Асланов Рамиль Махир оглы
кандидат юридических наук
E-mail: aslanov_ramil@yandex.ru

Проблемы защиты корпоративной информации в сети Интернет

В статье исследуется специфика защиты информации в глобальной сети Интернет, анализируются проблемы защиты. Предлагаются главные направления обеспечения безопасности корпоративных сетей при подключении к Интернету.

Ключевые слова: *регулирование, информация, безопасность, система, Интернет, конфиденциальность, идентификация.*

Dr. Ramil Aslanov
E-mail: aslanov_ramil@yandex.ru

Problems of the protection of corporate information in the network the Internet

This article tells about special ways to protect the information in the Internet and analyses problem, connected with that. The main ways of protection corporative networks, connected to the Internet.

Key words: *regulation, information, safety, system, the Internet, identification, confidentiality.*

Научно-технический и социальный прогресс, развитие инновационных технологий привели к возрастанию массива информации, получившему название «информационный взрыв». Наступила эпоха «информационного общества», в котором большинство работающих непосредственно связаны с поиском новых знаний, с получением, накоплением и распространением информации. Возрос интерес к информатизации всех сторон общественной жизни, расширились возможности дистанционного образования, сфера активного использования глобальной компьютерной сети «Интернет»[1].

Защита информации в сети Интернет сегодня является одним из самых проблемных вопросов современного общества. В процессе решения этой задачи возникает целый комплекс организационных, технических, правовых и иного рода проблем.

Кроме того, одной из насущных проблем является противоречие между интересами бизнеса и безопасностью пользователей Интернета.

Защита информации в глобальной сети Интернет имеет свою специфику, отличающую ее от способов защиты информации в локальных сетях. Важнейшей отличительной особенностью защиты информации в глобальной сети является тот факт, что она осуществляется посредством программно-аппаратных средств.

Существуют условия, в соответствии с которыми организация обязана размещать определенную информацию в Интернет. Например, саморегулируемая организация арбитражных управляющих обязана разместить с соблюдением требований федеральных законов, предъявляемых к защите информации (в том числе персональных данных), на своем сайте в сети Интернет учредительные документы саморегулируемой организации, стандарты и правила профессиональной деятельности, и пр.[2]

В соответствии со ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

[1] См.: Зверева Е.А. Правовой режим информации в отношениях с участием субъектов предпринимательской деятельности. — М.: Юстицинформ, 2008.

[2] Федеральный закон от 26.10.2002 N 127-ФЗ (ред. от 01.01.2012) «О несостоятельности (банкротстве)» // Парламентская газета. 2002. № 209-210.

информации»[3] защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Достаточно сложно обеспечить требования закона по защите информации, особенно в сети Интернет. Поэтому компании (организации, предприятия) часто сталкиваются с трудностями.

В глобальной сети потенциальную возможность доступа к ресурсам имеет любой пользователь сети, находящийся в любой точке Земного шара, и момент доступа к той или иной информации не может быть предсказан заранее.

Другой особенностью защиты информации является огромная скорость развития в Интернет программного обеспечения и технологий. Новые технологии преодоления систем защиты информации появляются каждые полгода, а арсенал используемых атакующими средств может меняться каждые 2–3 месяца.

Всемирная сеть позволяет сотрудникам компаний мгновенно обмениваться информацией, не покидая своего рабочего места. Однако с подключением к сети Интернет перед организациями встает проблема защиты корпоративных ресурсов от различных видов угроз. При использовании Интернет компании должны знать, что существуют следующие виды угроз:

1) Атаки на корпоративную сеть. Традиционные средства защиты, такие как межсетевые экраны и маршрутизаторы, обеспечивают контроль доступа в корпоративную сеть извне.

2) Атаки на web-портал и интернет-магазин. Здесь на первое место выступает защита доступа к базе данных, системе электронных платежей, своевременное обнаружение и устранение уязвимостей в программном обеспечении серверов.

3) Перехват незашифрованного трафика через проводные и беспроводные каналы. Эта угроза относится ко всем интернет-сервисам, используемым в организации. В проводных сетях данные могут быть перехвачены путем получения физического доступа к среде передачи. В беспроводных сетях злоумышленнику вовсе не обязательно пребывать на территории компании, достаточно попасть в зону действия радиосигнала корпоративной Wi-Fi точки доступа. Широкое распространение получили и несанкционированные беспроводные сети с бесплатными точками доступа. Когда пользователь подключается к ложной точке доступа, хакер может сделать с его компьютером все, что угодно, причем такую атаку обнаружить зачастую невозможно. Зараженная система ничего не подозревающего сотрудника становится «входной дверью» в корпоративную сеть. Более того, злоумышленники могут получить доступ к компьютеру пользователя, даже если он не подключен к Wi-Fi сети. Достаточно того, что устройство беспроводной связи в компьютере пользователя настроено по умолчанию, включено и занято поиском сети. Полученная любым из этих способов информация о корпоративной сети, в том числе логины и пароли сотрудников, помогают злоумышленникам провести успешную атаку. Незащищенная беспроводная точка доступа, подсоединенная к локальной сети, также представляет собой «открытую дверь» для хакеров.

Кроме того сотрудники компаний используют доступ к Сети в личных целях, что создает брешь в системе корпоративной безопасности, а при помегабайтной оплате трафика приводит к росту расходов на Интернет и невозможности эффективного планирования издержек. Пользователям часто приходится заполнять различные формы на сайтах, вводя логины и пароли, указывать почтовый ящик для связи. Многие сотрудники пользуются при этом корпоративным почтовым ящиком, корпоративными логинами и паролями. Кроме того, при скачивании различных файлов из Интернета, получении личной электронной почты, посещении хакерских и других опасных веб-ресурсов работники могут загрузить на свой компьютер вредоносные программы. Если используемое в компании антивирусное решение вовремя не сработает, в корпоративной сети появится лазейка для злоумышленников. Наихудшим вариантом развития событий будет получение хакерами конфиденциальной информации компании и полный контроль над сетью.

В свете вышесказанного главными направлениями обеспечения безопасности корпоративных сетей при подключении к Интернету являются:

[3] Российская газета. 2006. № 165.

- организация защиты, как от внешних, так и от внутренних угроз;
- маскировка внутренних адресов корпоративной сети;
- контроль доступа пользователей к ресурсам Интернета, а также контроль за использованием внутрикорпоративных ресурсов сотрудниками, находящимися за пределами сети организации;
- защита от вредоносных программ;
- предотвращение перехвата и искажения информации, передаваемой через Интернет;
- мониторинг пользователей и предоставление отчетов о расходе трафика и посещении сетевых ресурсов.

С целью обеспечения реализации указанных главных направлений обеспечения безопасности корпоративных сетей при подключении к Интернету необходимо, в ходе информационного обмена, выполнять следующие требования[4]:

запрещение прямого доступа из публичных внешних сетей к любым системным компонентам, на которых выполняется хранение данных;

- использование параметров безопасности и системных паролей, установленных производителем;
- изменение параметров, влияющих на защищенность, заданных производителем по умолчанию;
- защита данных при сохранении, в том числе ключей, использующихся для шифрования данных;
- шифрование данных, передаваемых по сетям общего пользования;
- включение постоянной антивирусной защиты. Механизмы обеспечения антивирусной защиты должны регулярно обновляться и обладать возможностью ведения журналов регистрации событий;
- разработка процедур, позволяющих персоналу легко отличать сотрудников от посетителей, особенно в тех помещениях, в которых существует возможность получения доступа к данным;
- использование журнала регистрации посетителей с целью хранения записей о них;
- обеспечение физической защиты всех бумажных и электронных носителей, содержащих защищаемые данные, а также должен обеспечиваться строгий контроль над внутренним или внешним перемещением носителей всех видов, содержащих такие данные;
- регистрация событий с целью восстановления данных. В регистрируемых событиях для каждого системного компонента должны записываться, по крайней мере – ID пользователя, тип события, дата и время, результат, источник события, ID данных;
- ежедневный просмотр журналов зарегистрированных событий для всех системных компонентов. Журналы регистрации событий должны храниться, по крайней мере, в течение 1 года (оперативная доступность – 3 месяца);
- должно производиться систематическое тестирование систем и процессов обеспечения безопасности, а также выполняться внутреннее и внешнее сканирование уязвимостей сети в случаях значительных изменений в структуре сети.

Кроме того, важную роль играет правильная организация процесса аутентификации в современных бизнес – структурах, особенно в финансовых учреждениях и банках.

Вслед за активным продвижением Интернета в России растет популярность интернет-банкинга. Все больше и больше банков активно развивают дистанционные каналы обслуживания клиентов. Но одно дело зайти в Интернет, чтобы найти нужную информацию — например, найти адрес ближайшего офиса, прочитать новости или расписание работы и совсем другое — чтобы получить информацию по своим счетам и банковским картам, открытым в банке и провести операции по ним. Ведь такая информация должна быть доступна только клиенту и соответственно должна быть надежно защищена. При использовании мобильного и интернет-банкинга клиент в первую очередь должен быть аутентифицирован[5]. Например, Сбербанк России с недавних пор стал выполнять двухуровневую систему аутентификации частных клиентов: логин-пароль при входе и получении информации и дополнительное подтверждение клиента при выполнении операций со средствами путем генерации пароля и пересылки его клиенту на мобильный телефон. Практически по такому же пути пошел и Банк Москвы. Ясно, что использование этих средств отвлекает значительные ресурсы банков, но в данном случае

[4] См.: Васенин, В. А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности / Под ред. В.П. Шерстюка. М.: МЦНМО, 2004.

[5] См.: Деменюк Ю.В. Аутентификация и защита информации в мобильном и интернет-банкинге // Расчеты и операционная работа в коммерческом банке. 2010. № 3.

цена вопроса (в широком смысле) дороже понесенных издержек.

Действующее в Российской Федерации законодательство, в том числе уголовное, содержит достаточные правовые гарантии для обеспечения информационной безопасности пользователей и операторов Интернета. Однако такие гарантии чаще всего пока не подкрепляются правоприменительными механизмами их соблюдения. Требуется внесение учитывающих специфику Интернета изменений и дополнений в Уголовно-процессуальный, Гражданский процессуальный и Арбитражный процессуальный кодексы Российской Федерации, Федеральный закон «О безопасности», а также в главу (о защите информации) Федерального закона «Об информации, информатизации и защите информации»[6].

Но с другой стороны Интернет представляет собой яркий пример того, насколько удачно и эффективно может развиваться столь сложная техническая система практически в отсутствие государственного регулирования, основываясь только на выработанных внутри Сети правилах. Это порождает важный вопрос о том, как скоро уровень развития социальных отношений, связанный с существованием подобной системы, потребует разработки и применения соответствующего правового регулирования. Следующим, очевидно, будет вопрос о том, насколько эффективным окажется такое регулирование для развития самой технической системы[7].

[6] Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации // Международное публичное и частное право. 2011. № 4. С. 22.

[7] Танимов О.В., Кудашкин Я.В. Перспективы правового регулирования отношений в сети Интернет // Информационное право. 2010. № 4. С. 17.