УДК 638.235.231

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Андрей Тимошенко
Общество с ограниченной ответственностью «Институт компьютерных технологий», г. Киев

Анотація: **Наведено опис комплексу засобів захисту інформації, що обробляється в розподілених обчислюваних мережах з протоколом TCP/IP, від несанкціонованого доступу, з використанням механизмів розмежування доступу та криптографічного захисту.**
Summary: **A description of the information protection system for wide-area TCP/IP networks, based on access mediation and cryptography security mechanisms is given.**
Ключові слова: **Мережа, доступ, автентифікація, шифрування.**

По мере развития Интернет и информационных технологий все большую привлекательность для различных организаций в качестве инструмента для автоматизации бизнес-процедур, документооборота, финансовых операций приобретают виртуальные частные сети (Virtual Private Network -VPN).

В общем случае VPN - это объединение локальных вычислительных сетей (ЛВС) или отдельных компьютеров, подключенных к распределенной вычислительной сети (РВС) общего пользования, в единую виртуальную (наложенную) сеть. VPN, создаваемые на базе РВС общего пользования (и, в первую очередь, Интернет), являются хорошей альтернативой изолированным корпоративным сетям, обладающей рядом несомненных достоинств [1, 2]:

- низкая стоимость арендуемых каналов и коммуникационного оборудования;
- развитая (в географическом смысле) топология сети;
- высокая надежность за счет наличия параллельных каналов передачи;
- легкость масштабирования (подключения новых ЛВС или пользователей);
- легкость конфигурирования.

Однако, необходимо не забывать, что создание VPN, решая одну проблему - существенное сокращение расходов на эксплуатацию собственной корпоративной сети, выдвигает на первое место другую - обеспечение безопасности обрабатываемой информации.

Комплекс PostCrypt-VPN предназначен для защиты информации, обрабатываемой в РВС с протоколом TCP/IP, от угроз целостности, конфиденциальности и доступности с использованием механизмов разграничения доступа и криптографической защиты. В состав PostCrypt-VPN входят программные модули-агенты средств защиты клиента и сервера, функционирующие на рабочих станциях (РС), имеющих доступ к РВС, автоматизированные рабочие места (АРМ) управления и администрирования и АРМ управления ключами центра сертификации открытых ключей (ОК).

Модуль-агент средств защиты клиента реализует следующие функции:

- прием запросов на установление защищенных соединений с сервером приложений от зарегистрированных РС;
- установление связи по протоколу TCP с модулем-агентом средств защиты сервера, функционирующим на противоположной стороне виртуального соединения;
- строгую аутентификацию модуля-агента средств защиты сервера с использованием механизма электронной цифровой подписи (ЭЦП) по алгоритму, установленному ГОСТ 34.310-95, 34.311-95;
- выработку сеансового ключа для шифрования данных, передаваемых по виртуальному соединению, обмен сеансовыми ключами, зашифрованными на ключе шифрования ключей (КШК), выработанном по схеме Диффи-Хеллмана, с модулем-агентом средств защиты сервера;
- шифрование/расшифрование данных, передаваемых по виртуальному соединению, по алгоритму, установленному ГОСТ 28147-89.

Модуль-агент средств защиты сервера реализует следующие функции:

- прием запросов на установление защищенных соединений с сервером приложений от зарегистрированных модулей-агентов средств защиты клиента;
- строгую аутентификацию модуля-агента средств защиты клиента с использованием механизма электронной цифровой подписи (ЭЦП), по алгоритму, установленному ГОСТ 34.310-95, 34.311-95;

- выработку сеансового ключа для шифрования данных, передаваемых по виртуальному соединению, обмен сеансовыми ключами, зашифрованными на ключе шифрования ключей (КШК), выработанном по схеме Диффи-Хеллмана, с модулем-агентом средств защиты клиента;
- установление связи по протоколу TCP с приложением сервера;
- шифрование/расшифрование данных, передаваемых по виртуальному соединению, по алгоритму, установленному ГОСТ 28147-89.

АРМ управления и администрирования реализуют:

- генерацию ключей ЭЦП пользователей комплекса с сохранением секретных ключей (СК) на специальных носителях (дискета, TouchMemory) и открытых ключей (ОК) в базе данных окрытых ключей (БД ОК);
- управление обменом ОК ЭЦП пользователей комплекса между собой через специально выделенную организацию, выступающую в качестве центра сертификации ОК, или напрямую;
- настройку параметров объектов защиты, входящих в состав ВЗС, и защищенных соединений, используемых для доступа к ВЗС.

АРМ управления ключами центра сертификации ОК реализует:

- генерацию ключей ЭЦП администратора центра сертификации ОК с сохранением СК на специальных носителях (дискета, Touch Memory) и ОК в БД ОК;
- управление приемом ОК пользователей комплекса, сертификацией данных ОК и передачей их в АРМ управления и администрирования объектов защиты.

Реализуемая технология управления криптографическими ключами соответствует требованиям [3].

В терминах нормативного документа системы технической защиты информации НД ТЗИ 2.5-0004-99 “Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа”, программные средства защиты информации, входящие в состав комплекса PostCrypt-VPN, реализуют следующие функциональные услуги безопасности:

{КВ-2, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НО-1, НЦ-1, НВ-2 }.

Разграничение доступа пользователей к защищаемым ресурсам осуществляется в соответствии с концепцией диспетчера доступа. В соответствии с данной концепцией все элементы вычислительной системы относятся к одному из следующих классов:

Объект-пользователь – пользователь, который пытается получить доступ к определенной информации. В соответствии с реализуемой средствами комплекса политикой безопасности обьекты-пользователи делятся на уполномоченных управлять средствами защиты (администраторов) и обычных пользователей.

Объект-процесс – порождаемый пользователем процесс, который пытается получить доступ к определенной информации. В соответствии с реализуемой средствами комплекса политикой безопасности обьектами-процессами являются приложения (процессы, функционирующие на РС ЛВС). Субьекты доступа представляются своими сетевыми адресами (IP - адрес).

Пассивный объект – пассивный источник/приемник информации, которая нуждается в защите. В соответствии с реализуемой средствами комплекса политикой безопасности защищаемыми объектами являются ресурсы серверов приложений (прикладные сервисы), представленные своими транспортными адресами (IP-адрес:порт)[4].

База данных авторизации – информация, определяющая права доступа (атрибуты доступа) объектов-пользователей и обьектов-процессов к пассивным обьектам.

База данных регистрации – записи о запросах и предоставлении доступа субъектов к объектам.

Механизм контроля (диспетчер доступа) – средства, которые реализуют функции защиты и обеспечивают безопасность информации путем управления созданием обьектов-пользователей, обьектов-процессов и пассивных обьектов, предоставления обьектам-пользователям и обьектам-процессам доступа к пассивным обьектам на основании проверки хранящихся в базе данных авторизации аттрибутов доступа пользователя, процесса и пассивного обьекта, с выполнением при этом регистрации событий (действий пользователей и процессов) в БД регистрации, т.е. реализуют правила разграничения доступа (ПРД), принятые в системе, и способствуют соблюдению политики безопасности информации, принятой в организации.

В комплексе реализовано административное разграничение доступа. Это означает, что управление потоками информации между пользователями, процессами и обьектами осуществляют только специально авторизованные пользователи (администраторы). Для каждого защищаемого ресурса (прикладного сервиса) администратор защиты может установить список доступа, в котором перечислены пользователи и процессы, имеющие права доступа к нему. Обычные пользователи изменять права доступа субъектов к объектам, а также выполнять любые другие функции управления системой защиты не могут.

Для получения доступа к защищаемому ресурсу сервера приложений приложение-клиент, функционирующее на РС ЛВС, инициирует запрос к модулю-агенту средств защиты клиента, функционирующему в этой же ЛВС (рисунок 1). Модуль-агент средств защиты клиента по списку доступа проверяет права РС на доступ к

защищаемому ресурсу по ее сетевому адресу (реализуя услугу НВ-1) и, если доступ разрешен, в свою очередь инициирует запрос на установление защищенного соединения к модуль-агенту средств защиты сервера, функционирующему в ЛВС сервера приложений. В процессе установления защищенного соединения модуль-агент средств защиты сервера проверяет полномочия соответствующего модуля-агента средств защиты клиента на доступ к защищаемым ресурсам по его сетевому адресу (реализуя услугу НВ-1) и, если такой доступ разрешен, клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию (реализуя услугу НВ-2), после чего согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности (реализутся услуги КВ-2, ЦВ-2) все данные, передаваемые по TCP-соединению. Взаимная строгая аутентификация выполняется с применением несимметричных криптографических алгоритмов.

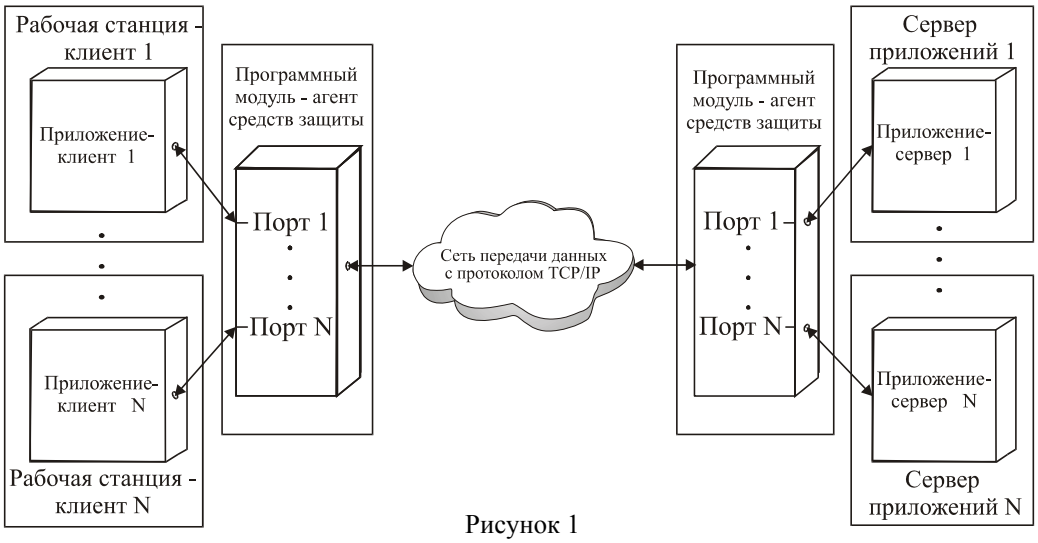

Рисунок 1

После завершения взаимной аутентификации модуль-агент средств защиты сервера устанавливает соединение с защищаемым ресурсом. Все взаимодействие модулей - агентов средств защиты между собой, а также с клиентским и серверным приложением осуществляется на транспортном уровне (четвертый уровень модели взаимодействия открытых систем). При этом на одном и том же узле РВС могут функционировать одновременно как модуль-агент средств защиты клиента (для обеспечения защиты исходящих соединений), так и модуль-агент средств защиты сервера (для обеспечения защиты входящих соединений), причем как исходящие, так и входящие соединения могут устанавливаться с любыми другими узлами ВЗС (в соответствии с выполненными настройками параметров защищенных соединений), а максимальное количество защищенных соединений ограничивается только возможностями соответствующей ОС.

В процессе установления защищенного соединения между модулями-агентами средств защиты, а также обмена данными между клиентским и серверным модулями-агентами средств защиты в специальные файлы протоколов, защищенные от модификации, в реальном времени выводятся сообщения обо всех критичных для безопасности событиях (реализуется услуга НР-2).

Обмен данными между клиентским (серверным) приложением и клиентским (серверным) модулем-агентом средств защиты происходит без доступа в РВС и защищается с использованием средств соответствующих ОС и прикладных программных средств.

При организации ВЗС программные средства комплекса могут использоваться в двух вариантах: для реализации защищенного доступа к ресурсам защищаемой подсети с их межсетевым экранированием и для реализации защищенного доступа к ресурсам сервера приложений.

При реализации защищенного доступа к ресурсам защищаемой подсети с их межсетевым экранированием программный модуль-агент средств защиты клиента запускается на рабочих станциях, на которых функционируют приложения-клиенты, осуществляющие доступ к ресурсам защищаемой подсети, а программный модуль-агент средств защиты сервера - на специально выделенном компьютере (выполняющем функции межсетевого экрана), имеющем два сетевых интерфейса (рисунок 2). Запросы на установление защищенных соединений принимаются модулем-агентом средств защиты клиента только от приложений, функционирующих на тех рабочих станциях, которым разрешен доступ к защищаемым ресурсам (выполняется фильтрация запросов на сетевом уровне) и передаются модулю-агенту средств защиты сервера. Модуль-агент средств защиты сервера принимает запросы на установление защищенных соединений от модулей-агентов

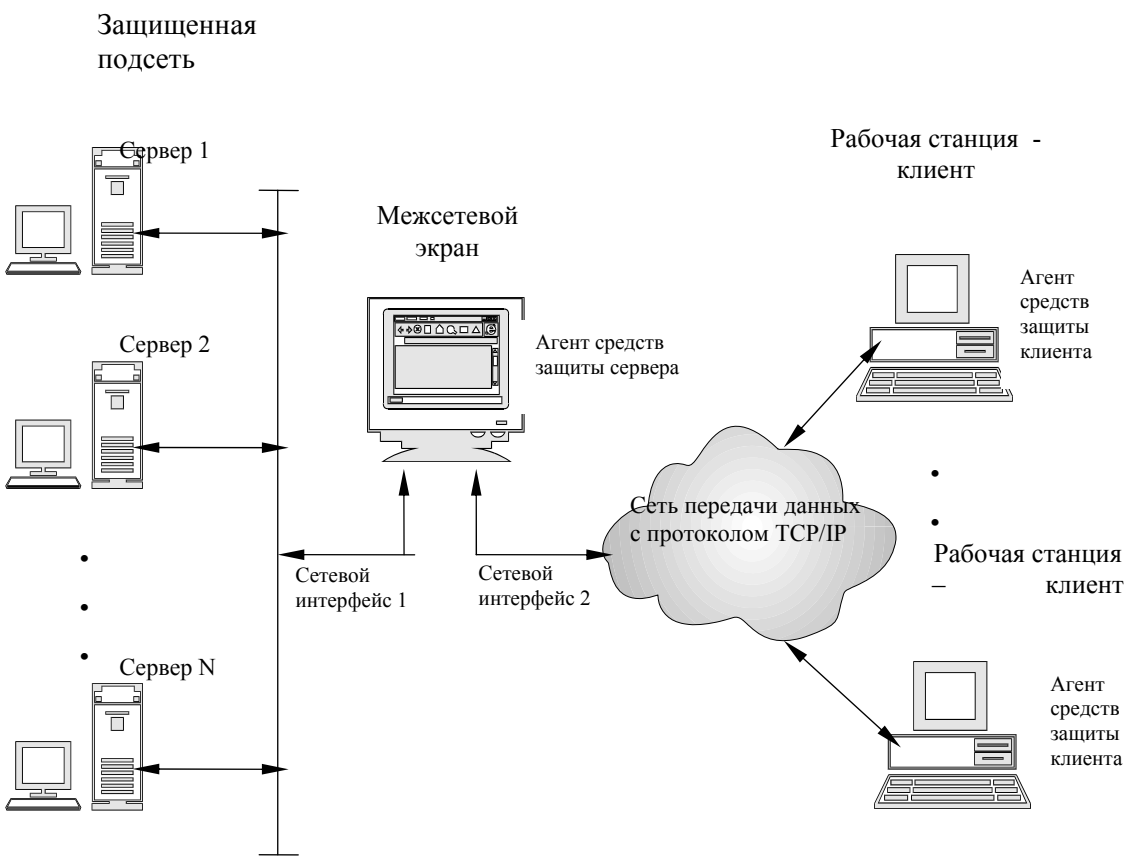

Рисунок 2

средств защиты клиентов через отдельный сетевой интерфейс (интерфейс 2), проверяет полномочия по доступу к защищаемым ресурсам с сетевого адреса данной рабочей станции (выполняет фильтрацию запроса на сетевом и транспортном уровне). При подтверждении полномочий по доступу клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию, согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности все данные, передаваемые между клиентской рабочей станцией и межсетевым экраном, после чего агент средств защиты сервера

устанавливает через другой сетевой интерфейс (интерфейс 1) соединение с соответствующим серверным приложением. При этом в ОС межсетевого экрана отключается автоматическая ретрансляция IP-пакетов с сетевого интерфейса 1 на сетевой интерфейс 2 и наоборот, что позволяет скрыть от внешнего мира (экранировать) ресурсы серверов, функционирующих в защищаемой подсети, сделав их доступными только для оснащенных средствами защиты и зарегистрированных в БД модуля-агента средств защиты сервера рабочих станций.

При реализации защищенного доступа к ресурсам сервера приложений с использованием комплекса PostCrypt-VPN программный модуль-агент средств защиты сервера запускается непосредственно на сервере приложений, а программный модуль-агент средств защиты клиента - на рабочей станции, на которой функционирует приложение-клиент (рисунок 3). Запросы на установление защищенных соединений принимаются модулем-агентом средств защиты клиента только от приложений, функционирующих на той же рабочей станции, что и агент защиты клиента. Принятый запрос передается модулю-агенту средств защиты сервера, который проверяет полномочия по доступу к защищаемому ресурсу с сетевого адреса данной рабочей станции (выполняет фильтрацию запроса на сетевом и транспортном уровне). При подтверждении полномочий по доступу клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию, согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности все данные, которыми обмениваются клиентское и серверное приложения, после чего агент средств защиты сервера устанавливает соединение с соответствующим серверным

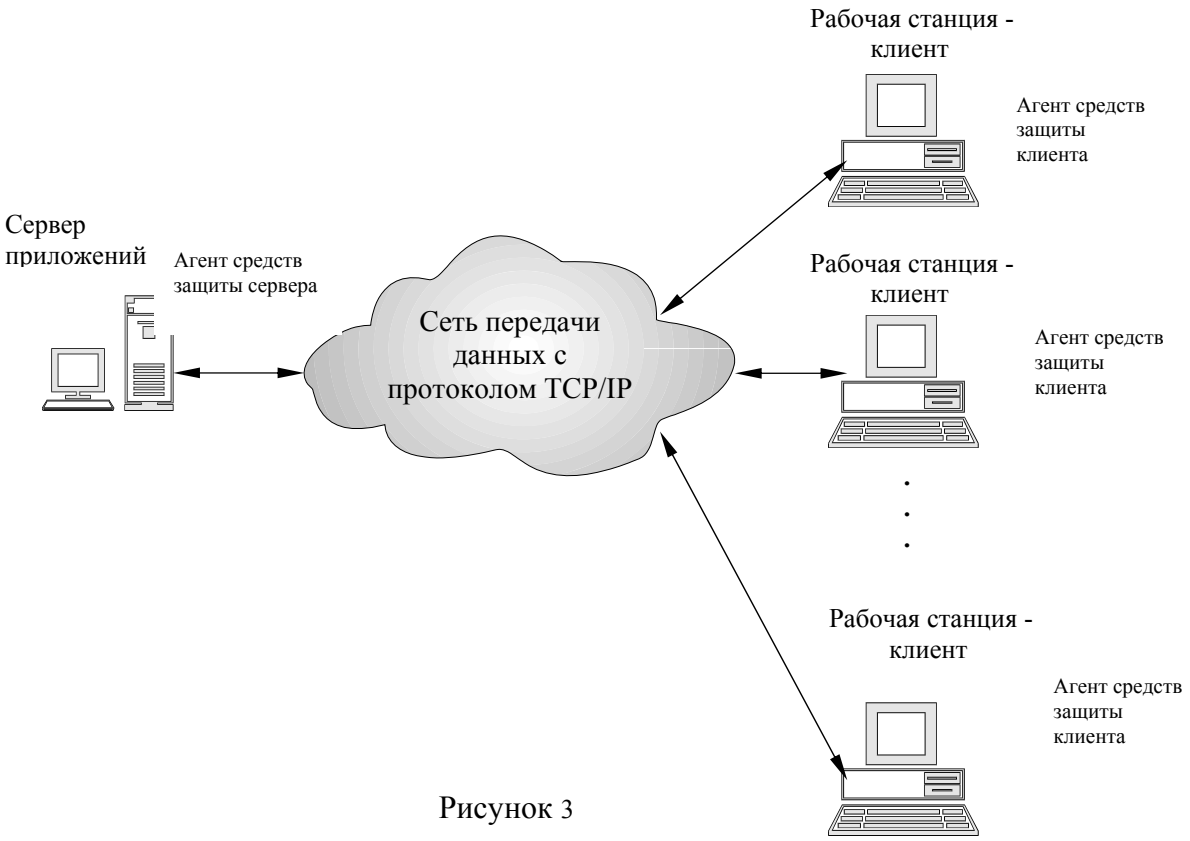

Рисунок 3

приложением. При этом приложение-сервер конфигурируется таким образом, чтобы допускать обработку запросов только от модуля - агента средств защиты сервера (только с сетевого адреса сервера приложений).

Литература: 1. Дениз Паппалардо. Виртуальная реальность? СЕТИ #05-06/99. 2. Роберт Ричардсон. Виртуальные частные сети: только между нами. Lan Magazine/Русское издание, (Март 1997, том 3, номер 2). 3. ITU Recommendation X. 509. The Directory: Authentication Framework (ISO/IEC 9594-8), 1993. 4. ISO 7498-2. Basic Reference Model – Part 2: Security Architecture. – February 1989.

УДК 681.3.067

К ПОСТРОЕНИЮ РАЦИОНАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

Василий Бриль
Военный институт Национального технического университета Украины "КПІ"

Анотація: **Ефективний захист інформації не може бути забезпечений простим включенням у склад автоматизованих систем механізмів та пристроїв захисту – захистом інформації необхідно постійно керувати.**
Summary: **The effective protection of the information can not be ensured with prime actuation in a structure of the automized systems of gears and protective systems - the protect of the information is necessary permanently for controling.**
Ключові слова: **захист інформації, автоматизована система обробки даних.**