Защита информации в ЛВС предприятия как фактор повышения его экономической безопасности

***Т.Д. Дегтярева**, д.э.н., профессор,*
***М.С. Кузьмин**, аспирант, ФГБОУ ВО Оренбургский ГАУ*

Переход к рыночной экономике, появление большого разнообразия организационно-правовых форм предприятий, широкое распространение частной инициативы и предпринимательства способствовали развитию оптовой и розничной торговли. Многообразие торговых предприятий, их высокая насыщенность товарной массой обусловили широкое внедрение автоматизированных рабочих мест, оснащённых современными средствами вычислительной техники. Существенно расширились информационные потоки, так как ежедневно в оптовые торговые предприятия и магазины поступает большое количество разнообразных товаров, денежных средств и др.

Повысились требования к экономической информации со стороны торговых предприятий. Её полнота, достоверность и своевременность явля-

ются важным условием их успешного функционирования и конкурентоспособности. Для предпринимателя наиболее ценной является информация, которую он использует для достижения целей фирмы, разглашение сведений коммерческого характера может лишить его возможности получить планируемую прибыль, т.е. создаёт угрозы его экономической деятельности. Это обстоятельство порождает необходимость применения средств защиты информации на каждом предприятии торговли, особенно конфиденциальной.

При современной глобализации мировой экономики практически нет ни одного персонального компьютера (ПК), подключённого к сети «Интернет», который хотя бы раз не оказался под воздействием компьютерных вирусов или несанкционированного доступа злоумышленников. Способов защиты от различного вида атак много. В частности, известны 10 правил компьютерной безопасности, рекомендуемых специалистами «Лаборатории Касперского»: периодически обновляйте антивирусную программу, проверяйте мобильные носители информации, выполняйте резервное копирование и др. [1].

Эти правила необходимы для всех групп пользователей. Однако для предприятий, работа которых построена на ежедневном хранении, обработке и передаче конфиденциальной коммерческой информации, одной лишь антивирусной защиты недостаточно. Развитие локальных вычислительных сетей (ЛВС) на торговых предприятиях, подключённых к глобальным информационным ресурсам, набирает всё больший темп. В связи с этим актуальна проблема защиты информации в этих сетях в контексте повышения экономической безопасности предприятий. В.Н. Ясенев угрозы безопасности подразделяет на 4 группы: конфиденциальности данных и программ, целостности данных, доступности данных, отказа от выполнения транзакций [2]. Системы защиты компьютера от чужого вторжения весьма разнообразны, общепринятой является их классификация в соответствии с применяемыми средствами защиты (табл. 1).

Активное развитие информационных технологий порождает потребность в постоянном совершенствовании средств защиты информации. По нашему мнению, все их целесообразно разделить на две группы: универсальные и ориентированные на решение одной проблемы. Естественно, что первые являются достаточно дорогими, а вторые – относительно дешёвыми. Их преимущества и недостатки в соответствии с наиболее важными критериями их оценки отображены в таблице 2.

Они имеют ещё и другие различия, обусловленные, как правило, решаемыми задачами. Однако главным недостатком существующих систем защиты второй группы методов является отсутствие возможности применения комплексных средств обеспечения безопасности, так как они изготавливаются для решения одной конкретной проблемы, а в первой – их высокая цена, поскольку они создаются как универсальные с целью получения коммерческой выгоды от их продажи. Это обстоятельство побуждает к поиску новых средств обеспечения компьютерной безопасности экономической информации и их внедрению на предприятиях.

Нами разработан программный комплексный продукт «Сеть безопасности», в котором для обеспечения защиты экономической информации применяют комплекс методов, но одновременно его стоимость значительно ниже существующих универсальных программно-аппаратных решений. В структуру разрабатываемого комплекса входят несколько компонентов (рис. 1):

1. Терминатор – программный модуль (ПМ), на который перенаправляются информационные потоки, поступающие с неиспользуемых портов, для гашения в сети исходящих от злоумышленников сигналов, подобно терминатору в коаксиальной сети.

1. Классификация средств защиты информации

Программный метод	Используемые средства защиты
Средства собственной защиты ПЭВМ, предусмотренные общим программным обеспечением	Элементы защиты, присущие программному обеспечению и препятствующие незаконным действиям (например, защита паролем документов MS Office)
Средства защиты в составе вычислительной системы	Средства защиты аппаратуры, дисков и штатных устройств (защитник Windows)
Средства защиты с запросом информации	криптографические методы защиты информации (Крипто про)
Средства активной защиты	Криптографические средства защиты, в том числе контроль целостности, средства активного реагирования на попытки несанкционированного доступа (антивирусная система Dr.Web Security Space PRO и др.)
Средства пассивной защиты	Программы шифрования защищаемых данных; программы защиты ПО (операционных систем, систем управления базами данных, программ пользователей и др.); вспомогательные программы (уничтожение остаточной информации, формирование грифа секретности выдаваемых документов, ведение регистрационных журналов, имитация работы с нарушителем, тестовый контроль механизма защиты и др.). Например, криптограф Atlansys Bastion

2. Сравнение средств защиты информации по основным параметрам

Критерий оценки средств защиты информации / Средство защиты информации	круглосуточная поддержка	своевременное обновление	информирование о новых версиях	информирование о новых смежных продуктах	информирование о новых угрозах	функциональность	информативность
Универсальные	+	+	+	+	+	+	+
Ориентированные на решение одной проблемы	–	+/–	+/–	+/–	+/–	–	–

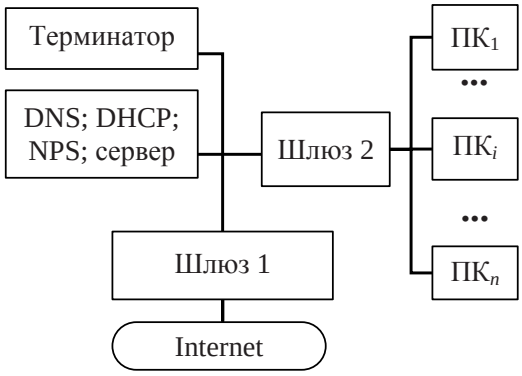


Рис. 1 – Компоненты сети безопасности

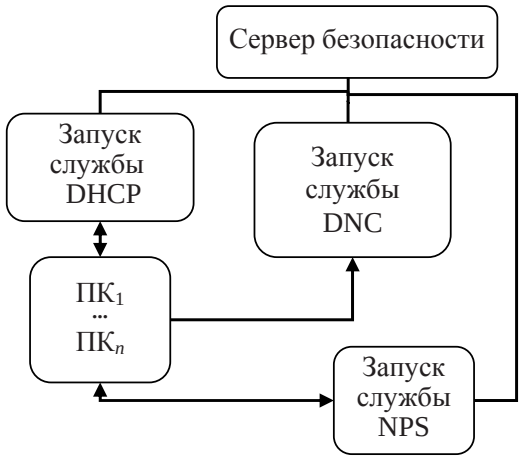


Рис. 2 – Блок-схема сервера безопасности

2. Сервер безопасности (рис. 2) – это ПМ, отвечающий за поддержание функции удалённой аутентификации, в его состав входят DNS-сервер, DHCP и NPS-сервер.

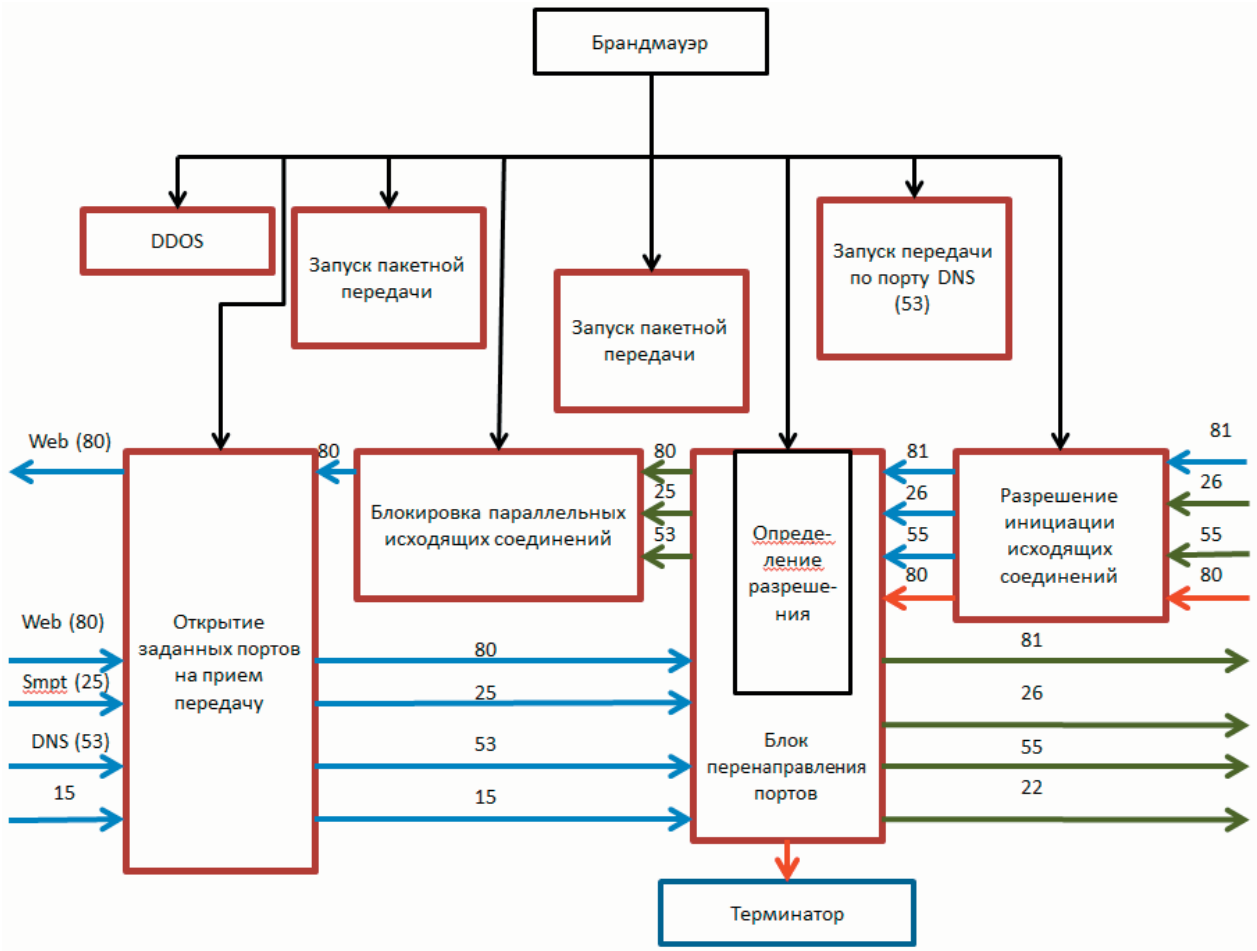
DNS-сервер – протокол разрешения имён для сетей TCP/IP, позволяющий клиентским компьютерам преобразовывать символьные имена DNS в IP-адреса, используемые компьютерами для связи друг с другом [3].

DHCP – один из стандартов IP, призванный упростить управление настройками IP-компьютеров. Этот стандарт предусматривает наличие DHCP-серверов, которые занимаются динамическим выделением IP-адресов и других сопутствующих настроек тем клиентам, которые поддерживают DHCP. В сети TCP/IP каждому компьютеру следует присваивать уникальный IP-адрес, который вместе с маской своей подсети определяет как компьютер, так и подсеть, в которую он входит. Благодаря DHCP назначение IP-адресов клиентам сети производится автоматически из базы данных IP-адресов DHCP-сервера. Для сетей на основе TCP/IP это позволяет снизить сложность и объём работы администраторов при перенастройке компьютеров.

NPS-сервер позволяет централизованно настраивать сетевые политики и управлять ими, используя для этого RADIUS-сервер, RADIUS-прокси и сервер-политик NAP. Процесс аутентификации пользователя происходит по распространённому приёму «логин – пароль». Система запрашивает у пользователя эти данные, затем они передаются на NPS-сервер, где происходит их сравнение с соответствующими сведениями в таблице доступа к ЛВС, составленной администратором. При несовпадении пользователю отсылается сообщение об ошибке. Эта процедура повторяется ещё дважды, в случае двукратного несовпадения пользователь блокируется на заранее установленный администратором интервал времени, затем пользователь получает ещё три попытки входа в ЛВС.

3. Шлюзы 1 и 2 – ПМ, оснащённые разработанным брандмауэром для защиты информации от несанкционированного удалённого доступа. На рисунке 3 показана блок-схема программы брандмауэра, которая отображает прохождение информационных потоков в виде пакетов данных по портам в локальную сеть предприятия торговли и из неё. В состав их программного обеспечения входят:

- DDOS – блок программы, отвечающий за защиту сети от внешних низкоуровневых сетевых атак;
- блок открытия заданных портов на приём и передачу, он позволяет установить разрешения на передачу данных между внешней и внутренней сетями;
- запуск пакетной передачи обеспечивает передачу данных, при этом блокировка параллельных исходящих соединений обеспечивает защиту от несанкционированного доступа к внешней сети программ-шпионов, так или иначе попавших в сеть предприятия;



Обозначения: Web (80), 80, 81 – порт для передачи пакетов web данных; Smpt (25), 25, 26 – порт передачи пакетов почтовых данных; DNS (53), 53, 55 – порт передачи пакетов имён; 15, 22 – порт, открытый администратором для передачи пакетов специальных программ (банк – клиент, 1С и т.д.)

Рис. 3 – Структура брандмауэра

• блок перенаправления портов служит для перенаправления пакетов данных с разрешённых внешних портов на внутренние и наоборот;

• блок определения и разделения пакетов данных, который необходим для защиты от программ-шпионов, последние из внутренний сети предприятия пытаются соединиться со злоумышленником во внешней среде (и наоборот);

отметим также, что: 1) программы злоумышленника обычно ориентированы на заранее выбранные порты, но он не знает, каким портам частной сети открыт доступ во внешнюю среду; 2) в случае попыток злоумышленника соединения со своей программой-шпионом для него остаётся неизвестным, какие внешние порты имеют доступ в частную ЛВС;

• запуск передачи по порту DNS необходим для того, чтобы была возможность проводить удалённую авторизацию пользователей частной сети;

• блок разрешения инициации исходящих соединений, он обеспечивает функцию доступа пакетов данных в шлюзовую систему и из неё.

Универсальные системы защиты экономической информации часто используют с помощью серверов безопасности. Эти системы более компактны, чем система, разрабатываемая нами. Универсальную систему можно разместить на одном сервере. Однако такое решение, несмотря на свою компактность, является дорогостоящим, так как необходимо использовать особый компъютор-сервер, который следует оснащать: двумя системами электропитания (основной и дублирующей); специализированной материнской платой, рассчитанной на два серверных процессора с расширенным количеством гнёзд для оперативной памяти, чтобы обеспечить повышенную производительность, и несколькими жёсткими дисками, объединенными в специальный массив для защиты от потери большого объёма данных. Помимо этого в нём присутствует большое количество охлаждающих элементов для обеспечения защиты от перегрева и повышения отказоустойчивости сервера. Все эти компоненты заключены в корпус с повышенной защитой от электромагнитного излучения. Перечисленные компоненты не только значительно удорожают создаваемую систему защиты, но и требуют специальных обученных кадров для их установки и эксплуатации. Это тоже повышает стоимость

такой системы. Кроме того, в таких системах защиты информации необходимо использование специальной серверной операционной системы или дополнительных программных надстроек (их стоимость от шестидесяти тыс. рублей и выше в зависимости от комплектации). Необходимо также приобретение брандмауэра для обеспечения функции фильтрации исходящих и входящих пакетов данных, что тоже обычно требует дополнительных финансовых затрат, как и установка, настройка и эксплуатация готовой системы безопасности.

Предлагаемый нами комплекс обладает большими размерами, так как использует четыре пользовательских компьютера, но при этом затраты на их приобретение в 3–3,5 раза ниже, чем в предыдущем варианте. Этого удаётся добиться, используя бесплатную операционную систему Linux. Использование одного пользовательского компьютера в качестве сервера принципиально возможно, но такое решение не обеспечивает необходимые производительность и отказоустойчивость, поэтому возникает необходимость разделения серверных функций между несколькими ПК. При этом реализуется такой важный принцип построения систем защиты, как модульность, которая позволяет добиться низких трудозатрат при модернизации отдельных компонентов программы, поскольку они расположены на разных ПК и имеют мало цепей взаимодействия. Также появляется возможность модернизации компонент аппаратной части системы за счёт реализации в системе принципа открытой архитектуры. Нововведением является использование компьютера-терминатора для заглушки всех несанкционированных пакетов данных, что напрямую повышает безопасность защищаемой экономической информации за счёт увеличения отказоустойчивости брандмауэра и понижает риск взлома защищаемой ЛВС предприятия.

В результате внедрения данного комплекса предполагается улучшить защиту информации, хранимой, обрабатываемой и передаваемой по локальной вычислительной сети предприятия торговли. Внедрение данного комплекса позволит не только защитить экономическую информацию от несанкционированного доступа, а ещё и своевременно выявлять ПЭВМ, заражённые вирусами, внутри клиентской сети и отслеживать первичные адреса злоумышленников.

Таким образом, предлагаемая система обеспечит высокий уровень отказоустойчивости корпоративной сети, повысит уровень информационной безопасности сети передачи данных и её управляемость, обеспечит возможность дальнейшего наращивания ёмкости сети без значительных дополнительных капиталовложений.

Литература

1. Воронцова Г.А. Защита информации: экономические и правовые вопросы // T-Comm. 2010. № 12. С. 68–69.
2. Ясенев В.Н. Защита информации в экономических системах // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Экономика и финансы. 2001. № 1. С. 210–216.
3. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации / под ред. А.П. Пятибратова. М.: Финансы и статистика, 2004. 512 с.