УДК 004.722

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ НА МАЛОМ ПРЕДПРИЯТИИ

Д.Е. Жукова kliotimpatra@mail.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Проанализированы и систематизированы основные виды угроз информационной безопасности локальных сетей, в том числе на малых предприятиях. Рассмотрены способы и методы защиты информации в компьютерных сетях

Ключевые слова

Безопасность, локальная сеть, пользователь, злоумышленник, атака

Поступила в редакцию 23.09.2016

Введение. В жизни человека компьютеры появились сравнительно недавно. Но уже сегодня они стали обязательными и незаменимыми для большинства предприятий, офисов и частных пользователей. Компьютеры активно используют во всех сферах деятельности, тем самым стимулируя разработку различных видов программного обеспечения (ПО).

Причиной интенсивного развития информационных технологий является возрастающая потребность в быстрой и качественной обработке информации. Объединение компьютеров в сети позволило значительно повысить производительность труда. В настоящее время локальные вычислительные сети (ЛВС) получили широкое распространение, и теперь в некоторых сферах деятельности невозможно обойтись без ЛВС (банковское дело, складские операции крупных компаний, электронные архивы библиотек и др.). В этих сферах каждая отдельно взятая рабочая станция не может хранить всей информации (в основном, по причине слишком большого ее объема). Сеть позволяет зарегистрированным на файл-сервере пользователям получать доступ к той информации, к которой их допускает оператор сети. Кроме того, основной областью применения локальных сетей является автоматизация:

– административной управленческой деятельности, организация «электронных офисов», где вместо бумажного документооборота используют электронную почту;

– производства, т. е. автоматизация технологических процессов, информационное обеспечение оперативного управления производством, планово-экономическое управление производством;

– научных исследований и разработок;

– обучения, подготовки и переподготовки кадров;

– учрежденческой деятельности и т. д.

Вследствие интенсивного развития компьютерной техники и систем передачи информации, все более актуальной становится проблема обеспечения безопасности

информации. Под угрозой безопасности информации понимают действие или событие, которое может привести к разрушению, искажению или несанкционированному (неразрешенному) использованию информационных ресурсов. Безопасностью информации называют состояние, при котором информационным ресурсам не угрожает опасность [1–3].

Актуальность проблемы обеспечения безопасности локальных сетей объясняется тем, что изменения, происходящие в экономической жизни нашей страны — создание финансово-кредитной системы, предприятий различных форм собственности и т. п. — оказывают заметное влияние на вопросы защиты информации. Долгое время в России существовала только одна форма собственности — государственная. Поэтому информация и секретные данные были тоже только государственными. Проблемы информационной безопасности усугубляются по мере проникновения во все сферы деятельности технических средств обработки и передачи данных, и прежде всего вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, ПО и базы данных, для которых технические средства являются окружением. Каждый сбой в работе компьютерной сети — это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, «безбумажного» документооборота и других, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что приведет к ощутимым материальным потерям. Неслучайно, защита данных в компьютерных сетях становится одной из самых острых проблем в современном мире.

В настоящее время сформулированы базовые принципы информационной безопасности, которые должны обеспечить:

– целостность данных;

– защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

– конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Угрозы безопасности информации могут быть случайными (непреднамеренными) — это угрозы, источником которых являются ошибки в ПО, выход из строя аппаратных средств, неправильные действия пользователей и проч., и умышленными, цель которых нанесение ущерба (например, получение информации, циркулирующей в каналах связи, посредством их прослушивания, вывод из строя компьютерной техники, искажение информации в базах данных и др.).

Обеспечение безопасности необходимо для любых организаций независимо от размеров и форм их деятельности, но уязвимыми чаще являются малые предприятия, связанные локальными информационными сетями. Поэтому защиту и контроль необходимо обеспечить на всех уровнях: физическом, программном, пользовательском и внешнем.

Основные технические угрозы безопасности ЛВС на малом предприятии

1. Ошибки в ПО. Источниками ошибок в ПО является работа конкретных людей, с их индивидуальными особенностями, квалификацией и т. п. Большинство ошибок не представляет никакой опасности, однако некоторые могут привести к серьезным последствиям таким, как получение злоумышленником контроля над сервером, несанкционированное использование ресурсов. Такие «уязвимости» устраняют с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка обновлений является необходимым условием безопасности сети.

2. DoS и DDoS-атаки. Атаки отказа в обслуживании DoS направляются обычно на информационные серверы предприятия, функционирование которых является критически важным условием для работоспособности всего предприятия. Для проведения таких атак злоумышленники координируют работу нескольких рабочих станций, в этом случае возможна и DDoS атака — рапределенная атака в отказе обслуживания. Злоумышленник захватывает управление над группой удаленных компьютеров, посылает мощный суммарный поток пакетов в атакуемый компьютер, вызывая его перегрузку, в результате чего происходит исчерпывание ресурсов операционной системы или процессора компьютера.

3. Вредоносные программы («троянский конь», «черви», компьютерные вирусы). Ущерб, наносимый вредоносными программами, может выражаться в хищении, искажении, уничтожении информации, а также приведение в нерабочее состояние ПО. Троянские программы выглядят как полезные приложения, но при установке или открытии файла заполняют рабочую станцию. Сетевые «черви» способны самостоятельно распространяться по локальной сети и глобальным сетям путем распространения своих копий. Вирусы внедряются в разные типы файлов, не изменяя размер самого файла [4].

С целью обеспечения безопасности отдельных компьютеров и локальной сети применяют:

1) антивирусную защиту, в основе работы которой три группы методов:

• методы анализа содержимого файлов — сканирование сигнатур (уникальная последовательность байтов, которая всегда присутствует в определенном виде вирусов и по которой этот вид вируса можно с большой вероятностью опознать) вирусов, а также проверка целостности и сканирование подозрительных команд. Для каждого вируса специалист выполняет анализ кода, на основании которого требуется сигнатура. Полученный кодовый фрагмент помещают в базу данных вирусных сигнатур. Далее работает антивирусная программа, которая будет сканировать файлы на наличие вирусов и, в случае обнаружения опасности, заблокирует файл (временно зашифрует зараженный файл);

• методы, отслеживающие проведение программ при их выполнении — протоколирование всех событий, угрожающих безопасности системы;

• регламентация порядка работы с файлами и программами — в системе корпоративной сети выполняются только те программы, запись о которых присутствует в списке программ, разрешенных к выполнению в данной системе. Этот список формирует администратор сети из проверенного ПО;

2) для доступа в Интернет прокси-серверы, на которых установлено антивирусное ПО;

3) серверную фильтрацию электронной почты, приходящей в локальную сеть на предмет наличия спама и активного содержимого;

4) запрет автоматического просмотра активного содержимого вложений в электронную почту;

5) запрет передачи и получения исполняемых файлов (программ и скриптов) по каналам электронной почты в открытом виде.

Общие принципы обеспечения безопасности

1. Сетевое оборудование, выполняющее маршрутизацию трафика в сеть Интернет должно быть оснащено системой фильтрации трафика с запретами по умолчанию.

2. Локальная сеть должна иметь минимальное количество глобальных адресов.

3. Весь трафик должен быть получен с использованием кэширования информации посредством прокси-серверов.

4. Прокси-сервер должен иметь настроенные Access Control List.

5. На прокси-сервере должно быть установлено антивирусное ПО, запрещающее доступ к потенциально опасным источникам.

6. Прямой доступ к сети Интернет с использованием механизма трансляции сетевых адресов (NAT) может быть включен только для ограниченного числа пользователей, чтобы предотвратить обращения извне к внутренним хостам. ПО для просмотра информации по http-протоколу должно использовать максимальный уровень безопасности и предупреждать пользователя обо всех потенциально небезопасных действиях.

7. В сети, имеющей выход в Интернет, должна быть разработана политика автоматической установки всех дополнений и исправлений, выпускаемых поставщиком операционной системы. Установка обновлений и дополнений должна выполняться для всех компьютеров сети, вне зависимости от прав пользователя компьютера на получение доступа к сети Интернет.

8. Все сетевые компьютеры должны быть оснащены антивирусным ПО. Обновление антивирусного ПО должно выполняться ежедневно в определенное время.

9. Для компьютеров, использующих прямой выход в Интернет следует уменьшить до минимума число одновременных подключений.

10. Для всех, без исключения, пользователей должна быть запрещена установка нового ПО [5].

Угрозы по причине человеческого фактора

1. Уволенные или недовольные сотрудники: данная категория людей наиболее опасна, так как многие из таких сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы. Они оставляют «черные ходы» для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д. [6].

2. Промышленный шпионаж. Форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получения преимуществ при осуществлении предпринимательской деятельности, а равно получения материальной выгоды. В основном защита осуществляется с помощью охранной системы.

3. Недостаточная квалификация сотрудника при работе с локальной сетью может привести к ряду ошибок. Например, позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть.

Для предотвращения обозначенных угроз необходимо:

- предусмотреть наличие единой системы аутентификации пользователей, на основе дерева каталогов. Это может быть любая из систем, например, Microsoft Active Directory, Novell NDS, Система OpenLDAP (Linux);
- обеспечить хранение учетной информации пользователей в зашифрованном виде;
- отказаться от протоколов передачи пароля в незашифрованном виде;
- разработать политику периодической замены паролей пользователями;
- выработать требования к обязательному составу паролей пользователей;
- вести учет входов в сеть пользователями;
- разработать систему предоставления прав использования ресурсов сети пользователям на основе групп безопасности;
- запретить использование пользователями компьютеров с правами администратора;
- разработать меры безопасности, предотвращающие использование сменных носителей пользователями.

Таким образом, чтобы минимизировать риск перечисленных выше факторов, необходимо провести ряд мероприятий при проектировании и вводе в эксплуатацию ЛВС.

1) Разработать систему периодического резервного копирования информации серверов на сменные носители.

2) Предусмотреть наличие в сети выделенного сервера, выполняющего резервирование информации. На нем должна быть установлена серверная часть ПО резервного копирования.

3) На всех серверах системы, включенных в план резервного копирования установить программное обеспечение, выполняющее функции агента системы резервного копирования.

4) Обеспечить автоматическое выполнение резервного копирования по расписанию.

5) Ограничить удаленный доступ к системе резервного копирования компьютером администратора.

6) Разработать систему мониторинга состояния ключевых элементов сети и оповещения администратора сети о потенциальных проблемах. В крупных сетях эту функцию необходимо возложить на отдельный сервер, поскольку объем информации мониторинга может достигать внушительных значений.

7) Предусмотреть использование терминального клиент-серверного режима для работы с корпоративными приложениями там, где это возможно. Это избавит от необходимости поддержания целостности данных на множестве компьютеров, уменьшит объемы резервного копирования информации, в некоторых случаях позволит использовать бездисковые рабочие станции.

8) Отключить функции автоматического просмотра содержимого сменного носителя на всех машинах, входящих в сеть.

Выводы. Обеспечение безопасности информации локальных сетей на малом предприятии — это комплекс мероприятий, направленных на предотвращение несанкционированного получения информации, ее физического уничтожения, а также модификации (видоизменения) защищаемой информации. Использование этих мероприятий поможет малым предприятиям успешно развиваться, сохранить свое ноу-хау, быть конкурентоспособными и финансово стабильными.

Литература

1. *Андерсон К.*, *Минаси М.* Локальные сети. Полное руководство. СПб.: Корона принт, 1999. 624 с.

2. *Борисенко А.А.* Локальная сеть. Просто как дважды два. М.: Эксмо, 2007. 160 с.

3. *Ватаманюк А.* Создание, обслуживание и администрирование сетей на 100 %. СПб.: Питер, 2010. 523 с.

4. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2010. 918 с.

5. *Базовые* принципы обеспечения безопасности ЛВС // RuView. URL: http://www.ruview.ru/downloads/netsecurity.pdf (дата доступа: 11.04.2016).

6. *Зараковский Г.М., Смолян Г.Л.* Информационно-психологическая безопасность: основные понятия // Психология и безопасность организаций. М.: ИП РАН, 1997. С. 40–44.

Жукова Дарья Евгеньевна — магистрант кафедры «Системы обработки информации и управления», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Г.И. Ревунков, канд. техн. наук, доцент кафедры «Системы обработки информации и управления», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

ENSURING LOCAL AREA NETWORK SECURITY FOR SMALL BUSINESSES

D.E. Zhukova kliotimpatra@mail.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

We analysed and classified primary threat types concerning information security in local area networks, including those of small businesses. We discuss techniques and methods for information protection in computer networks

Keywords

Security, local area network, user, intruder, attack

References

[1] Anderson C., Minasi M. Mastering local area networks. 1999, Sybex. 751 p. (Russ. ed.: Lokal'nye seti. Polnoe rukovodstvo. Sankt-Petersburg, Korona print Publ., 1999. 624 p.)

[2] Borisenko A.A. Lokal'naya set'. Prosto kak dvazhdy dva [Local network. As simple as ABC]. Moscow, Eksmo Publ., 2007. 160 p. (in Russ.).

[3] Vatamanyuk A. Sozdanie, obsluzhivanie i administrirovanie setey na 100 % [100% network creation, maintenance and administration]. Sankt-Petersburg, Piter Publ., 2010. 523 p. (in Russ.).

[4] Olifer N., Olifer V. Computer networks: principles, technologies and protocols for network design. Wiley, 2005. (Russ. ed.: Komp'yuternye seti. Printsipy, tekhnologii, protokoly. Sankt-Petersburg, Piter Publ., 2010. 918 p.)

[5] Bazovye printsipy obespecheniya bezopasnosti LVS [Basic principles of LAN security]. *RuView*. URL: http://www.ruview.ru/downloads/netsecurity.pdf (accessed 11.04.2016).

[6] Zarakovskiy G.M., Smolyan G.L. Informatsionno-psikhologicheskaya bezopasnost': osnovnye ponyatiya. *Psikhologiya i bezopasnost' organizatsiy* [Information-psychological security: basic terms. In: organization psyhology and security]. Moscow, IP RAN Publ., 1997. P. 40–44 (in Russ.).

Zhukova D.E. — graduate student of Information Processing and Control Systems Department, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — G.I. Revunkov, Cand. Sci. (Eng.), Assoc.Professor of Information Processing and Control Systems Department, Bauman Moscow State Technical University, Moscow, Russian Federation.