УДК 004.056.(52)

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ С ЗАКРЫТОЙ ПОДСЕТЬЮ

Лебедев Р. В.
Научный руководитель – Потуремский И. В.
Сибирский федеральный университет

Основной проблемой обеспечения безопасности информационных систем предприятий является снижение эффективности применяемых мер защиты. В силу различных факторов, таких как размеры вычислительной сети, ее структурная сложность, множество сетевых сервисов, а также наличие распределенных вычислительных систем и изолированных подсетей, возникают трудности в организации системы защиты, поддержании ее работоспособности и процессов управления, усложняются задачи обработки данных, снижается оперативность реагирования и пресечения нарушений.

Принципиально важной становится задача приведения элементов защищаемой информационной системы к некоторому структурному подобию, что позволит организовывать их защиту на основе единых правил, технических и программных средств, тем самым упростит общую модель защиты информационной системы.

В данной статье рассмотрен пример приведения к общей структуре закрытого сегмента сети. Защита информации как внутри сегмента, так и на его границе (защита периметра) организуется на основе требований федеральных нормативных актов в сфере защиты информации, что дает основание считать данный сегмент защищенным по умолчанию. Однако, как элемент информационной системы, такая подсеть, как правило, не будет укладываться в рамки разрабатываемой модели защиты, а значит, должна быть рассмотрена как потенциальная угроза безопасности. Задачу ликвидации этой угрозы усложняют ограничения, налагаемые на технические и программные средства, используемые внутри закрытой подсети, что, в принципе, превращает эту подсеть в некоторую «вещь в себе». Таким образом, организовывать защиту такой подсети можно только на ее последней миле.

Как правило, подобные сети изолированы от общей вычислительной сети. Если же необходимость связи существует, то для решения вполне конкретных задач, что в свою очередь может быть использовано при унификации подсети и ее последующей защиты в рамках общей модели защиты информационной системы. В данном примере такой задачей является обмен с внешней сетью электронной почтой.

С целью снижения числа «степеней свободы» для соединений между открытым и закрытым сегментами вычислительной сети могут быть применены следующие меры по ограничению проходящего между сетями трафика:

1) Ведение списка разрешенных соединений – список пар узлов подсетей, между которыми разрешено устанавливать соединение; соединения между любыми другими парами запрещаются.

2) Ограничение соединений по протоколам, как на нижних, так и на верхних уровнях модели OSI: подобные ограничения позволят исключить все сеансы связи за исключением сеансов, предназначенных для передачи/получения электронной почты (прикладной протокол SMTP (англ. Simple Mail Transfer Protocol – простой протокол передачи почты), порт TCP-соединения 25).

3) Ограничение соединений на уровне приложений. Такие ограничения не достижимы возможностями сетевых устройств защиты, но под силу устройствам защиты рабочих станций (и, как следствие, средствам мониторинга и контроля конечных узлов

сети); возможность запрета/разрешения соединений конкретным приложениям может рассматриваться как дополнительный неявный эшелон защиты подсетей.

Также стоит отметить необходимость ведения базы передаваемой электронной почты в обоих направлениях. Почта, отправляемая из закрытой подсети должна попадать в открытую сеть только после соответствующей проверки ее содержимого.

Исходя из сформулированных выше принципов, защищенный информационный обмен между закрытой подсетью и основной вычислительной сетью предприятия можно организовать, сведя всё множество возможных соединений к одному – соединению между почтовыми серверами одной и другой подсетей.

В качестве возможного решения по защите периметра закрытого сегмента от внешних угроз была построена следующая модель информационных потоков между открытым и закрытым сегментами сети. Она представлена на рисунке 1.

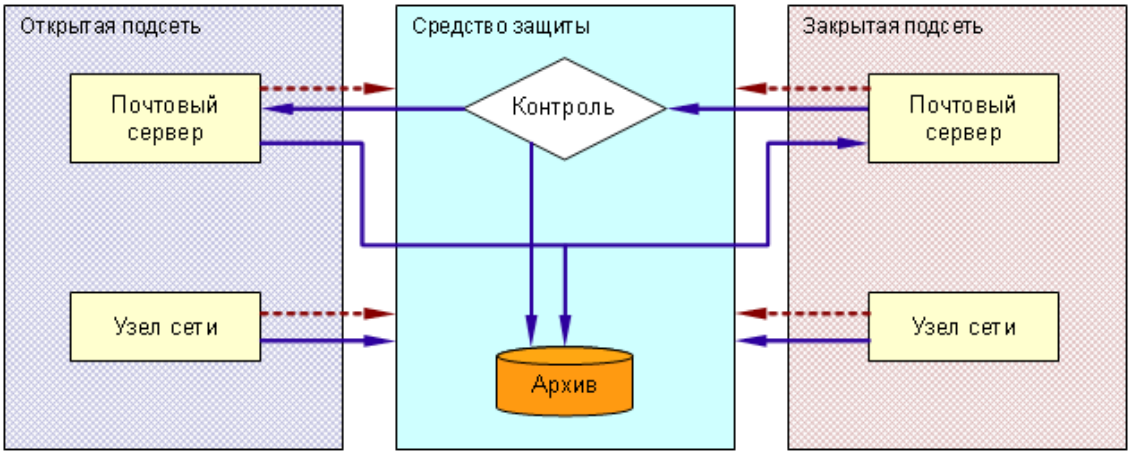

Рисунок 1 – Модель информационных потоков между открытым и закрытым сегментами сети предприятия

Как показано на рисунке, модель информационных потоков предусматривает передачу из одной подсети в другую только почтового трафика, при том, только между двумя почтовыми серверами. Прочий сетевой трафик, включая почтовый, но исходящий от других узлов сети, блокируется средством защиты периметра. Прямого информационного потока из закрытой подсети в открытую *не существует*, канал данных может быть образован только транзитом через узел «Контроль».

В качестве варианта решения целесообразно применить схему организации защиты периметра закрытой подсети, состоящей из последовательно соединенных транзитного почтового сервера и сертифицированного межсетевого экрана. Схема приведена на рисунке 2.

Рисунок 2 – Схема защиты периметра закрытой подсети

Посредством межсетевого экрана производится фильтрация трафика между подсетями. Фиктивный почтовый сервер выполняет функции управления почтовым трафиком: архивирование, задержка исходящего трафика для проверки. Также транзитный сервер является естественным фильтром прикладного уровня модели OSI, обрабатывая трафик только протокола SMTP.

На рисунке 3 изображена схема информационных потоков между открытым и закрытым сегментами, полученная за счет использования в качестве меры защиты предложенного выше варианта решения.

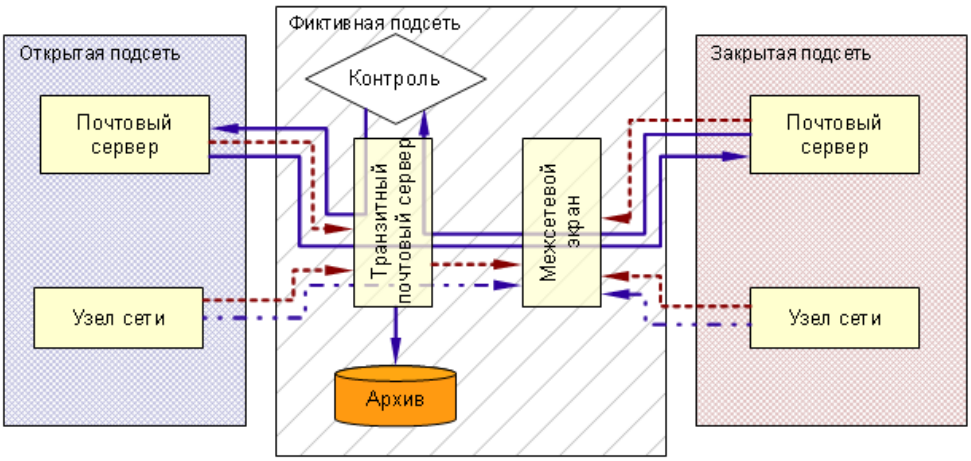

Рисунок 3 – Модель решения для организации взаимодействия открытой и закрытой сетей

Можно отметить некоторые особенности предложенного решения:

1) Данное решение удовлетворяет всем сформулированным выше требованиям:

- осуществляется фильтрация трафика как на нижних уровнях модели OSI посредством межсетевого экранирования, так и на верхнем (прикладном) за счет применения транзитного почтового сервера;
- определено только одно допустимое соединение между узлами подсетей;
- отсутствует прямой информационный поток из закрытой подсети;
- поскольку транзитный почтовый сервер выполняет только одну функцию (перенаправление почтового трафика между почтовыми серверами открытой и закрытой подсетей), при использовании средств контроля рабочих станций задачи их настройки значительно упрощаются;
- за счет настроек транзитного почтового сервера появляется возможность дублирования трафика в архив корреспонденции и перенаправления его в подразделение контроля.

2) Граница между подсетями преобразована в отдельную фиктивную подсеть:

- закрытый сегмент сети теперь полностью изолирован от открытого;
- расширяется список возможностей по усилению системы защиты периметра закрытого сегмента;

3) Ввиду естественной фильтрации сетевого трафика транзитным почтовым сервером сокращается нагрузка на межсетевой экран; фактически ему приходится фильтровать трафик, приходящий только от одного узла, что повышает отказоустойчивость всего эшелона защиты.

Использование транзитного почтового сервера позволяет ассоциировать закрытую подсеть с обычной рабочей станцией сети, тем самым, интегрируя ее в структуру информационной системы, и применять меры по защите в рамках общей модели защиты.