Банько Юлия Александровна
студентка
Кокорева Ангелина Максимовна
студентка
Михнев Илья Павлович
канд. техн. наук, доцент, доцент
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

СОВРЕМЕННЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ: ЧТО РЕАЛЬНО УГРОЖАЕТ БИЗНЕСУ?

Аннотация: *в статье рассмотрен анализ современных угроз безопасности информации в сфере бизнеса, определены основные требования международным стандартам информационной безопасности по некоторым видам деятельности, изложен перечень угроз безопасности, а также возможные решения данной проблемы.*

Ключевые слова: *бизнес, угрозы, информационная безопасность, стандарт безопасности, комплексная система защиты, средства криптографической защиты.*

Для благополучия бизнеса информационная безопасность имеет основополагающее значение. В настоящее время у бизнеса есть силы и возможность привлечь специалистов для быстрого роста компании.

Говорить о проблемах с информационной безопасностью в малом бизнесе не приходится, так как руководители в состоянии проконтролировать порядок в небольшом коллективе сотрудников, наряду с тем, что интерес со стороны злоумышленников невелик. Когда же компания перешагивает порог в тысячу сотрудников и появляются сотни удаленных офисов (филиалов) – наступает переломный момент, который (в отсутствие должного внимания со стороны

специалистов по информационной безопасности) погубит бизнес. По большей части появление новых угроз связано с развитием информационных технологий. Раньше обеспечение непрерывности бизнеса в основном ложилось на плечи IT-подразделений, то теперь эта работа перекладывается на службу информационной безопасности [1].

В этой статье мы постараемся предложить анализ процессов информационной безопасности в компании и тех угроз в бизнесе, которые могут возникнуть при отсутствии той или иной процедуры. Сегодня вся коммерческая информация, бухгалтерские данные, финансовая отчетность, клиентские базы, договора, новаторские идеи сотрудников фирмы, планы и стратегия ее развития, хранятся в локальной информационно-компьютерной сети. Далеко не всегда и не все документы дублируются на бумажных носителях, ведь их объем информации очень велик. В таких условиях информационная безопасность предусматривает систему мер, которые призваны обеспечить надежную защиту серверов и рабочих станций от сбоев и поломок, ведущих к уничтожению информации или ее частичной потере. Хакеры преднамеренно осуществляют хищение данных, промышленный шпионаж и сбор утечек информации по вине собственных сотрудников представляющих наибольшую угрозу. В данном случае, информационная безопасность принимает меры, направленные на контроль инсайдеров и многоступенчатую защиту серверов от хакерских атак [1; 3].

Непредумышленный вред конфиденциальным сведениям причиняется по простой халатности или неосведомленности работников. Всегда есть возможность того, что кто-нибудь откроет письмо и внедрит вирус с личного ноутбука на сервер компании. Или, например, скопирует файл с конфиденциальными сведениями на планшет, внешний носитель информации или карманный персональный компьютер для работы в командировке. И ни одна компания не застрахована от пересылки невнимательным сотрудником важных файлов не по тому адресу. В такой ситуации информация оказывается весьма легкой добычей [3; 4].

Недоступность или ухудшение качества работы публичных веб-сервисов в результате DDoS-атак (*Distributed-Denial-of-Service – «Распределенный отказ в*

обслуживании») может продолжаться довольно длительное время, от нескольких часов до нескольких дней. Обычно подобные атаки используются в ходе конкурентной борьбы, шантажа компаний или для отвлечения внимания системных администраторов от неких противоправных действий вроде похищения денежных средств со счетов.

Следует знать, что использование пиратского нелицензионного программного обеспечения не дает защиты от мошенников, заинтересованных в краже информации с помощью вирусов. Обладатель нелицензионного программного обеспечения не получает технической поддержки, своевременных обновлений, предоставляемых компаниями-разработчиками. Вместе с ним он покупает и вирусы, способные нанести вред системе компьютерной безопасности. Ответ на вопрос о необходимости наличия в штате организации собственных специалистов по информационной безопасности однозначен – да, нужны. Внешний консалтинг не сможет решить все вопросы информационной безопасности. При помощи консалтинга можно выявить и формализовать потребности бизнеса, грамотно обосновать необходимость затрат, написать проекты организационно-распорядительной документации, запустить комплекс технических средств, организовать его техническое сопровождение. Но многие функции отдавать внешним специалистам по разным причинам неправильно. Например, такие как информирование высшего менеджмента, защита бюджетов, проведение расследований инцидентов информационной безопасности, организация работы по обучению и информированию персонала, контроль за соблюдением норм информационной безопасности в его организационной части, аудит действий администраторов автоматизированных систем. Более того, любая заинтересованная в обеспечении информационной безопасности организация должна иметь в штате подразделение информационной безопасности, которое должно подчиняться высшему руководству и быть независимым от других подразделений. Наличие в штате организации специалистов, имеющих соответствующее образование, предусмотрено и законодательством. Например, наличие собственных систем дистанционного банковского обслуживания с применением технологий электронной цифровой

подписи, т.е. средств криптографической защиты информации, автоматически подпадает под Закон о лицензировании отдельных видов деятельности, в частности требуется лицензия ФСБ России на обслуживание шифровальных (криптографических средств), а данная лицензия, как и все остальные лицензии ФСТЭК (Федеральная служба по техническому и экспортному контролю) России и ФСБ России, связанные с деятельностью по защите информации, предполагает штатных специалистов по информационной безопасности [1; 3].

Актуальность проблемы, связанной с обеспечением безопасности информации, возрастает с каждым годом. Наиболее часто потерпевшими от реализации различных угроз безопасности являются финансовые и торговые организации, медицинские и образовательные учреждения. Если посмотреть на ситуацию десятилетней давности, то основной угрозой для организаций были компьютерные вирусы, авторы которых не преследовали каких-то конкретных целей, связанных с обогащением. Современные хакерские атаки стали более изощренными, организованными, профессиональными, разнообразными и, главное, имеющими конкретную цель. Например направленными на хищение данных банковских счетов в конкретных банковских системах. Совершенствование сферы информационных услуг, особенно в сфере дистанционного банковского обслуживания, способствует развитию интеллекта киберпреступников. Статистика подтверждает необходимость комплексной системы защиты информации. В России, как и за рубежом, она обусловлена двумя во многом пересекающимися группами факторов: требованиями бизнеса и законодательства. К требованиям бизнеса относятся:

– минимизация рисков, связанных с утечками информации;

– безопасность ключевых бизнес-процессов;

– выполнение требований информационной безопасности в рамках договоров с контрагентами.

Должный уровень информационной безопасности организации обеспечивает дополнительную привлекательность в лице партнеров, заказчиков или инвесторов. В части российского законодательства основным стимулом для

развития информационной безопасности является Федеральный закон от 27.07.06 г. №152-ФЗ «О персональных данных» (в ред. от 29.07.2017 г.), требования которого распространяются практически на все российские организации. Для выполнения требований законодательства необходимо руководствоваться нормативно-методологической базой ФСТЭК России (в части, касающейся некриптографических методов защиты информации) и ФСБ России (в части, касающейся криптографических методов защиты информации), а также стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», который пока носит рекомендательный характер для финансовых организаций [2, 3].

Распространение на российские организации требований международных стандартов информационной безопасности, как правило, имеет добровольный характер. Однако некоторые виды деятельности требуют обязательного выполнения международных стандартов, например стандарт PCI DSS (*Payment Card Industry Data Security Standard* – стандарт безопасности данных индустрии платежных карт, разработанный Советом по стандартам безопасности индустрии платежных карт, учрежденным международными платежными системами Visa, MasterCard, American Express, JCB и Discover). Стандарт представляет собой совокупность двенадцати детализированных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платежных карт. PCI DSS является обязательным для выполнения банковскими организациями с собственным процессингом платежных карт [4; 5].

Для построения комплексной системы защиты информации необходимо понимание руководством актуальности проблемы. Создание системы обычно закладывается и формулируется в документе «Политика информационной безопасности», доступность которого для каждого сотрудника – одно из многочисленных необходимых условий эффективного результата. Для разработки

политики информационной безопасности следует провести подготовительную работу – выявить потребности бизнеса в области информационной безопасности (это первый этап построения системы). На этапе обследования к активному участию привлекаются руководители бизнес-подразделений, являющихся ключевыми с точки зрения критичности бизнеса. Результатом обследования становятся зафиксированные и формализованные потребности всех заинтересованных сторон в обеспечении информационной защиты. Сегодня вопрос об осуществлении информационной безопасности волнует организации любого уровня. Таким образом, следует разрабатывать и внедрять внутри компании четко сформулированную коммуникационную (или информационную) политику.

Список литературы

1. Михнев И.П. Мультимедийные технологии в образовательном процессе // Современные наукоемкие технологии. – 2004. – №2. – С. 109–112.

2. Митячкина Е.С. Правовое регулирование положения главы местной администрации и муниципального служащего в Российской Федерации / Е.С. Митячкина, С.В. Михнева // Гуманитарные исследования: журнал фундаментальных и прикладных исследований. ФГБОУ ВПО «Астраханский государственный университет». – 2016. – №2 (58). – С. 157–162.

3. Кузнецов И.Н. Бизнес-безопасность. – 4-е изд. – М.: Дашков и К, 2016. – 416 с.

4. Михнев И.П. Обучение и контроль знаний студентов с помощью UniTest // Фундаментальные исследования. – 2008. – №1. – С. 94–95.

5. Чернышев П.М. Использование интернет-ресурсов в юридической практике // Марийский юридический вестник. – 2016. – №4(19). – С. 34–36.

6. «Финансовая газета»: «комплексная система защиты информации» [Электронный ресурс]. – Режим доступа: http://www.technoserv.com/about/company/press/articles/554/ (дата обращения: 19.12.2017).