А.В. Серезевский, А.В. Голубев, В.А. Николаев
(НИЦ "Охрана" МВД России; e-mail: golubev@mail)

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУНКТОВ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ НА ОСНОВЕ МАРШРУТИЗАТОРОВ

Анализируются информационные угрозы централизованной охране. Даны рекомендации по обеспечению безопасности с использованием маршрутизаторов.
Ключевые слова: угрозы информационной безопасности, пункты централизованной охраны.

A.V. Serezevskij, A.V. Golubev, V.A. Nikolaev

COUNTERING THREATS TO INFORMATION SECURITY ITEMS CENTRALIZED SECURITY BASED ROUTERS

Analyzes threat protection using the Internet. Recommendations on security using routers.
Key words: threats of information security, points of the centralized protection, protection of information.

Статья поступила в редакцию Интернет-журнала 12 декабря 2014 г.

Развитие Интернета и GSM позволяет использовать их для целей централизованной охраны более широко и интенсивно. Вместе с тем, некоторые ***пульты централизованного наблюдения (ПЦН)***, до подключения к Интернету, не сталкивавшиеся с вопросами защиты информации, могут оказаться неподготовленными к изменившейся ситуации [1].

В системах передачи информации атакам может быть подвергнуто как объектовое оборудование – ***устройства объектовые оконечные (УОО)***, ***приборы приёмно-контрольные охранные (ППКО)***, так и пультовое оборудование – компьютеры ***автоматизированых рабочих мест (АРМ)***, серверы баз данных, коммутаторы. Целями атак могут быть: захват управления АРМ, копирование базы данных клиентов, корректировка базы данных, блокирование тревожных сигналов с объектов охраны [2].

Если АРМ реализован на базе локальной или распределенной информационной системы, подключенной к сетям общего пользования и (или) сетям международного информационного обмена, то в ней могут возникать угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Вредоносные программы могут быть внесены в процессе эксплуатации АРМ. Они основаны на использовании уязвимостей программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционирован-

ного исследования параметров АРМ без вмешательства в функционирование АРМ, до уничтожения служебной информации и программного обеспечения АРМ) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тысяч сигнатур компьютерных вирусов.

Производители технических средств охраны рекомендуют обычную для небольших компьютерных сетей защиту при подключении ПЦН к Интернету. Из особенных требований можно выделить:

- использование межсетевых экранов;
- применение трансляции сетевых адресов (NAT);
- организация резервного канала для подключения к хосту в случае выхода из строя основного канала;
- организация третьего – аварийного канала для подключения ПЦН к Интернету в случае выхода из строя основного и резервного каналов.

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют ***межсетевым экраном (МЭ)***. В переводной литературе также встречаются термины "firewall" или "брандмауэр".

Межсетевой экран – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), осуществляющее контроль информации, поступающей в автоматизированную систему и/или исходящей из неё. МЭ повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию конфиденциальности во внутренней области режима. Кроме функций разграничения доступа, МЭ может обеспечивать выполнение дополнительных функций безопасности (аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий).

При настройке политики межсетевого экранирования рассматривают два аспекта сетевой безопасности: политику доступа к сетевым ресурсам и политику реализации собственно МЭ. Политика доступа к сетевым ресурсам отражает общие требования по безопасности той или иной организации, и при её разработке должны быть сформулированы правила доступа пользователей к различным сервисам, используемым в организации. Указанные правила опи-

сывают, какой внутренний (внешний) пользователь (группа пользователей), когда, с какого внутреннего (внешнего) узла сети и каким сервисом может воспользоваться с уточнением, в случае необходимости способов аутентификации пользователей и адресов целевых серверов.

Трансляция сетевых адресов (NAT) – технология, которая позволяет маршрутизатору выполнять функцию прокси-сервера по сокрытию информации об узлах внутренней сети. В целях сокрытия информации о внутренней сети, маршрутизатор с NAT функционирует следующим образом:

- при передаче запросов клиентов защищаемой сети во внешнюю сеть заменяет их IP-адреса на IP-адрес своего внешнего интерфейса (может использоваться и диапазон IP-адресов);

- при возврате ответов серверов клиентам производит обратную замену: свой адрес в поле получателя меняет на адрес клиента, отправившего исходный запрос.

Преимущество использования трансляции сетевых адресов состоит в том, что при подключении внутренней сети к Интернету технология NAT позволяет существенно увеличить адресное пространство за счет использования IP-адресов из диапазона частных сетей, не обрабатываемых маршрутизаторами Интернета.

При этом тип оборудования для защиты линий ПЦН необходимо выбирать из государственного реестра сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. В соответствии с указом Президента РФ от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", " … при необходимости подключения информационных систем … такое подключение производится только с использованием специально предназначенных для этого средств защиты информации … получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для … владельцев … вычислительной техники".

Сегодня на рынке имеются десятки различных производителей маршрутизаторов. Поскольку их тираж огромен, надо стараться максимально учитывать практический опыт работы с данными устройствами.

При приобретении межсетевых экранов необходимо тщательно выбрать нужную архитектуру и компоненты. Правильно настроить программное обеспечение и тестировать конфигурацию межсетевого экрана.

Подключение ПЦН к Интернету должно осуществляться через маршрутизатор, в котором используется NAT-проброс одного порта на один компьютер. Этого достаточно для минимального обеспечения безопасного подключения ЛВС ПЦО к Интернету [4].

Известно, что наличие открытых портов для таких протоколов, как Telnet, http и другие, может помочь администрировать сеть. Тем не менее, целесообразно их отключать пусть и в ущерб удобству. Сам факт наличия открытого

порта дает возможность нагрузить трафик сети бесконечными запросами, даже если по этому порту не поднята никакая управляющая программа. Таким образом, необходимо запретить все протоколы типа Telnet, http и другие, кроме необходимых для работы.

Целесообразно на всех работающих станциях устанавливать и обновлять антивирусные базы не реже, чем один раз в месяц. Необходимо применять хорошо показавшую себя антивирусную программу из числа получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

Необходимо ежемесячно анализировать детализацию от интернет-провайдера по всем подключениям относительно размера входного/выходного трафика; адресов обращений. В случае обнаружения подозрительной активности целесообразно через провайдера блокировать доступ по указанному адресу. Это даст возможность превентивной блокировки потенциально опасных ресурсов.

Необходимо физически выключать или блокировать доступ приборов от клиентов, расторгнувших договор на охрану. По факту расторжения договора на охрану при использовании VPN-сети необходимо принять меры для отключения этого абонента не только от услуг охраны, но и от возможности входа в саму среду передачи данных. Самое правильное – запретить в явном виде доступ для этого абонента к невостребованному ресурсу.

Таким образом, межсетевые экраны являются необходимым средством обеспечения информационной безопасности, они формируют "первую линию" обороны. Однако для полной безопасности необходимо выполнять перечисленные выше дополнительные организационно-технические требования.

Литература

1. ***Членов А.Н., Николаев В.А.*** Задачи повышения эффективности сбора и обработки информации в автоматизированной системе противокриминальной защиты объектов // Матер. 23-й науч.-техн. конф. "Системы безопасности – 2014". М.: Академия ГПС МЧС России, 2014. С. 316-318.

2. ***Базовая*** модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

3. ***Распоряжение*** Правительства РФ от 23 марта 2006 г. № 441-РС (в редакции распоряжения Правительства РФ от 18 августа 2010 г. № 1361-РС "Об утверждении Перечня критически важных объектов РФ").

4. ***Приказ*** МВД России № 734 от 19 сентября 2006 г. "Об утверждении Правил предоставления и использования ресурсов сети "Интернет" в системе МВД России".