УДК 681.31

В.И. Белопушкин, А.Н. Кириллычев

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Семинар № 10

Одной из важных задач стоящих перед руководителями государственных структур и коммерческих организаций различных форм собственности является обеспечение конфиденциальности информации[1]. Эта информация может быть представлена в бумажном виде или в виде акустических колебаний, а также в цифровом виде на электронных носителях. Если для первых двух видов информации достаточно хорошо проработаны вопросы ее сохранности, то при подготовке, обработке, хранении, передачи информации цифровом в виде, стоит серьезная проблема организации обеспечения информационной безопасности и защиты от несанкционированного доступа к ней.

Информационная безопасность должна обеспечивать физическую и логическую целостность информации, блокирование несанкционированного доступа к ней, наличие эффективных средств ее защиты и контроля. Нарушение информационной безопасности при хранении, обработки и передачи информации может привести к серьезным последствием и даже существенному материальному ущербу.

Это связано с тем, что к конфиденциальной информации возможен неавторизованный доступ. Информация может быть уничтожена, повреждена, похищена или скопирована незаметно для авторизованного пользователя.

Для защиты от несанкционированного доступа (НСД) к информации в электронном виде стоит задача создания системы информационной безопасности в существующих или проектируемых корпоративных информационно-вычислительных сетях различного назначения.

Законодательство Российской Федерации[2] предоставляет собственнику информации право защиты конфиденциальности от НСД и установление режима коммерческой тайны[3]. Режим коммерческой тайны подразумевает применение правовых мер, проведения организационных и технических мероприятий по охране конфиденциальности и противодействия НСД.

К правовым мерам охраны конфиденциальности относятся следующие положения.

1. Соблюдать нормативно-правовые акты и регламентирующие документы.

2. Регулировать отношения по использованию конфиденциальной информации работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

3. Требовать возмещение причиненных убытков от физических и юридических

[1]Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и уровнем доступа к информационному ресурсу.

[2]Гражданский кодекс Российской Федерации, Федеральный законы Российской Федерации "Об информации, информатизации и защите информации", "О цифровой подписи", "О коммерческой тайне", Указ Президента Российской Федерации "Об утверждении перечня сведений конфиденциального характера".

[3]Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем (собственником) информации меры по охране ее конфиденциальности.

лиц.

К организационным мероприятиям охраны конфиденциальности можно отнести следующие положения.

1. Провести анализ фактического состояния системы защиты от НСД.

2. Определить перечень информации, составляющей конфиденциальную информацию.

3. Назначить ответственное лицо за соблюдение режима конфиденциальности.

4. Ограничить доступ к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

5. Разработать памятку по обеспечению режима конфиденциальности.

6. Вести учет лиц, получивших доступ к конфиденциальной информации и лиц, которым такая информация была предоставлена или передана.

7. Наносить на материальные носители (документы и т.д.), содержащие конфиденциальную информацию, соответствующий гриф.

8. Организовать обучение работников правилам обращения с информацией конфиденциального характера.

К техническим мероприятиям охраны конфиденциальности можно отнести следующие положения.

1. Разработать модель вероятного противника и определить его техническую оснащенность.

2. Установить вероятные каналы утечки информации.

3. Составить схему инженерных и проводных (слаботочные и электросиловые) коммуникаций.

4. Провести ревизию проводных коммуникаций, промаркировать их.

5. Контролировать прокладку коммуникаций ведется и схему соединений.

6. Организовать контроль за проведением ремонтных, регламентных и профилактических работ на проводных слаботочных и электросиловых коммуникациях.

7. Контролировать сохранность опечатанных слаботочных и электросиловых распределительных коробок (щиты, шкафы и т.п.) на предмет несанкционированного вскрытия.

8. Разграничить права доступа локальных, территориально-распреде-ленных и удаленных пользователей к конфиденциальным информационным ресурсам, в том числе к сети Internet.

9. Составить перечень сертифицированных инженерно-технических, программно-аппаратных средств защиты и контроля.

10. Соблюдать рекомендации по подбору технических средств защиты, их использованию и правил эксплуатации.

Исходя из требований положений к организационно-техническим мероприятиям обеспечения режима коммерческой тайны, можно сделать вывод, что для защиты конфиденциальной информации от несанкционированного доступа необходимо построение системы информационной безопасности.

Система информационной безопасности (СИБ) должна соответствовать следующим требованиям.

1. Охватывать полный комплекс задач по защите информации.

2. Решения комплекса задач по защите информации должны:

- по возможности не снижать производительность информационных систем;
- обладать развитыми функциями мониторинга и контролем событий;
- иметь интуитивно понятный интерфейс, просты в установке и конфигурации;
- быть прозрачными для конечного пользователя;

3. Технические средства СИБ должны предотвращать НСД к корпоративным вычислительным сетям, а также утечку информации по техническим каналам.

4. СИБ должна фиксировать отклонения от заданных режимов функционирования.

СИБ включает в себя следующие подсистемы.

1. Подсистема аутентификации и авторизации пользователей при доступе к ресурсам вычислительной сети.

2. Подсистема обеспечения безопасности на уровне 2.

3. Подсистема создания защищенного соединения с удаленными офисами.

4. Подсистема защищенного соединения с Интернет[4].

5. Подсистема обнаружения вторжений.

6. Подсистема модуля управления (сеть управления).

7. Подсистема антивирусной защиты Интернет-трафика[5].

1. Подсистема аутентификации и авторизации пользователей

Для обеспечения авторизации и аутентификации пользователей при доступе к ресурсам вычислительной сети используют механизмы, предоставляемые контроллером домена, построенном на базе операционной системы Microsoft Windows 2000 Professional с развернутой единой службой каталогов - Active Directory.

2. Подсистема обеспечения безопасности на уровне 2

Для обеспечения безопасности на 2-м уровне модели OSI6 используют технологию построения на базе корпоративной сети виртуальных локальных сетей (VLAN[7]). В рамках корпоративной сети выделяют следующие виртуальные локальные сети, маршрутизация между которыми осуществляется коммутатором:

- VLAN для каждого структурного подразделения, размещенного в здании и входящего в единую структуру корпоративной сети;
- VLAN для сети управления;
- VLAN для активного сетевого оборудования;
- VLAN серверного комплекса.

Использование виртуальных локальных сетей позволяет использовать списки доступа (Access List) на коммутаторе типа Cisco Catalyst. Использование модуля маршрутизации на таком виде коммутатора позволит сделать структуру VLAN-ов прозрачной для всего домена, а также производить первичную фильтрацию трафика и блокирования несанкционированного доступа (НСД) внутри локальной сети.

Предотвращение угрозы НСД достигается фильтрацией подсетей:

- запрет передачи трафика между VLAN-ми структурных подразделений;
- запрет передачи трафика в VLAN для активного сетевого оборудования, кроме трафика из VLAN для сети управления;
- разрешить передачу трафика между VLAN-ми структурных подразделений и серверным VLAN.

3. Подсистема создания защищенного соединения с удаленными офисами

Для обеспечения защищенного соединения и обмена информационными потоками между территориально удаленными структурными подразделениями используют специализированные программно-аппаратные продукты. Наиболее распространенным является программно-аппаратный продукт ViPNet[8].

---

[4]Интернет (Internet) - глобальная информационная сеть, части которой логически взаимосвязаны друг с другом посредством единого адресного пространства, основанного на протоколе TCP/IP. Интернет состоит из множества взаимосвязанных компьютерных сетей и обеспечивает удаленный доступ к компьютерам, электронной почте, доскам объявлений, базам данных и дискуссионным группам.

[5]Интернет трафик - полный информационный поток в коммуникационной системе. Трафик измеряется в нужных точках сети числом проходящих блоков данных и их длин, выраженным в битах в секунду.

[6]OSI (Open Systems Interconnection) - взаимодействие открытых систем, правила сопряжения систем с открытой архитектурой от различных производителей.

[7]VLAN (Virtual LAN) - виртуальная локальная вычислительная сеть (ЛВС), объединение конечных станций, подсоединенных к физически различным сегментам ЛВС, в логические рабочие группы.

Для объединения центрального офиса с удаленными офисами в единую корпоративно-вычислительную сеть по защищенным каналам связи используют VipNet Tunnel и VipNet Administrator.

В составе пакета программ ViPNet Tunnel поставляется 2 лицензии на ViPNet (Координатор) и 20 туннельных лицензий для компьютеров защищаемых локальных сетей.

VipNet (Координатор) это модуль, осуществляющий следующие функции:

- выполняет маршрутизацию защищенных пакетов при взаимодействии объектов сети между собой;
- в реальном времени осуществляет регистрацию и предоставление информации о состоянии объектов сети и значении их динамических адресов;
- обеспечивает работу защищенных компьютеров локальной сети в VPN от имени одного адреса (функция proxy);
- осуществляет туннелирование пакетов от обслуживаемой ViPNet (Координатором) группы незащищенных компьютеров локальной сети для передачи трафика от них к другим объектам VPN в зашифрованном виде по открытым каналам Интернет/ Интранет[9];
- фильтрует трафик от источников, не входящих в состав VPN, в соответствии с заданной политикой безопасности (функция межсетевого экрана);
- обеспечивает возможность работы защищенных по технологии ViPNet компьютеров локальной сети через сетевые экраны и прокси-сервера[10] различных производителей.

VipNet (Администратор) это модуль, создающий инфраструктуру сети, осуществляющий мониторинг и управление объектами сети, а также формирует первичную ключевую и парольную информацию для объектов сети, сертифицирует ключевую информацию, сформированную объектами сети.

Еще одним достоинством продукта VipNET является криптографическое ядро «Домен-К», который имеет сертификаты[11] уполномоченных федеральных органов.

В центральном узле выделяется модуль VPN удаленного доступа. Данный модуль терминирует трафик VPN, поступающий от территориально удаленных офисов, действует в качестве концентратора для

---

[8]Программный продукт VipNET имеет следующие сертификаты Гостехкомиссии при Президенте Российской Федерации №№ 545, 546 от 17.12.2001 г.:

- сертификат Гостехкомиссии России на программный комплекс ViPNet - по классу защищенности 1В для Автоматизированных систем (АС) и по 3 уровню контроля отсутствия недекларированных возможностей (НДВ);
- сертификат Гостехкомиссии России при президенте Российской Федерации на межсетевой экран ViPNet - по 3 классу защищенности для Межсетевых экранов (МЭ) и по 3 уровню контроля отсутствия не декларированных возможностей (НДВ).

[9]Интранет (Intranet) - распределенная корпоративная вычислительная сеть, предназначенная для обеспечения теледоступа пользователей к корпоративным информационным ресурсам и использующая программные продукты и технологии Интернет.

[10]Прокси-сервер (Proxy server) - специальный Интернет-сервер, управляющий входящим и исходящим трафиком интернета в локальной сети.

[11]Сертификат соответствия № СФ/114-0470 от 01 июня 2001 года, удостоверяющий, что программное средство криптографической защиты информации (СКЗИ) "Домен-К" соответствует требованиям ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34, 11-94 и требованиям ФАПСИ к стойкости СКЗИ Класса КНВ 2.99 и может использоваться для формирования ключей шифрования и ключей электронной цифровой подписи, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну.

Сертификат соответствия № СФ/124-0471 от 01 июня 2001 года, удостоверяющий, что аппаратно-программное средство криптографической защиты информации (СКЗИ) "Домен-К" соответствует требованиям ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34, 11-94 и требованиям ФАПСИ к стойкости СКЗИ Класса КНВ 2.99 и может использоваться для формирования ключей шифрования и ключей электронной цифровой подписи, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну.

терминирования этого трафика. Весь трафик, направляемый в локальную вычислительную сеть, поступает от территориально удаленных пользователей, которые аутентифицируются и получают право прохода через межсетевой экран.

В данном модуле размещается оборудование для обеспечения защищенных соединений с территориально удаленными офисами, а также поддержка передачи голосовых сообщений по защищенным каналам связи.

Структурно в состав модуля входят маршрутизатор типа Cisco. За маршрутизатором устанавливается программное обеспечение (ПО) VipNet (Координатор), обеспечивающее шифрование каналов связи. Если в данном модуле предполагается передача голосовых сообщений, то после ПО VipNet (Координатор) необходимо дополнительно установить еще один маршрутизатор голосового шлюза, обеспечивающий приоретизацию голосового трафика. Голосовой шлюз подключается к существующей цифровой телефонной станции. Модуль VPN удаленного доступа подключается к отдельным интерфейсам центрального межсетевого экрана, а также резервного центрального межсетевого экрана. В этом модуле необходимо предусмотреть установку сенсор системы обнаружения вторжений, обеспечивающего мониторинг трафика.

Использование модуля VPN позволит предотвратить угрозы по раскрытию сетевой топологии и исключит возможность передачи трафика на несанкционированные порты.

4. Подсистема защищенного соединения с Интернет

Схема защиты подключения корпоративной сети к глобальной информационной сети Интернет строится по расширенному трехуровнему принципу:

- маршрутизатор доступа;
- демилитаризованная зона;
- внутренний фильтрующий маршрутизатор.

Все точки доступа в локальную вычислительную сеть извне замыкаются на основном и резервном межсетевом экране, работающих в режиме горячей замены и выступающие в роли внутреннего фильтрующего маршрутизатора.

К межсетевым экранам подключаются несколько изолированных зон, часть из которых является выделенными сегментами для каждого типа доступа:

- внешняя сеть (Интернет);
- внутренняя сеть (локальная вычислительная сеть);
- зона доступа к ресурсам подключенных по выделенным каналам связи;
- демилитаризованная зона, в которой размещаются Mail[12], DNS[13] и WWW сервера.

Межсетевой экран обеспечивает выполнение функций NAT/PAT для доступа к сети Интернет из корпоративной вычислительной сети и доступа из сети Интернет к выделенным серверам демилитаризованной зоны, а также обес-печивают фильтрацию трафика между изолированными зонами при помощи списков доступа и механизма Stateful Firewall.

Для обеспечения требований по отказоустойчивости доступа в Интернет, предлагается использовать два внешних канала связи двух различных провайдерах. Маршрутизаторы доступа выступают в качестве периферийного маршрутизатора и осуществляют базовую фильтрацию входного трафика, которая пропускает только ожидаемый (по адресам и IP-услугам) трафик для блокирования атак типа IP спуфинг.

Демилитаризованная зона подключается на отдельный интерфейс межсетевого

[12]e-Mail (Электронная почта) - сетевая служба, позволяющая пользователям обмениваться сообщениями или документами без применения бумажных носителей.

[13]Domain name system (DNS) - система имен доменов - в сети Internet, распределенная служба формирования имен узлов, используемая в Internet, устанавливающая соответствие между именами узлов и доменов с одной стороны и IP-адресами с другой стороны.

экрана и предназначена для размещения в ней серверов общего доступа, к которым должен быть разрешен доступ в корпоративной сети строго по определенным IP адресам и портам.

Внутренний фильтрующий маршрутизатор использует технологию «private VLAN» и обеспечивает снижение угрозы атаки на защищаемую сеть в случае получения НСД к одному из серверов демилитаризованной зоны.

Данная структура построения защищенного соединения с Интернет блокирует следующие виды угроз:

- НСД с помощью фильтрации на уровне провайдера (ISP), периферийного маршрутизатора и корпоративного межсетевого экрана;
- атаки на уровне приложений с помощью IDS[14] на уровне хоста и сети;
- атаки на пароли, контролируемые средствами операционной системы и IDS;
- отказ в обслуживании (DoS) на периферии ISP и с помощью контроля установлений сессий TCP на межсетевом экране;
- выявление вирусных программ, в том числе "троянский конь" с помощью фильтрации содержания электронной почты;
- обнаруживает попытки ведения сетевой разведки.

5. Подсистема обнаружения вторжений

В состав системы обнаружения вторжений входят сенсоры, осуществляющие мониторинг трафика в режиме реального времени и проверки на наличие в потоке данных сигнатур атак, и консоль управления, на которую подаются сигналы об обнаружении вторжения.

Сенсорные компоненты подсистемы обнаружения вторжений устанавливаются в ключевых точках корпоративной вычислительной сети на границе интернет-модуля и сети Интернет. Это устройство, находящееся на общедоступной стороне межсетевого экрана, производит мониторинг атак и обеспечивает:

- распознавание сигнатур типовых атак;
- использование пополняемой базы данных по сигнатурам атак;
- пропускную способность необходимую для проверки всего трафика в обслуживаемом сетевом сегменте;
- механизм реакции на обнаружение атаки, включающей в себя сброс соединения, блокирование дальнейших попыток атак с IP адреса атакующего хоста, занесение информации в журнал и вывод сообщения на монитор управления;
- создание VPN-соединений между сенсорами обнаружения вторжений и консолью управления;
- защиту и мониторинг ключевых сегментов корпоративной вычислительной сети.

6. Подсистема модуля управления (Сеть управления)

Главная цель модуля управления состоит в том, чтобы обеспечить безопасное управление всеми устройствами и хостами в корпоративной вычислительной сети. Потоки отчетности и информации для лог-файлов[15] поступают с устройств на хосты управления, тогда как изменения конфигурации и новое программное обеспечение поступают с хостов управления на устройства.

Сеть управления использует адресное пространство, непересекающееся с адресным пространством корпоративной вычислительной сети, межсетевые экраны настраиваются таким образом, чтобы пропускать в сеть управления только трафик, относящийся к задачам управления и мониторинга и выполняющим следующие функции:

- блокирование потоков НСД трафика

[14]IDS - Система обнаружения вторжений.

[15]Лог-файл - файл, содержащий системную информацию о работе сервера и информацию о действиях пользователей: дату и время визита пользователя, IP-адрес компьютера пользователя, наименование браузера пользователя, URL запрошенной пользователем страницы.

при помощи списков доступа;

- блокирование потоков трафика, использующих «чужое» адресное пространство;

- терминирование VPN туннелей от сенсоров обнаружения вторжений.

В сети управления размещаются средства мониторинга и управления корпоративной вычислительной сети типа VipNET Administrator, который предназначен для создания инфраструктуры защищенных сетевых соединений, мониторинга и управления объектами сети, а так же формирования первичной ключевой и парольной информации для объектов корпоративной вычислительной сети, построенной на базе программного обеспечения VipNET Corporate.

Данный программный продукт позволяет Администратору безопасности корпоративной вычислительной сети проводить следующие виды контроля:

- мониторинг возможных атак на определенные хосты (WWW сервер);

- мониторинг всего трафика для определения шаблонов атак;

- коррелировать информацию, собираемую с различных IDS сенсоров;

- получать раннее предупреждение об атаках.

Подсистема модуля управления позволяет блокировать следующие виды угроз:

- НСД за счет фильтров межсетевого экрана, что пресекает почти все потоки несанкционированного трафика в обоих направлениях;

- хакерскую разведку корпоративной сети, т.к. весь трафик, связанный с управлением, передается по частной сети провайдера;

- атаки на идентификационные пароли, т.к. сервер контроля доступа может поддерживать различные типы аутентификации на каждом устройстве.

7. Антивирусная защита SMTP/ HTTP трафика

Для обеспечения антивирусной защиты корпоративной вычислительной сети используют программное обеспечение, в состав которого входят следующие пакеты прикладных программ:

- защита от вирусов в реальном времени шлюзов Интернет;

- защита корпоративной системы обмена сообщениями и групповой работы Microsoft Exchange;

- защита файл-серверов (NT, NetWare, Linux);

- защита рабочих станций.

Коротко об авторах

Белопушкин Виктор Иванович – профессор, кандидат технических наук,
Кириллычев Александр Николаевич – доцент, кандидат технических наук,

кафедра «Автоматизированные системы управления», Московский государственный горный университет.