь трафик» отображает объем информации, полученный за сутки, неделю, месяц или весь период работы Dallas Lock. При ознакомлении с данными статистики нужно принимать во внимание то, что учёт трафика производится с начала суток (00 часов 00 минут), с начала недели (понедельник), с первого дня месяца (1-е число отчётного месяца). Для отображения информации нужно нажать кнопку «Весь трафик» на панели «Параметры статистики». Панель действий включает в себя опции обновления и сброса текущей информации.

### Статистика по процессам

В параметре «Статистика по процессам» отображается трафик, использованный рабочими процессами, с указанием отчётного периода.

### Статистика по пользователям

«Статистика по пользователям» показывает, сколько было отправлено/принято трафика во время работы каждого системного процесса за отчётный период.

**Отключение МЭ** Для временного прекращения работы МЭ необходимо нажать кнопку «Отключить МЭ» и в появившемся окне подтвердить действие

## Журналы

МЭ В Dallas Lock 8.0 реализована функция сбора и отображения информации о сетевых пакетах и установленных соединениях ПЭВМ (или компьютера).

Для того чтобы ознакомиться с данной информацией, нужно открыть общую вкладку «Журналы» и выбрать «Журнал пакетов» или «Журнал соединений». По умолчанию журналы отключены, и сбор информации не ведётся. На панели «Действия» расположено три кнопки. При нажатии кнопки «Обновить» отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображённую в журналах МЭ, нужно нажать кнопку «Архивировать». После этого в папке программы появится файл с архивом данных. Для открытия такого файла нужно использовать категорию «Журнал из файла» и в её окне на панели действий нажать кнопку «Открыть журнал», а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Кнопка «Экспорт» отвечает за сбор и конвертирование информации журналов межсетевого экрана в файлы c расширением txt (с табуляцией или без), CVS, HTML или XML. Для осуществления данной функции нужно нажать кнопку «Экспорт», указать имя файла и выбрать место для его хранения.

### Служебный журнал

Служебный журнал нужен для создания файла со списком заблокированных пакетов в формате pcapng, в случае возможных проблем детектирования пакетов и может понадобиться при обращении в службу технической поддержки.

Чтобы включить служебный журнал МЭ необходимо нажать правой кнопкой мыши на параметре «Служебный журнал МЭ» и в появившемся окне выбрать пункт «Вкл.» и нажать кнопку «Ок». Журнал располагается в папке DL, например, «C:\DLLOCK80\Firewall\Logs» и его имя может зависеть от названия используемого сетевого адаптера. Например, имя файла журнала может быть таким «C:\DLLOCK80\Firewall\Logs\VMware\_Accelerated\_AMD\_PCNet\_Adapter 2015- 04-30.pcapng».

### Журнал пакетов

Журнал пакетов содержит в себе сведения об отправленных и принятых сетевых пакетах, прошедших через межсетевой экран. Для настройки отображения фиксируемой информации нужно нажать правой кнопкой мыши на строке параметра «Журнал пакетов МЭ» и в контекстном меню выбрать пункт «Свойства»

Данные настройки идентичны настройкам для правил межсетевого экрана. Возможно включить запись TCP-пакетов, не соответствующих таблице состояния (out of state TCP-пакеты).

Параметр «Мандатный уровень» доступен только для Dallas Lock 8.0 редакции «С».

После настройки параметров в журнале пакетов во вкладке «Журналы» начнётся сбор и отображение информации по указанным при настройке сетевым пакетам.

### Журнал соединений

Журнал соединений отображает информацию об осуществлённых в процессе работы МЭ сетевых соединениях. Для осуществления дальнейших настроек нужно щёлкнуть правой кнопкой мыши на строке параметра «Журнал соединений МЭ» и в контекстном меню выбрать пункт «Свойства».

Настройки отображения информации, собранной журналом соединений МЭ идентичны настройкам правил работы межсетевого экрана (см. раздел «Правила МЭ»). Исключение составляет отсутствие пункта «Дополнительно» и описание правила, оно присваивается по умолчанию.

В ходе данной практической работы выполняется настройка системы сетевой защиты. Выполнение работ при установке и настройке системы защиты информации для действующей информационной системы в общем случае разделяется на следующие этапы:

1. Подготовка средств вычислительной технике к настройке;
2. Установка и настройка общесистемного программного обеспечения;
3. Установка и настройка прикладного программного обеспечения;
4. Установка и настройка сетевого оборудования;
5. Установка и настройка периферийного оборудования;
6. Установка и настройка средств антивирусной защиты;
7. Установка и настройка системы защиты информации от несанкционированного доступа.

В этой работе подробно рассмотрен последний 7-ой этап работ. В этом случае этап подготовки к установке и настройке МЭ включает в себя:

1. Проверку наличия дистрибутива МЭ последней версии.
2. Проверку наличия лицензионного ключа.
3. Проверку наличия матрицы доступа.

***Постановка задачи.*** Выполнить все шаги работы, необходимые для осуществления настройки МЭ. Результаты зафиксировать в отчете.

***Последовательность действий.***

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать свой сетевой профиль с возможностью использования сети Интернет только из доверенной (корпоративной) сети.

Шаг 4. Выполнить настройку правил МЭ используя режим обучения МЭ.

Шаг 5. Посредством настройки механизма фильтрации осуществить контроль сетевого трафика по его содержимому.

Шаг 6. Разрешить определенным пользователям пользоваться почтой по протоколам SMTP/POP3/IMAP для серверов mx.yandex.ru.

Шаг 7. Настроить анализ SSL трафика.

Шаг 8. Осуществить сбор и отображение информации о сетевых пакетах и установленных соединениях ПЭВМ;

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение А представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [1, 5].

**Контрольные вопросы**

1. Перечислите основные руководящие документы ФСТЭК по классификации АС, средств вычислительной техники (СВТ), межсетевых экранов (МЭ) и программного обеспечения (ПО)?
2. Каким приказом определены требования Межсетевым экранам
3. Перечислите типы МЭ?
4. Охарактеризуйте МЭ типа «А»:
5. Охарактеризуйте МЭ типа «Г»:
6. Каким угрозам безопасности информации должен противодействовать МЭ типа «А» согласно «Профилям МЭ»?
7. Каким угрозам безопасности информации должен противодействовать МЭ типа «Б» согласно «Профилям МЭ»?
8. Что следует учитывать при написание правил МЭ
9. Опишите назначение и возможности механизма защиты МЭ Dallas Lock?
10. Что включает в себя подсистема регистрации и учета МЭ Dallas Lock?

**Дополнительные материалы, информационные источники**

1. Сайт компании ”Конфидент” https://dallaslock.ru/

2. Конфидент Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации // Dallas Lock [Электронный ресурс]. 19.12.2019. – URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/%D0%A1%20%D0%98%D0%9A5%202017/RU.48957919.501410-02%2092%20%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%BF%D0%BE%20%D1%8D%D0%BA%D1%81%D0%BF%D0%BB%D1%83%D0%B0%D1%82%D0%B0%D1%86%D0%B8%D0%B8.pdf (дата обращения: 19.12.2019).

3. Макаренко С.И., Ковальский А.А., Краснов С.А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учеб. пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. - СПб.: Наукоемкие технологии, 2020. - 357 с.

4. Краснов, Сергей Александрович. Настройка средств защиты компьютерной информации [Текст]: учеб.­метод. пособие / С. А. Краснов, А. К. Племянников, Д. А. Решетняк, 2020. ­71 с.

**Методика текущего контроля**

Текущий контроль включает в себя контроль посещаемости (не менее 80 % занятий), сдача 4 коллоквиумов по тематике дисциплины (проверка знаний и умений по каждой теме) по результатам которого студент получает допуск на экзамен. На коллоквиумах проводится защиты работ, которые проводились на практических занятиях. В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях. самостоятельной работы студентов

Изучение дисциплины сопровождается самостоятельной работой студентов (СРС) с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет. Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины. Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Текущая СРС по ПЗ № 5 состоит из:

1. Работа с лекционным материалом, с учебной литературой – 1,5 ак.ч;

2. Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) 1 ак.ч.

3. Самостоятельное изучение разделов дисциплины - 1 ак.ч.

4. Подготовка к лабораторным работам, к практическим и семинарским занятиям - 2 ак.ч

5. Подготовка к контрольным работам, коллоквиумам - 1 ак.ч.

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методике, описанной выше.

Доцент кафедры ИБ

Краснов С.А.