УДК 004.7+004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Х. Чжэнце
Магистрантка кафедры проектирование информационных компьютерных систем БГУИР

Ж. Сюньхуань
Магистрантка кафедры проектирование информационных компьютерных систем БГУИР

Н.Л. Шенец
Учитель ГУО «Гимназия №17 г. Минска»

Л.П. Пилиневич
Профессор кафедры инженерной психологии и эргономики БГУИР, доктор технических наук, профессор

Л.В. Жавнерчик
Магистрантка кафедры инженерной психологии и эргономики БГУИР

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь
Государственное учреждение образования «Гимназия №17 г.Минска», Республика Беларусь
E-mail: Pilinevich@bsuir.by, snl1276@gmail.com

Аннотация. В данной работе рассмотрены основные причины и угрозы нарушения безопасности локальных вычислительных сетей, а также методы и средства обеспечения безопасности в локально вычислительных сетях. Показано, что обеспечить информационную защиту с наибольшей вероятностью возможно только применив комплексный подход.

Ключевые слова: сеть, информационная безопасность, защита, угрозы, человеческий фактор, вирус, информация.

Локальная вычислительная сеть (ЛВС) — это совокупность аппаратного и программного обеспечения, объединенные в единую распределенную систему получения, передачи, обработки и хранения информации. К аппаратному обеспечению можно отнести компьютеры, с установленными на них сетевыми адаптерами, повторители, концентраторы, коммутаторы, мосты, маршрутизаторы и др., соединенные между собой каналами связи (сетевыми кабелями или радиоканалами).

К программному обеспечению можно отнести сетевые операционные системы и протоколы передачи информации. Назначение локальной вычислительной сети – создание единого информационного пространства организации.

Сегодня благополучие многих организаций зависит не только от мгновенного получения

необходимой информации и скорости ее обработки, но и от обеспечения информационной безопасности систем обработки и хранения информации, а также систем контроля и управления различными объектами. Для нормального и безопасного функционирования информационных систем необходимо поддерживать их безопасность и целостность, т.е. необходимо применять специальные средства и методы предотвращения искажения и утери информации, находящейся в локальных вычислительных сетях (ЛВС). Широкое распространение и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации.

Основными угрозами информационной безопасности ЛВС являются: стихийные бедствия и аварии, сбои и отказы оборудования (ошибки при проектировании и разработке аппаратных средств, технологий обработки информации, программ и т.п.), ошибки при эксплуатации и преднамеренные действия нарушителей и злоумышленников.

Целью данной работы является определение основных факторов нарушения информационной безопасности в локальных вычислительных сетях, а также методов и средств их устранения.

В настоящее время определились три основные аспекта уязвимости информации:

- подверженность физическому уничтожению или искажению;
- возможность несанкционированного изменения;
- несанкционированное получение информации лицами, для которых она не предназначена.

Исходя из вышеуказанных угроз основными задачами обеспечения безопасности локальных вычислительных сетей являются:

- обеспечение сохранности целостности информационных данных;
- обеспечение конфиденциальности данных;
- обеспечение безопасного доступа к данным.

Существуют два основных вида угроз нарушения безопасности локальных вычислительных сетей, это технические угрозы и человеческий фактор [1]. К техническим угрозам можно отнести: ошибки в программном обеспечении, компьютерные вирусы, различные DoS- и DDoS-атаки, снифферы, устройства съема информации и др. К человеческому фактору относятся: недовольные уволенные или работающие сотрудники, промышленный шпионаж, халатность или низкая квалификация сотрудников, а также не знание или не соблюдение правил и инструкций по обеспечению политики информационной безопасности. Рассмотрим каждый вид угроз более подробно и определим рекомендации их устранения.

Технические угрозы.

1.Ошибки в программном обеспечении. Программное обеспечение информационной безопасности включает программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. [2]. Ошибки в программном обеспечении могут привести к различным негативным последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособности сервера, несанкционированному использованию ресурсов и др. Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО, поэтому своевременная установка обновлений является необходимым условием для устранения данных угроз сети. Кроме того, необходима идентификация каждого пользователя, запрещается разглашение параметров доступа к любым корпоративным сервисам, а также необходимы ограничения полномочий конечного пользователя для исключения возможности сознательного запуска или установки не предусмотренных служебными обязанностями программ [3].

2. Компьютерные вирусы. Компьютерные вирусы - программы, которые создаются специально для нанесения ущерба пользователям ПК, они могут рождаются, размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков и др. Активизация вируса

может вызвать уничтожение программ и данных. В ЛВС компьютерный вирус наиболее часто использует для своего распространения электронную почту или уязвимости в программном обеспечении.

Методов борьбы с вирусами достаточно много, одним из них является своевременная установка обновлений [4]. Обнаружение зараженных вирусами файлов и дисков, а также уничтожение обнаруженных вирусов на каждом компьютере позволяет избежать распространения вирусной эпидемии на другие компьютеры ЛВС. Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Известны следующие виды антивирусных программ: антивирусные сканеры, программы-доктора или фаги, программы-ревизоры, программы-фильтры.

Антивирусные сканеры – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса.

Программы-доктора или фаги находят зараженные вирусами файлы и «лечат» их, возвращая файлы в исходное состояние. Среди фагов выделяют полифаги – самые универсальные и эффективные антивирусные программы, они проверяют файлы, загрузочные сектора дисков и оперативной памяти на поиск новых и неизвестных вирусов.

Программы-ревизоры запоминают исходное состояние программ, каталогов и системных областей диска, а затем периодически сравнивают текущее состояние с исходным. При сравнении проверяются длина файла, код циклического контроля, дата и время модификации.

Программы-фильтры предназначены для обнаружения подозрительных действий при работе компьютера, характерных для вирусов, например, изменение атрибутов файла, загрузка резидентной программы и др. При обнаружении таких действий программа-фильтр посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Рекомендуется не запускать файлы сомнительного источника без предварительной проверки их антивирусными программами.

3. DoS- и DDoS-атаки. Denial Of Service (отказ в обслуживании) — агрессивное внешнее воздействие на вычислительные ресурсы сервера или рабочей станции, предназначенное для выведения сети или сервера из работоспособного состояния. При DoS-атаках (атака проводится с одиночного компьютера) могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). DDoS-атаки (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Принцип действия DoS и DDoS-атак заключается в отправке на сервер большого потока информации, который загружает вычислительные ресурсы процессора, оперативной памяти, забивает каналы связи или заполняет дисковое пространство. Атакованные вычислительные ресурсы сервера или рабочей станции не справляются с обработкой поступающих данных и перестают откликаться на запросы пользователей.

Безопасность рабочих станций обеспечивают межсетевой экран и антивирус, а также локальные и доменные настройки, политики информационной безопасности, ограничивающие влияние пользователя на критичные (для безопасности) параметры системы. Также необходима оперативная установка обновлений, выпускаемых производителем ОС и разработчиками приложений, предназначенных для работы в Глобальной сети.

4. Снифферы. Сниффинг (Sniffing) - это перехват передаваемых по сети данных. В локальной сети перехватчиком может быть любой узел сети, в интернет – провайдер. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому.

При передаче данных по глобальным сетям эта проблема встает наиболее остро, поэтому необходима защита локальной сети от внешнего доступа, например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным. Обеспечить ограничение доступа из локальной сети к внешней, например, можно запретить доступ к интернету каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, а также ограничить доступ к сети неавторизированным пользователям и случайным людям.

5. Устройства съема информации. Устройствами съема информации называются скрытно внедряемые в места возможного съема информации малогабаритные электронные устройства, предназначенные для несанкционированного съема информации [5]. В зависимости от вида информации, перехватываемой устройствами съема информации, последние можно разделить на акустические, телефонные и аппаратные закладки, а также закладные телевизионные системы. Данный вид угроз используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим, поэтому основным мероприятием защиты от данного вида угроз является ограничение доступа посторонних лиц к возможным местам съема информации и шифрование информации. При передаче данных по сети немаловажным аспектом является шифрование трафика, так как для перехвата передаваемой информации не нужно физическое воздействие, а достаточно просто подключиться к сети и, «подслушивая» канал, перехватывать информацию. На данный момент существуют несколько видов шифрования: WEP, WPA, WPA-PSK, WPA2 и др. [6].

Человеческий фактор. Теоретические и практические вопросы обеспечения информационной безопасности с учетом аспектов человеческого фактора подробно описаны В.В. Гафнером [7].

Нарушителей информационной безопасности ЛВС могут быть две категории: внутренние (из числа сотрудников) и внешние (посторонние лица).

Внутренними нарушителями могут быть один или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации. Ими могут быть: пользователи ЛВС; персонал, обслуживающий технические средства (инженеры, техники); сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты); технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие, имеющие доступ в здания и помещения, где расположены компоненты ЛВС); сотрудники службы безопасности предприятия и др.

Внешними нарушителями могут быть: клиенты (представители организаций, граждане); посетители (приглашенные по какому-либо поводу); сотрудники организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; сотрудники конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию и др.

Большинство нарушений информационной безопасности ЛВС предприятия связаны, как правило, с действиями сотрудников этого предприятия. В классификации внутренних угроз в первую очередь можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности.

Нарушителями информационной безопасности ЛВС предприятия, совершившими утечку конфиденциальных данных или ценной информации из корыстных или других злонамеренных целей могут быть: сотрудники, затаившие злобу или обиду, причиной для которой может низкая заработная плата, понижения в должности, различные наказания за нарушения должностных обязанностей и др.; сотрудники, использующие секретные информационные ресурсы предприятия для собственной выгоды, например, интеллектуальную собственность

предприятия, коммерческую тайну и др.; завербованные сотрудники или специально внедренные конкурентами или иностранными спецслужбами.

Нарушения информационной безопасности ЛВС предприятия, совершаемые без злого умысла, по неосторожности, халатности или технической некомпетентности являются наиболее распространенными и наиболее часто совершаемыми. Нарушения информационной безопасности могут происходить из-за не установленных вовремя обновлений, запуска исполняемых файлов и скриптов, неизмененных настроек «по умолчанию», ошибок ввода данных при работе с локальными сетями или интернетом до утери носителя информации (USB-накопитель, оптический диск), пересылки данных по незащищённым каналам связи до непредумышленной загрузки вирусов с развлекательных веб-сайтов. Часто сотрудники, нарушают политику безопасности, используя флеш-устройства или просматривая разные сайты в рабочее время, открывая почту от неизвестных отправителей и пр., тем самым способствуют проникновению вредоносных вирусов в ЛВС предприятия.

Аналитический центр Falcongaze определил признаки, согласно которым необходимо уделять внимание вопросом защиты от утечек информации - это отсутствие корпоративной политики безопасности, высокая ротация кадров и частые сокращения, неконтролируемое использование сотрудниками мессенджеров, электронной почты, наличие сотрудников, много времени проводящих в деловых поездках и командировках, неконтролируемый документооборот, вследствие чего доступ к конфиденциальным сведениям может получить кто угодно.

Для защиты локальной сети от данного вида угроз необходимо на компьютеры, подключенные к сети Интернет установить все исправления безопасности, как для операционной системы, так и для всех используемых программ, обеспечить ограничение внешнего доступа, например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным. Ограничение доступа из локальной сети к внешней, например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета локальным пользователям, фильтровать вирусы. Пользователи данного компьютера должны иметь доступ только к тем локальным и сете- вым ресурсам, которые им необходимы для выполнения рабочих обязанностей. Защита от внутренних угроз также требует комплексного подхода. Он заключается в разработке и принятии политик информационной безопасности, назначении ответственных за информационную безопасность сотрудников, контроле документооборота, контроле и мониторинге пользователей, введении механизмов аутентификации для доступа к информации разной степени важности, введении функционала защиты от утечек данных, обучении пользователей, создании соответствующих документов и повышении квалификации сотрудников в области информационной безопасности. Необходимо также отметить, существенно влияет на уровень информационной безопасности наличие централизованного управления антивирусной защитой сети. Внедрение системы централизованного управления позволяет создавать различные настройки для различных групп пользователей без необходимости настройки защиты на каждый конкретной компьютер, а также гарантировать, что антивирус на каждой рабочей станции не отключен и работает именно с теми настройками, которые задал администратор сети. Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении необходимо производить в автоматизированном режиме.

Согласно политики обеспечения информационной безопасности определены правила использования информационными ресурсами ЛВС [8].

1. Пользователь информационных ресурсов ЛВС обязан:

1.1. Использовать ресурсы ЛВС для служебных целей.

1.2. Знать и помнить имя компьютера, персональный логин и пароль (выдается памятка).

1.3. По требованию системного администратора производить выход из баз данных

вплоть до полного отключения от сети.

1.4. При смене должности, рабочего места или уровня доступа к информации немедленно сообщать администратору ЛВС.

1.5. Иметь пароль, соответствующий требованиям информационной безопасности.

1.6. Сообщать о любых случаях использования другими пользователями ресурсов ЛВС в личных, не связанных с производственной деятельностью, целях.

1.7. Сохранять рабочую документацию (письма и т.д.) на сетевом диске.

2. Пользователю информационных ресурсов ЛВС запрещается:

2.1. Без согласования с системным администратором подключать к ЛВС любые устройства (компьютеры, принтеры, концентраторы и т.д.).

2.2. Использовать предоставляемые ресурсы ЛВС для хранения развлекательной информации, такой как: игры, картинки, музыку и др., не связанное с производственной необходимостью.

2.3. Самостоятельно изменять настройки компьютера, подключенного к ЛВС (имя компьютера, IP- адрес, сетевые службы и протоколы и др.).

2.4. Открывать для общего доступа любые ресурсы закрепленного за пользователем компьютера.

2.5. Применять к информации, хранящейся в ЛВС, любые методы шифрования данных.

2.6. Хранить персональный пароль на любых материальных носителях и в электронном виде (бумага, диски компьютера и т.д.), сообщать кому- либо свой пароль.

2.7. Хранить личную информацию (фотографии, видео и т.д.) на ЛВС.

3. Особые условия

3.1. В случае, не соблюдения правил использования информационных ресурсов ЛВС пользователь может быть отключен от ЛВС без предварительного уведомления.

3.2. Повторное подключение пользователя к информационным ресурсам ЛВС производится после предварительного предоставления пользователем объяснительной на имя директора компании.

Для защиты информации, циркулирующей в локальной сети можно применить криптографические методы, например, шифрование информации и электронную цифровую подпись. Сегодня многие компании, специализирующиеся на решениях защиты информационных систем, предлагают средства контроля и управления доступом в корпоративную сеть с автоматизированных рабочих мест сотрудников компании на основе решения Cisco Network Admission Control (CNAC). Решение CNAC интересно, прежде всего, крупным организациям, со сложной инфраструктурой, объединяющей сотни компьютеров сотрудников, и с политикой безопасности, предусматривающей работу в корпоративной сети «мобильных» пользователей.

Список литературы

[1]. Алексеева М. С., Иванова Е. В. Угрозы безопасности локальных вычислительных сетей // Молодой ученый. — 2014. — №18. — С. 212-213.

[2]. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008. - 274 с.

[3]. Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб: Питер, 2008. - 358 с.

[4]. Безручко, В. Т. Информатика (курс лекций): учеб. пособие / В. Т Безручко. - М.: Инфра-М : Форум, 2009. - 432 с.

[5]. Хорев А.А. Техническая защита информации/ учеб. пособие для студентов вузов/ в 3-х томах. − т. 1: Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.

[6]. Шатдинов Р. С., Утопленников Д. С., Насретдинова Д. Р. Угрозы безопасности информации при работе в открытых беспроводных сетях Wi-Fi [Текст] // Современные тенденции технических наук: материалы II Междунар. науч. конф.— Уфа: Лето, 2013. — С. 16-19.

[7]. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. - 324 с.

[8]. SecurityPolicy.ru - Документы по информационной безопасности | 2009-2017 | feedback@securitypolicy.ru.

INFORMATIONAL SECURITY OF LOCAL COMPUTING NETWORK

X. ZHENGJIE
Master of information Systems Design Department of BSUIR

R. XUNHUAN
Master of information Systems Design Department of BSUIR

N.L SHENEC
Teacher of the state institution of education Gymnasium No. 17

L.P. PILINEVICH,
Doctor of Engineering Sciences
Professor of department of engineering psychology and ergonomics of BSUIR, professor

L.V. ZHAVNERCHIK
Master student of department of Human Engineering and Ergonomics of BSUIR

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus
State Institution of Education "Gymnasium No. 17 in Minsk", Republic of Belarus
E-mail: Pilinevich@bsuir.by, snl1276@gmail.com

Abstract. In this paper, we consider the main causes and threats of security breaches of local computer networks, and also methods and means of providing security in local area networks. It is shown that it is possible to provide information protection with the greatest probability only by applying a complex approach.

Key words: Network, informational security, protection, threats, human factor, virus, information.