УДК 339:004.738.5

Т. А. Заяц (za-t-a@yandex.ru),
старший преподаватель
Белорусского торгово-экономического
университета потребительской кооперации

ОРГАНИЗАЦИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИЗНЕСЕ

В статье дается классификация угроз информационной безопасности, приводится статистика правонарушений в сфере информационных технологий, рассматриваются актуальные вопросы формирования системы информационной безопасности на предприятиях Республики Беларусь.

The article provides the classification of information security threats, presents the statistics of offenses in the sphere of information technologies, deals with topical issues of formation of the information security system of Belarusian enterprises.

Ключевые слова: угроза информационной безопасности; информационная система; система информационной безопасности; информационная защита; политика безопасности; источники угроз информационной безопасности.

Key words: information security threat; information system; information security system; information security; security policy; the sources of information security threats.

Введение

В современных условиях предприятия стремятся использовать передовые информационные технологии для достижения успеха в своей деятельности. С их внедрением значительно упрощается процесс обработки больших объемов данных, предоставляется возможность быстро реагировать на изменения в микро- и макросреде предприятия, осуществлять бизнес-планирование.

Однако концентрация всех экономических данных и ресурсов в единой автоматизированной информационной системе имеет некоторые отрицательные последствия: возрастает вероятность утечки корпоративной информации из-за различного рода угроз информационной безопасности.

Защита информации представляет собой деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию; это процесс, направленный на достижение состояния защищенности информационной среды.

В соответствии с признаками классификации выделяют следующие угрозы информационной безопасности (ИБ):

1. По объекту информационной безопасности, на который направлены угрозы:
- угрозы конфиденциальности (неправомерный доступ к информации);
- угрозы целостности (неправомерное изменение данных);
- угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

2. По расположению источника угроз:
- внешние (несанкционированный доступ к информации, ввод в программные продукты и проекты «логических бомб», разработка и распространение вирусов, компрометация электронных подписей, перехват информации);
- внутренние (преднамеренные действия и непреднамеренные ошибки персонала, отказы технических средств, сбои программного обеспечения).

3. По характеру происхождения угроз:
- стихийные (пожары, землетрясения, наводнения, ураганы);
- антропогенные (хакеры, персонал, представители служб защиты);
- техногенные (средства связи, некачественные технические и программные средства обработки информации).

Проблема обеспечения информационной безопасности становится одной из важнейших задач в работе предприятий. В связи с отсутствием (или недостаточным количеством) квалифицированного

персонала и экономией (отсутствием) финансовых средств, необходимых для разработки и внедрения комплексной системы информационной безопасности, предприятиям малого и среднего бизнеса довольно сложно противостоять основным угрозам без помощи специальных технических средств и соответствующего программного обеспечения. Пренебрежение проблемой информационной защиты может привести к серьезным последствиям, вплоть до остановки деятельности предприятия вследствие финансовых потерь, сорванных сделок и утраты конфиденциальности коммерческой информации.

По данным источника [1] в 2014 году в Республике Беларусь было выявлено 8 тыс. 739 компьютерных преступлений, из которых было раскрыто 96%.

За первое полугодие 2015 года в Беларуси выявили 4 295 преступлений в сфере высоких технологий. Злоумышленники, действующие в «компьютерной» сфере криминала, – это молодые люди в возрасте до 18 лет, 58% – от 18 до 25 лет, причем около 70% из них имеют высшее либо незаконченное высшее образование.

Основная часть преступлений, с которыми приходится иметь дело, – это компьютерные преступления, связанные с незаконным доступом к информации и с использованием вредоносных программ. Было отмечено, что оперативные работники органов внутренних дел довольно успешно борются с подобными видами преступлений.

Согласно статистике процент раскрываемости противоправных действий в сфере высоких технологий составляет 96%. Самое громкое преступление, раскрытое «компьютерными» сыщиками, – поимка 7 хакеров, которые украли у 8 тыс. владельцев банковских пластиковых карт около 21 млн долл. США. На территории России проведена операция по задержанию группы хакеров, которые с использованием вредоносных программ осуществляли атаки на серверы банков и букмекерских компаний в Великобритании. Злоумышленники требовали у потерпевших за прекращение противоправных действий от 5 тыс. до 50 тыс. долл. США. В настоящее время находятся под арестом двое из подозреваемых. Им вменяется в вину 273 случая изготовления и распространения вредоносных компьютерных программ и 163 случая вымогательства [1].

Во избежание подобных ситуаций предприятия должны позаботиться о политике безопасности – разработке норм и правил, определяющих принятие в организацию мер по обеспечению безопасности информации, связанной с деятельностью организации. Только человек, четко осознающий цели организации и условия ее функционирования, может определить, какую информацию необходимо защищать и насколько существенными могут стать потери от несанкционированного распространения, искажения или разрушения информации.

При любом виде деятельности у каждой компании есть определенный набор сведений, которые являются основой существования фирмы. Эти сведения и связанный с ними документооборот являются коммерческой тайной компании, и, разумеется, требуют защиты от утечек и разглашения. Эффективная защита информации от утечек требует комплексного подхода. Для успешного построения системы информационной безопасности необходимы анализ и аудит всей информационной деятельности предприятия.

Предприятия должны позаботиться о следующих способах обеспечения информационной безопасности:

1. Использование межсетевого экрана (firewall-a).

Системы фильтрации пакетов данных не позволяют попадать в Интернет пакетам, передающимся по локальной сети, а также ограждают локальную сеть от попадания в нее некоторых пакетов данных из Интернета.

2. Защита электронной почты.

Антивирусная программа на корпоративном сервере электронной почты анализирует поток данных, проходящий через почтовые серверы, и не допускает передачи сообщений с зараженными файлами.

Программа – клиент электронной почты, предупреждающая о содержащемся в письме вирусе, может защитить от целого класса вредоносных программ.

3. Использование антивирусной защиты.

Файловая программа – антивирус блокирует заражение еще на этапе записи вредоносного кода на компьютер. Но даже, если компьютер уже содержит инфицированные файлы, они будут проверены и обезврежены при попытке запуска.

4. Совершенствование системы аутентификации пользователей.

Установка специального программного обеспечения, позволяющего хранить пароли в защищенной памяти электронных идентификаторов и в нужный момент извлекать их и предоставлять соответствующим системным или прикладным компонентам.

5. Шифрование данных.

Для защиты данных в процессе хранения от посторонних лиц необходимо шифровать данные, размещенные на жестких дисках, дисковых массивах и в хранилищах.

6. Использование систем, блокирующих порты персонального компьютера.

В зависимости от прав доступа пользователя, такие системы могут запретить использование внешних накопителей информации.

7. Ограничение доступа к оборудованию.

Необходимо по возможности переместить сетевое оборудование в запираемую комнату и выдать ключи только работающим с оборудованием сотрудникам.

8. Установление уровня полномочий.

Необходимо разграничить полномочия пользователей, предоставив им доступ только к конкретным программам.

9. Отключение сетевого доступа для бывших сотрудников. Предполагает исключение возможности входа в сеть бывших сотрудников.

10. Отказ от беспроводных сетей.

По возможности, стоит отказаться от использования беспроводных сетей, как более уязвимых по сравнению с проводными.

11. Подготовка и обучение персонала.

Периодически необходимо проводить семинары с сотрудниками, обсуждая основные правила информационной безопасности и возможные угрозы.

12. Внедрение DLP-системы.

DLP-система (Data Leak Prevention, система предотвращения утечек данных) – это комплекс программных или программно-аппаратных средств, предотвращающий утечки конфиденциальной информации за пределы предприятия.

Новое исследование компании *Spiceworks* [2] показало, что конечные пользователи внутри предприятия возглавили список угроз информационной безопасности. Это в очередной раз подчеркнуло необходимость выбора заказчиками решений по управлению и контролю данными. В рамках использования систем информационной безопасности было выявлено, что 80% предприятий имели серьезные проблемы с безопасностью в 2015 году.

Итоги доклада «Battling the Big Hack» [2] свидетельствуют о том, что самой существенной причиной активности инсайдеров и проникновений извне является недостаточная осведомленность и отсутствие бдительности конечных пользователей. Порядка 54% предприятий, участвующих в опросе, очень озабочены распространением вредоносных программ, которые им сложно отслеживать, 53% обеспокоены угрозами программ-вымогателей (например, вирусов-шифроваль-щиков, требующих деньги за дешифрацию данных), 46% – фишингом.

Только 18% компаний заявили, что у них не было обнаружено ни одной инсайдерской атаки за 2015 год.

Угрозы информационной безопасности по источникам распределились следующим образом: атаки инсайдеров (36%), организованных преступных группировок (25%), кибер-террори-стических групп (12%) и национальных/спонсируемых государством хакеров (12%).

Наиболее распространенные действия, которые предпринимаются в ходе инсайдерских атак, следующие: обновление аппаратного/программного обеспечения (76%), применение политики безопасности для конечных пользователей (73%), обучение конечных пользователей (72%).

К главным проблемам ИТ-безопасности относятся ограниченные знания в области рисков и безопасности конечными пользователями (69%), непринятие проблемы конечными пользователями, сопротивление (57%).

В настоящее время компаниями-разработчиками создаются программные комплексы, направленные на построение комплексной системы информационной безопасности. Например, компания *SafenSoft* предлагает сбалансированную защиту от утечки данных, разработанную специально для среднего и малого бизнеса. Программный комплекс строит защиту, которая не нарушает текущие алгоритмы документооборота в компании, но в то же время сохраняет информацию от неавторизованного доступа, копирования или изменения.

Не пустить лишних людей к важным данным, защитить информацию от взлома и заражения извне, исключить оплошности при работе с информацией, дать возможность полного контроля и

мониторинга действий сотрудников – по таким принципам созданы продукты для информационной безопасности бизнеса *SysWatchEnterpriseSuite* и *DLP Guard*. В них реализован весь необходимый перечень услуг по предотвращению утечек информации [3] и источников угрозы безопасности: ошибок пользователей и персонала; атак извне; обиженных или нечестных сотрудников; вирусов; проблем физической безопасности [4].

Также предотвратить и минимизировать утечки информации поможет DLP-система *SecureTower*. Она представляет собой программный продукт, позволяющий решить две основные задачи: обеспечивать защиту корпоративных данных от утечек и осуществлять мониторинг деятельности персонала на рабочих местах. Руководствуясь принципами комплексного подхода к вопросам защиты данных, SecureTower позволяет не только предотвратить утечки конфиденциальной информации, но и повысить эффективность работы всего предприятия в целом.

Контроль множества каналов коммуникации (мессенджеры, электронная почта, внешние устройства, принтеры и т. д.), подкрепленный функциональными возможностями для мониторинга сотрудников на рабочих местах, делают систему *SecureTower* незаменимым средством для обеспечения информационной безопасности предприятия.

Система контролирует следующие типы данных:

- электронные письма почтовых клиентов, использующих протоколы POP3, SMTP, IMAP, MAPI (например, MS Outlook, Thunderbird, The Bat!), электронная почта, защищенная по стандарту S/MIME, электронные сообщения MS Exchange Server, IBM Lotus Notes/Domino, Kerio Connect, Sendmail, hMailServer и многих других;
- веб-трафик, включая электронные письма внешних почтовых служб (gmail.com, mail.ru, rambler.ru и т. д.), сообщения на форумах и в блогах, трафик в социальных сетях и других веб-службах;
- почтовые сообщения, отправляемые и получаемые при помощи облачного сервиса Microsoft Office 365;
- сообщения в мессенджерах, использующих протоколы обмена мгновенными сообщениями OSCAR (ICQ/AIM), MMP (Mail.Ru Агент), MSN (Windows Messenger), XMPP (Jabber) (Miranda, Google Talk, QIP Infium, PSI), YIM (Yahoo! Messenger), SIP, а также текстовые и голосовые сообщения в Skype, Viber, MS Lync;
- файлы, передаваемые по протоколам FTP, FTPS, HTTP и HTTPS, а также в программах-мессенджерах (ICQ, Windows Messenger и т.д.) или по электронной почте в качестве вложений;
- HTTP- и HTTPS-трафик по протоколу ICAP с корпоративного прокси-сервера;
- SSL-трафик, передаваемый по шифрованным протоколам (включая HTTPS, FTPS, защищенные протоколы SSL для POP3, SMTP и мессенджеров);
- содержимое баз данных MS SQL Server, Oracle, PostgreSQL, SQLite, MySQL;
- данные, передаваемые на внешние устройства (USB-накопители, WiFi- и GPRS-модемы, внешние жесткие диски и др.);
- информация, отправляемая на сетевые диски пользовательских компьютеров и терминальных серверов;
- данные, отправляемые на печать на локальные и сетевые принтеры;
- регистрация нажатий клавиш на клавиатуре (кейлогер);
- IP-телефония (текстовые и голосовые сообщения, передаваемые по протоколу SIP);
- любая текстовая и числовая информация, копируемая в буфер обмена;
- запись с микрофонов, как встроенных, так и подключенных к рабочим станциям;
- распознавание конфиденциальной текстовой и числовой информации на изображениях.

Заключение

Опыт эксплуатации различных информационных систем (ИС) показывает, что проблема обеспечения безопасности еще окончательно не решена. Имеющиеся в продаже средства защиты информации значительно различаются друг от друга по решаемым ими задачам, используемым методам и достигаемому результату.

Угрозы информационной безопасности предприятия совершенно реальны, их нельзя недооценивать. Кроме противодействия внешним угрозам особое внимание следует уделить угрозам внутренним. Важно помнить, что утечки корпоративных секретов случаются не только по злому умыслу – как правило, их причина в элементарной халатности и невнимательности работника. При выборе средств защиты следует строить надежную модульную систему безопасности, закрытую от рисков вторжения извне и позволяющую осуществлять контроль и мониторинг за потоком

информации внутри компании [5]. Внедрение мер обеспечения ИБ предполагает: безопасность серверов и рабочих станций, защиту от утечек конфиденциальной информации, управление правами доступа к информации, безопасность корпоративных бизнес-приложений, безопасность web-ресурсов, безопасность корпоративных порталов, безопасность электронной почты, безопасность удаленного доступа к корпоративным ресурсам, безопасность использования мобильных устройств, идентификацию, аутентификацию и управление правами доступа, криптографическую защиту информации, контроль носителей информации, противодействие мошенничеству и др. [5].

Также руководству предприятий необходимо осуществить и провести правовые мероприятия – создать в организации нормативно-правовую базу информационной безопасности: разработать на основе законодательных актов Республики Беларусь необходимые руководящие и нормативно-методические документы, перечни охраняемых сведений, меры ответственности лиц за нарушение порядка работы с конфиденциальной информацией.

В современных условиях обеспечение безопасности информации регулируется следующими нормативными актами:

1. Законом Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 г. № 455-З (ред. от 04.01.2014 г.).

В главе 3 «Правовой режим информации» имеется 6 статей об информационной безопасности. В главе 4 «Распространение и предоставление информации» – 4 статьи [6].

2. Уголовным кодексом Республики Беларусь от 09.07.1999 г. № 275-З (ред. от 24.10.2014).

В главе 31 «Преступления против информационной безопасности» имеется 7 статей, касающихся защиты компьютерной информации [7].

Список использованной литературы

1. **Петров, А. А.** Компьютерная безопасность: криптографические методы защиты / А. А. Петров. – М. : ДМК Пресс, 2014. – 250 с.

2. **«Battling** the Big Hack:Inside the ring and out... IT pros plan to land some blows in 2016 // Spiceworks.com [Электронный ресурс]. – Режим доступа : http://www.spiceworks.com/marketing/it-security/report. – Дата доступа : 18.02.2016.

3. **Шаньгин, В.Ф.** Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.

4. **Шаньгин, В. Ф.** Информационная безопасность компьютерных систем и сетей : учеб. пособие. – М. : ФОРУМ : ИНФРА-М, 2011. – 416 с.

5. **Ярочкин, В. И.** Информационная безопасность : учеб. пособие для вузов. – М. : Академ. проект, 2006. – 544 с.

6. **Закон** Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 г. № 455-З (в ред. от 11.05.2016 г.) // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016.

7. **Уголовный** кодекс Республики Беларусь : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. Беларусь 24 июля 1999 г. // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016.

Получено 25.10.2016 г.