Список цитируемых источников

1. Документация React [Электронный ресурс]. — Режим доступа: http://reactjs.org/ . — Дата доступа: 16.04.2019.
2. Документация Redax [Электронный ресурс]. — Режим доступа: http://npmjs.com/package/redax . — Дата доступа: 16.04.2019.
3. Документация Material-UI [Электронный ресурс]. — Режим доступа: http://material-ui.com/ . — Дата доступа: 17.04.2019.
4. *Макфарланд, Д. С.* Новая большая книга CSS / Д. С. Макфарланд. — СПб. : Питер, 2017. — 720 с.
5. *Фримен, Э.* Изучаем HTML, XHTML и CSS / Э. Фримен — СПб. : Питер, 2010. — 656 с.

УДК 004.056.53

В. О. Богушевич, Е. Н. Босая
Учреждение образования «Барановичский государственный университет», Барановичи

ЗАЩИТА ИНФОРМАЦИИ В СЕТИ

Введение. Информационная безопасность в Сети — действия, направленные на защиту работоспособности и целостности сети и данных, для предотвращения и мониторинга попыток несанкционированного доступа, модификации информации, возможного отказа работы всей компьютерной сети и других сетевых ресурсов.

Современный мир — это мир компьютерной техники, и люди, живущие в этом мире, чувствуют себя в нём комфортно, они легко осваивают компьютер, мобильные устройства, новомодные гаджеты и ими пользуются. Интернет сегодня — это гораздо больше, чем просто общение с друзьями, социальные сети, игры, онлайн-покупки [1, с. 367]. Это открытая система информации, и, если кажется, что вам нечего скрывать или ваша информация никому не нужна, вы глубоко заблуждаетесь. Любая информация о вас может быть использована не теми, кому она предназначалась. Абсолютно любая информация, которой ежедневно делятся люди с друзьями и близкими, может в любой момент оказаться у злоумышленников.

Основная часть. Быстрое развитие процессов автоматизации и проникновение вычислительных машин во все сферы жизни привели к появлению очень важной проблемы надежного обеспечения сохранности информации. Особую роль в этом процессе сыграло появление персональных ЭВМ, локальных и глобальных сетей, спутниковых каналов связи, эффективной технической разведки и конфиденциальной информации, программное обеспечение и другие информационные технологии, доступные для широкой публики. Широкое распространение ПК и невозможность эффективного контроля за их использованием привели к снижению уровня безопасности информационных систем, что существенно обострило проблему защиты информации [2, с. 392].

Информационная безопасность — состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Информационная безопасность включает в себя такие аспекты: целостность информации — предотвращение несанкционированной модификации или разрушения информации; конфиденциальность — предотвращение несанкционированного ознакомления с информацией.

Многие организации не до конца понимают истинную силу виртуальной интернет-угрозы, поэтому ограничиваются лишь элементарными средствами защиты. Как правило, это традиционная блокировка компьютерного вируса или введение ограничений на спам-сообщения в электронной почте [3, с. 594].

В сложившейся ситуации обработка данных вывела проблемы информационной безопасности в ранг самых важных государственных проблем. Решение проблемы плохой информационной безопасности предполагает комплекс мер, прежде всего такие действия государства, как разработка системы классификации, документирование методов защиты информации, правил доступа к данным и меры наказания против нарушителей информационной безопасности. Порядок хранения данных должен быть четко определен в правовых актах и предусматривать полную безопасность носителей, контроль за работой с информацией, ответственность за несанкционированный доступ к носителям в целях их копирования, изменения или уничтожения.

Обеспечение информационной безопасности в компьютерных сетях и ПК, работающих автономно, достигается комплексными организационными, техническими и программными мерами.

Организационные методы защиты информации включают в себя: доступ к обработке и передаче конфиденциальной информации только определенным должностным лицам; исключение посторонних лиц для просмотра содержания материалов, обрабатываемых через дисплей, принтер.

Технические методы: ограничение доступа в помещения, в которых происходит обработка информации (сигнализация и устройства, ограничивающие доступ в помещения, и установка на дверях помещений кодовых замков); хранение носителей информации и документов в закрытых от несанкционированного доступа сейфов и помещениях; уничтожение информации на жестких дисках при отправке ком-

пьютера в ремонт; установка оборудования, которое обеспечивает энергонезависимую работу ЭВМ (источник бесперебойного питания); оборудование охранных зон с помощью скрининговых машинных залов и организация систем пересечения границ.

Программные методы: блокировка данных и ввод ключа; контроль доступа к различным уровням памяти компьютера; контроль доступа с помощью ввода пароля, идентификационной карты; распределенный доступ к ЭВМ (администратор — гость).

Нужно отметить, что именно руководитель организации принимает решение о том, какую информацию необходимо защитить на производстве, а отдел информационных технологий разрабатывает методы, которыми будет защищена информация [4, с. 587].

Вопрос безопасности является определяющим при отправке конфиденциальной информации, такой как номера кредитных карт при покупке в интернет-магазине. Например, рассмотрим процесс покупки книги в Интернете. В ходе данного процесса необходимо ввести номер своей кредитной карты в форму заказа для обработки данных платежа. Если один из промежуточных компьютеров под контролем злоумышленника, то данные могут быть утрачены. Трудно сказать, как часто это происходит, но технически это возможно.

Чтобы избежать рисков, в веб-браузере следует установить высокий уровень почтовых оповещений. Google, FireFox, Opera и Internet Explorer отображают блокировку, когда веб-страница защищена, и позволяют отключить или удалить файлы “cookies”.

Если пользоваться услугами онлайн-банка, необходимо убедится, что банк использует цифровые сертификаты. Популярный метод безопасности (безопасных электронных транзакций) — оповещение о снятии денег с карточки.

Точно также, когда сообщение из электронной почты перемещается по сети, оно временно создает копию на многие компьютеры. Это означает, что его могут читать недобросовестные люди, которые производят незаконные действия в компьютерных системах.

Единственный способ защитить сообщение — поместить его в своего рода «конверт», т. е. закодировать его с помощью любой формы шифрования или передавать заархивированный файл. Система, предназначенная для отправки электронной почты в частном порядке, это довольно хорошая конфиденциальность, бесплатная программа, написанная Филом Циммерманом.

Частные сети, подключенные к Интернету, могут быть атакованы злоумышленниками, которые пытаются получить ценную информацию, такую как номера социального страхования, банковские счета или исследовательские и деловые отчеты [5, с. 233].

Для защиты важных данных компании нанимают консультантов по безопасности, которые анализируют риски и предоставляют решения по безопасности. Наиболее распространенными методами защиты являются пароли для систем контроля доступа, шифрования и дешифрования, а также брандмауэры.

Вирусы могут проникать на ПК через файлы с дисков, Интернета или систем доски объявлений. Если необходимо защитить свою систему, не стоит открывать вложения электронной почты от незнакомых людей и быть осторожным при загрузке файлов из Интернета (обычная текстовая электронная почта не может передать вирус). Актуально также обновлять антивирусные программы как можно чаще, так как появляются новые вирусы.

Профилактические советы по безопасности: не стоит открывать вложения электронной почты от неизвестных людей, всегда необходимо принимать к сведению расширение файла; устанавливать и периодически обновлять антивирусную программу; установить брандмауэр — программу, предназначенную для предотвращения доступа шпионских программ к внутренней сети; не принимать файлы из источников высокого риска; использовать цифровой сертификат, электронный способ подтверждения личности; не сообщать номера кредитных карт посторонним.

Заключение. Проблема защиты информации в Сети (с той или иной степенью эффективности волнует пользователей с момента появления коммуникационных технологий. Наблюдаемый в последние годы взрывной рост популярности сетей и связанных с ними коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в Интернете [6, с. 703]. Причем если ранее основной задачей защиты было сохранение ресурсов преимущественно от хакерских атак, то в настоящее время актуальной становится задача защиты коммерческой информации. Чтобы снизить риск угрозы для информации, необходимо осуществлять все возможные меры для ее защиты.

Список цитируемых источников

1. *Емельянова, Н. З.* Защита информации в персональном компьютере : учеб. пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. — М. : Форум, 2013. — 368 с.
2. Защита информации : учеб. пособие / А. П. Жук [и др.]. — М. : ИЦ РИОР : НИЦ ИНФРА-М, 2013. — 392 с.
3. *Шаньгин, В. Ф.* Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — М. : ДМК Пресс, 2012. — 592 с.
4. *Бузов, Г. А.* Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. — М. : ГЛТ, 2016. — 586 с.
5. *Малюк, А. А.* Защита информации в информационном обществе : учеб. пособие для вузов / А. А. Малюк. — М. : ГЛТ, 2015. — 230 с.
6. *Шаньгин, В. Ф.* Информационная безопасность и защита информации / В. Ф. Шаньгин. — М. : ДМК, 2014. — 702 с.