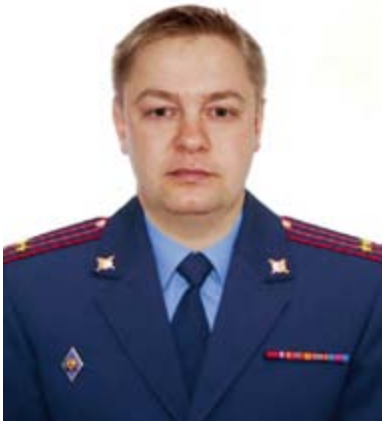
Организация доступа к ресурсам международной сети Интернет из защищённых сегментов ЛВС ОВД

Пикалов
Олег Геннадьевич,
заместитель начальника ООТЗИ УЗИ ДИТСиЗИ МВД России, к.т.н., подполковник внутренней службы



Паньчев
Сергей Владимирович,
старший специалист ООТЗИ УЗИ ДИТСиЗИ МВД России, к.т.н., подполковник внутренней службы

В условиях бурного развития систем автоматизации деятельности сотрудников ОВД использование международной сети Интернет для выполнения служебных обязанностей является насущной необходимостью. Вместе с тем необходимо отметить, что обязанности сотрудников также подразумевают необходимость обработки на своих рабочих местах информации ограниченного доступа, законодательно подлежащей защите. Также существует возможность получения из сети Интернет информации, не относящейся к деятельности сотрудников ОВД, в т.ч. и вредоносных программ.

Таким образом, актуальными являются следующие задачи:

- предоставление сотрудникам ОВД доступа к сети Интернет без возможности передачи в сеть Интернет информации с АРМ, обрабатывающего информацию ограниченного доступа;
- обеспечение хранения информации, загруженной пользователем из сети Интернет, без возможности неконтролируемого сохранения контента на АРМ, обрабатывающем информацию ограниченного доступа;
- обеспечение межсетевого экранирования трафика на границе с сетью Интернет;
- обеспечение контентной фильтрации данных, загружаемых из сети Интернет;
- интеграция с существующей в ЛВС Заказчика системой разграничения доступа;
- обеспечение антивирусной защиты.

Представляется наиболее эффективным решение вышеперечисленных задач с помощью специализированного программно-аппаратного комплекса защищенного доступа в международную сеть Интернет (ПАК «Интернет»).

В состав ПАК «Интернет» (рис. 1) входят следующие основные компоненты:

- прокси-сервер;
- терминальный сервер;
- контроллер домена внешнего леса;
- сервер межсетевого экранирования.

Прокси-сервер предназначен для выполнения функций контентной фильтрации, антивирусной защиты и кэширования.

На прокси-сервере устанавливается следующее программное обеспечение:

- ОС Microsoft Windows Server 2003 Enterprise Edition x86;
- ПО Microsoft ISA Server 2006.

Основным функциональным элементом сервера является интернет-шлюз Microsoft ISA Server 2006.

- Microsoft Internet Security and Acceleration (ISA) Server 2006 является комплексным интернет-шлюзом безопасности и содержит следующие встроенные модули:
- брандмауэр сетевого уровня, обеспечивающий обнаружение и защиту от атак на сетевом уровне, включая защиту от отключения или перехвата контроля над ПО ISA Server 2006;
- шлюз безопасности для проверки на прикладном уровне;
- прямой и обратный веб-прокси и кэш-сервер;
- сервер удаленного доступа к VPN;
- шлюз Site to site VPN.

Microsoft ISA Server 2006 служит для распределения, учёта и контроля доступа пользователей в сеть Интернет. Управление ПО Microsoft ISA Server 2006 осуществляется через графический интерфейс.

Microsoft ISA Server 2006 устанавливается на границе между локальной сетью и межсетевым экраном, подключенным к сети Интернет, и обеспечивает взаимодействие пользователей с глобальной сетью.

Терминальный сервер обеспечивает выполнение всех операций пользователя, связанных с обработкой данных из сети Интернет, и хранение пользовательских файлов.

На терминальном сервере устанавливается следующее программное обеспечение:

- ОС Microsoft Windows Server 2008 Enterprise Edition R2;
- Службы удаленных рабочих столов из состава дистрибутива ОС семейства Microsoft Windows Server.

Контроллер домена внешнего леса предназначен для интеграции с существующей системой разграничения до-

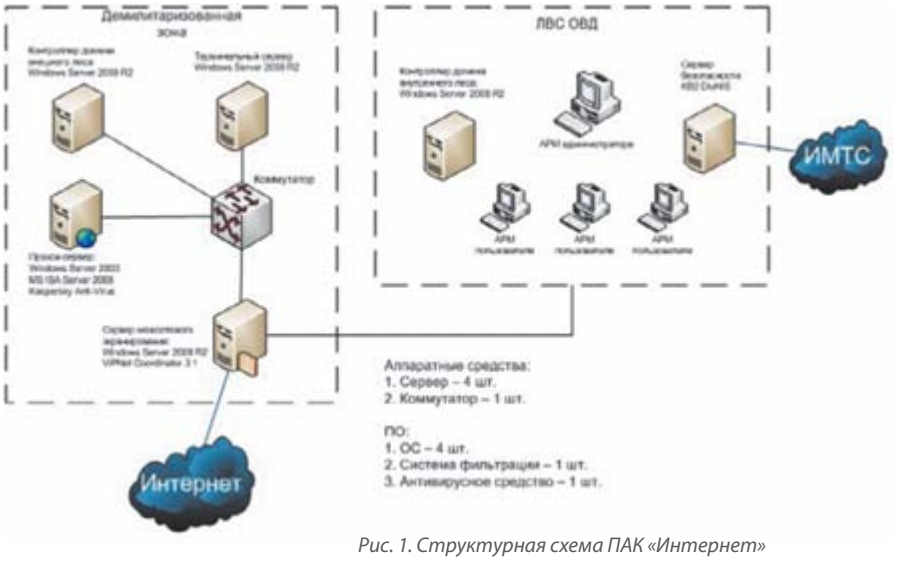


Рис. 1. Структурная схема ПАК «Интернет»

ступа и обеспечения аутентификации пользователей с использованием учетной записи домена внутреннего леса.

На контроллере домена внешнего леса устанавливается следующее программное обеспечение:

- ОС Microsoft Windows Server 2008 Enterprise Edition R2;
- доменные службы Active Directory из состава дистрибутива ОС семейства Microsoft Windows Server;
- DNS-сервер из состава дистрибутива ОС семейства Microsoft Windows Server.

Сервер межсетевого экранирования предназначен для контроля и фильтрации трафика из сетей общего доступа.

На сервере межсетевого экранирования устанавливается следующее программное обеспечение:

- ОС Microsoft Windows Server 2008 Enterprise Edition R2;
- ПО VipNet Coordinator 3.1.

Основным функциональным элементом сервера является межсетевой экран ViPNet Coordinator.

Межсетевой экран ViPNet Coordinator выполняет фильтрацию открытого и туннелируемого трафика: проверяет весь входящий и исходящий IP-трафик и принимает решение о возможности его дальнейшего направления к пункту назначения, т.е. служит для предотвращения несанкционированного доступа из одной сети в другую.

Межсетевой экран ViPNet Coordinator обеспечивает:

- включение в корпоративную сеть открытых и защищенных компьютеров, находящихся в этих локальных сетях, независимо от способа подключения и типа IP-адреса компьютера;
- разделение и защиту сетей от сетевых атак;
- оповещение клиентских компьютеров о состоянии других сетевых узлов, с ним связанных.

Межсетевой экран ViPNet Coordinator выполняет фильтрацию открытых пакетов на каждом сетевом интерфейсе в соответствии с заданными настройками по адресам, протоколам и портам. Данная функция позволяет блокировать нежелательные IP-пакеты и IP-адреса и осуществляет беспрепятственное соединение с доверенными узлами, не входящими в сеть ViPNet. Помимо настраиваемых правил фильтрации, в программе имеется система обнаружения вторжений, блокирующая наиболее распространенные сетевые атаки.

При взаимодействии с компьютерами, находящимися за межсетевым экраном (координатором), приложения ViPNet по умолчанию обращаются к ним по виртуальным адресам.

Фильтрации подвергается весь трафик, проходящий через сетевой узел:

- открытый (нешифрованный) трафик (локальный или транзитный);
- защищенный трафик (перед его шифрованием и после расшифровки);
- туннелируемый трафик (перед его шифрованием и после расшифровки).

Интегрированный межсетевой экран ViPNet Coordinator имеет пять предустановленных режимов безопасности:

- блокировка IP-пакетов всех соединений;
- блокировка всех соединений, кроме разрешенных;
- разрешение всех исходящих соединений, кроме запрещенных;
- разрешение всех соединений;
- разрешение IP-пакетов на всех интерфейсах без обработки.

Обобщенный алгоритм работы ПАК «Интернет» заключается в следующем:

- пользователь осуществляет процедуру идентификации и аутентификации на своей рабочей станции под учетной записью пользователя домена внутреннего леса;
- пользователь на своей рабочей станции подключается к удаленному рабочему столу терминального сервера (инициирует RDP-сессию);
- пользователь осуществляет процедуру идентификации и аутентификации на терминальном сервере под учетной записью пользователя домена внешнего леса;
- пользователю предоставляется удаленный рабочий стол для доступа в Интернет;
- пользователь открывает веб-браузер для получения доступа в Интернет;
- по окончания работы пользователь завершает сеанс (разрывает RDP-сессию);
- файлы, загруженные пользователем в ходе работы из сети Интернет, сохраняются на терминальном сервере;
- для переноса файлов с терминального сервера на свою рабочую станцию пользователю необходимо обратиться к администратору.

Необходимо отметить, что технические решения по созданию защищенного доступа сотрудников ОВД в международную сеть Интернет были успешно реализованы в МВД по Республике Татарстан, а затем были подтверждены как перспективные и соответствующие требованиям правовых актов и регуляторов в области обеспечения информационной безопасности на апробации в УМВД России по Рязанской области.

Таким образом, описанный комплекс ПАК «Интернет», при условии постановки на снабжение, может решить задачу организации доступа к ресурсам международной сети Интернет из защищённых сегментов ЛВС ОВД.