от выбранной тематики. Но в топ выдачи поисковой системы попадет только тот, в котором уделялось внимание не только его созданию, но и наполнению. Именно такой сайт будет качественным и актуальным, сможет заинтересовать пользователя и принесет определенную выгоду своему владельцу.

Список источников:

1. Адамс Д.Р., Флойд К.С. Основы работы с XHTML и CSS: учебное пособие. – М.: Интернет-Университет Информационных Технологий, 2007. – 478 с.

2. Алексеев, А.П. Введение в Web-дизайн: учебное пособие. – М.: СОЛОН-ПРЕСС, 2008. – 185 с.

3. Керниган Б.В., Ричи Д.М. Язык программирования С: учебник. – М.: Интернет-Университет Информационных Технологий, 2006. – 272 с.

4. Нужнов Е.В. Мультимедиа технологии: учебное пособие. – 2-е изд., перераб. и доп. – Таганрог: Издательство Южного федерального университета, 2016. – 180 с.

5. Панфилов К.С. Создание веб-сайта от замысла до реализации: практические советы. – М.: ДМК Пресс, 2009. – 438 с.

6. Савельев А.О., Алексеев А.А. HTML5. Основы клиентской разработки. – 2-е изд., испр. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 272 с.

7. Брэнд К., Спикльмайр Д., Фридли К., Спикльмайр С. Zope. Разработка Web-приложений и управление контентом: практические советы / пер. с англ. – М.: ДМК Пресс, 2007. – 462 с.

УДК 004.772

Рубцова Л.Ю.

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Рубцова Лилия Юрьевна*[*]; обучающаяся 4 курса; ФГБОУ ВО «Орловский государственный университет экономики и торговли»; РФ, 302028, г. Орел, ул. Октябрьская, д. 12; e-mail: irina-smag@yandex.ru*

Актуальность проблемы защиты информации сегодня не вызывает сомнений. Успех современной компании и ее развитие в условиях острой конкуренции в значительной степени зависят от применения информационных технологий, а следовательно, от степени обеспечения информационной безопасности. Для современных предприятий характерно стремительное развитие их информационной среды. Постоянное накопление информации требует ее надлежащей обработки и хранения. Совершенствование угроз при передаче данных по открытым сетям диктует необходимость новых технологических решений, обеспечивающих защиту. Использование интернет-технологий при создании распределенных баз данных и построении информационных систем различного назначения в последнее время стало доминирующим в мировом информационном пространстве. Данный фактор несет в себе угрозу в виде возможности легкой кражи, изменения, порчи и подмены передаваемой информации. В связи с растущими объемами информации и документов на предприятии встает вопрос об их оптимальном хранении и защите.

Настоящая статья посвящена такой важной проблеме, как безопасность информации. Дается перечень рекомендаций по повышению безопасности информации при передаче данных в сети.

Ключевые слова: безопасность, конфиденциальность, несанкционированный доступ, передача данных, сеть.

[*] ***Научный руководитель: Смагина Ирина Валерьевна,*** *к.э.н., доцент; e-mail: irina-smag@yandex.ru*

Rubtsova L.Yu.

INFORMATION SECURITY TECHNOLOGIES AT DATA TRANSMISSION IN COMPUTER NETWORKS

Rubtsova Lilia Yurievna, *Orel State University of Economics and Trade; 12 Oktyabrskaya Street, Orel 302028, Russian Federation; e-mail: ivv88@ogiet.ru*

There is no doubts about the urgency of the problem of information protection today. The success of modern company and its development under conditions of intense competition substantially depend on information technologies and, hence, on the degree of information safety. For modern enterprises prompt development of their information environment is a characteristic. Constant accumulation of information requires its appropriate processing and storage. Perfection of threats to data transmission on open networks requires the necessity of information protection of new technological decisions providing such protection. The use of the Internet technologies while creating distributed databases and information systems of different purposes has recently become dominating in the world information field. This factor means the possibility of easy theft, change, damage and substitution of transmitted information. Because of growing volumes of information and documents at the enterprise, there is a question on their optimum storage and protection.
The article is devoted to such important problem as information security. Besides, recommendations about improvement of information security at data transmission in the network are given in the article.

Keywords: security, confidentiality, non-authorized access, data transmission, network.

Актуальность проблемы защиты информации сегодня не вызывает сомнений. Успех современной компании и ее развитие в условиях острой конкуренции в значительной степени зависят от применения информационных технологий, а следовательно, от степени обеспечения информационной безопасности.

Любое предприятие располагает различными видами информации, представляющими интерес для злоумышленников. Прежде всего, это коммерческие данные, информация, являющаяся интеллектуальной собственностью предприятия, и конфиденциальные данные.

Ни одна компания не может обойтись без документа и, следовательно, документооборота. Документооборот является обязательной частью деятельности организации. Это активно используется конкурентами, они пытаются проникнуть в процесс обработки информации, чтобы помешать работе компании. Зачастую в компаниях численностью до ста сотрудников эти проблемы игнорируются, а иногда носят чисто формальный характер.

Например, программы 1С представляют собой универсальные решения для хранения важных данных и их обработки. Справочники, журналы и документы лишь оболочки для удобного обращения с данными и связи между ними. Нередко возникает необходимость выгрузить эти данные из 1С. Цели могут быть самые разные – выгрузка для обмена с другими программами 1С, выгрузка для банка, отчетность в налоговые органы и т.п., выгрузка данных в файлы различных форматов и другие. Такие сведения чаще всего и интересуют киберпреступников.

В настоящее время большое количество компьютерных сетей объединено посредством интернета. Поэтому очевидно, что для безопасной работы организации необходимо принять определенные меры, поскольку практически с любого компьютера можно получить доступ к сети любой организации. При этом угроза значительно возрастает по той причине, что для взлома не требуется физического доступа.

Администраторы локальных сетей все чаще сталкиваются с проблемами информационной безопасности. Это особенно важно в сетях, где нужно работать с информацией, требующей дополнительной защиты. Это сети государственных учреждений, компаний, связанных с выпуском определенных продуктов, и других организаций, раскрытие внутренней информации которых может нанести серьезный экономический ущерб. Эта проблема особенно

важна, когда локальные сети должны быть доступны через глобальную сеть, когда к ним должны быть подключены мобильные пользователи или сотрудники удаленных отделов, когда пользователи локальной сети имеют доступ к глобальной сети.

Использование интернет-технологий в создании распределенных баз данных и в построении информационных систем для различных целей в последнее время играет доминирующую роль в глобальном информационном пространстве. Этот фактор представляет угрозу в виде возможности легкой кражи, изменения, повреждения и замены предоставленной информации.

В связи с растущим объемом информации и документов в компании возникает вопрос об их оптимальном хранении и защите.

Существует множество причин, которые могут серьезно повлиять на работу локальных и глобальных сетей и привести к потере ценной информации компании.

Среди них можно выделить следующие:

1. Несанкционированный доступ извне, копирование или изменение информации случайные или умышленные действия, приводящие к:

- искажению либо уничтожению данных;
- ознакомление посторонних лиц с информацией, составляющей банковскую, финансовую или государственную тайну.

2. Некорректная работа программного обеспечения, приводящая к потере или порче данных из-за:

- ошибок в прикладном или сетевом ПО;
- заражения систем компьютерными вирусами.

3. Технические сбои оборудования, вызванные:

- отключением электропитания;
- отказом дисковых систем и систем архивации данных;
- нарушением работы серверов, рабочих станций, сетевых карт, модемов.

4. Ошибки обслуживающего персонала.

Основные проблемы защиты информации можно разделить на три группы:

- нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в корпоративной сети, может иметь высокую ценность для владельца. Ее использование другими лицами наносит ущерб интересам организации;
- нарушение целостности информации. Потеря целостности информации (компрометация, дезинформация). Ценная информация может быть модифицирована или удалена;
- нарушение доступности информации. Вывод из строя или изменение режимов работы элементов компьютерной сети. Может привести к получению неверных результатов, отказу компьютерной сети от потока информации или отказам при обслуживании.

Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений в развитии информационных технологий.

Современные компании характеризуются быстрым развитием их информационной среды. Постоянное накопление информации требует ее правильной обработки и хранения.

В результате работы с данными важной задачей является организация защиты информации на предприятии. Если правильно не организовать работу в этом направлении, то можно потерпеть крах в современной экономической среде, которая не всегда отличается доброжелательной конкуренцией.

Зачастую все обстоит по-другому. Конкурирующие фирмы стараются правильными и неправильными способами получить информацию о своем конкуренте, чтобы опередить его в развитии и продвижении на рынке.

На сегодня защита информации на предприятии представляет собой комплекс мер, которые направлены на то, чтобы сохранить целостность, уберечь от кражи и подмены следующие данные:

1. Базу данных клиентов и партнеров;

2. Электронный документооборот компании;

3. Технические нюансы деятельности предприятия;

4. Коммерческие тайны.

Система защиты информации на предприятии должна разрабатываться с учетом рисков, которые наиболее часто встречаются в информационной среде современных компаний.

К основным из них следует отнести:

- попытки получения доступа к данным, которые недоступны для неавторизованных пользователей информационной системы предприятия;

- несанкционированное изменение и подмена информации, которая может привести к потере предприятиями своей репутации и имиджа;

- попытки получения доступа и кражи конфиденциальной, секретной и технической информации.

Учитывая перечисленные угрозы, защита конфиденциальной информации на предприятии должна строиться как на аппаратном, так и программном уровне. Только в комплексе можно успешно защитить свои данные от киберзлоумышленников.

Аппаратные средства применяются на всех организационных уровнях. Однако особенно важно правильно организовать хранение информации.

Задача аппаратных средств при этом:

- обеспечивать нужную скорость доступа к данным;

- гарантировать надлежащую скорость систем проведения расчетов;

- обеспечивать целостность данных и гарантию их сохранения при выходе из строя отдельных средств хранения;

- организовывать резервное копирование, быстрое восстановление информации при сбоях;

- обеспечивать взаимодействие со средствами связи;

- реагировать и минимизировать ущерб при аварийных ситуациях (пожар, затопление);

- сохранять работоспособность основного оборудования во время отключения основного источника энергии (генераторы, источники бесперебойного питания).

- обрабатывать запросы подключенных пользователей.

В хранилищах данных для решения поставленных задач применяются серверы, оснащенные RAID-массивами, дисками требуемой производительности.

Обязательно в той или иной мере реализуется принцип дублирования ключевых систем. Используются сетевые контроллеры, распределительные средства и многое другое.

Аппаратные технологии защиты информации в интернете включают также межсетевые экраны, программно-управляемое оборудование, системы идентификации, управления доступом и многое другое.

Область программных средств – самая обширная. Выбор конкретного списка пакетов зависит от используемых платформ и операционных систем, принятых механик доступа.

Среднестатистический список защитных мер включает:

1. Систему обнаружения сетевых атак и попыток несанкционированного доступа на узел в составе программно-управляемого оборудования;

2. Комплексы шифрования (программные или аппаратные);

3. Средства подтверждения подлинности, электронные ключи и системы для работы с ними;

4. Средства управления доступом, которые могут включать и аппаратные средства.

На практике правильно выбранный комплекс программных средств может в принципе исключить прямую атаку на хранилище или отдельный узел системы обработки данных.

Подводя итог, хочется еще раз подчеркнуть важность такой проблемы, как защита информации при передаче данных по сети, служащей неотъемлемой частью деятельности любой организации. Соблюдение данных правил позволит обезопасить компанию от раскры-

тия внутренней информации, которая, в свою очередь, может привести к серьезному экономическому ущербу.

Список источников:

1. Абраров Р.Д., Курязов Д.А. Информационная безопасность в компьютерных сетях // Молодой ученый. – 2016. – №9-5 (113). – С. 10-12.

2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях. – СПб.: Изд-во СПбГУЭФ., 2014. – 267 с.

3. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. – М.: Проспект, 2015. – 216 с.

4. Вишневский В.М. Теоретические основы проектирования компьютерных сетей: монография. – М.: Техносфера, 2003. – 512 с.

4. Гаврилов А.Д., Волосенков В.О. Угрозы информационной безопасности автоматизированной системы обработки данных // Проблемы безопасности российского общества. – 2015. – №4. – С. 85-92.

5. Макаренко С. И. Информационная безопасность. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2015. – 371 с.

6. Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Издательский центр «Академия», 2014. – 331 с.