УДК 004.056 + 004.451.36 + 658.1:004.056

ОБ ОСОБЕННОСТЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО БИЗНЕСА

И.А. Прохорова, Л.Ю. Овсяницкая

Показано, что информация является ценнейшим ресурсом бизнеса. Проанализированы места уязвимости малого бизнеса, способствующие овладению кибермошенниками персональными данными сотрудников и информацией, позволяющей похитить средства с банковских счетов работников и предприятия в целом. Доказано, что принимаемые решения должны позволить реализовать оптимальную защиту информационной системы и данных – обеспечить максимально возможный результат при ограниченных вложениях средств.

Ключевые слова: информационные технологии, информационная безопасность, малый бизнес, киберугрозы, алгоритмы защиты коммерческой тайны.

В настоящее время невозможно представить направление малого бизнеса, не использующего информационные технологии для проведения финансовых расчетов, организации документооборота, рекламы своей дея-

тельности, поиска поставщиков и покупателей, реализации онлайн-сервисов, использования информации как объекта товарно-денежных отношений.

Однако существуют факторы, которые могут не только дезорганизовать работу любого предприятия или организации, но и остановить на какое-то время всю деятельность, что является недопустимым явлением, ведущим к материальным и репутационным потерям. Речь идет об информационной безопасности и о способах и методах организации защиты информации.

Понимая достаточно высокий уровень информационной безопасности, присутствующий в крупных компаниях, обусловленный высокой квалификацией сотрудников IT-отделов, использованием лицензионного информационного обеспечения и вложениями средств в обеспечение безопасности в целом, киберпреступники все бóльшее внимание начинают уделять уязвимому среднему и малому бизнесу как наиболее легкому способу овладения персональными данными сотрудников и информацией, позволяющей похитить средства с банковских счетов работников и предприятия в целом.

Специалисты «Лаборатории Касперского» периодически проводят опросы специалистов, занимающихся информационными технологиями и занятых в малом, среднем и крупном бизнесе во всем мире. Цель данных исследований заключается в изучении мнения людей, касающегося различных вопросов информационной безопасности: об используемом специализированном программном обеспечении, о знаниях и готовности противостоять киберугрозам, о проблемах, связанных с вопросами кибербезопасности, которые могут возникнуть в ближайшей перспективе.

Полученные результаты выявляют современные тенденции в сфере информационной безопасности и отображают объективную ситуацию наличия проблем в области информационной безопасности бизнеса. Итоги исследования показали следующие результаты [1]:

– 41 % компаний обозначили защиту конфиденциальных данных от целевых атак главным приоритетом деятельности в области информационных технологий;

– 91 % компаний недооценивают опасности и количество существующего вредоносного программного обеспечения;

– антивирусное программное обеспечение является наиболее распространенной мерой обеспечения информационной безопасности в организациях;

– в течение года 98 % предприятий сталкиваются с инцидентами кибербезопасности, источники которых находятся за пределами компании;

– четверть компаний теряют данные в результате внешних кибератак;

– 87 % компаний пострадали от внутренних угроз, почти четверть (24 %) таких инцидентов привели к потере конфиденциальных данных;

– ущерб от одного инцидента информационной безопасности в среднем составляет около 20 млн рублей для крупной компании и свыше 780 тыс. рублей для компании сегмента среднего или малого бизнеса;

– на ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн руб., а небольшие – около 300 тыс. рублей;

– чаще всего в результате инцидентов кибербезопасности компании теряют операционные данные о внутренней деятельности, персональные данные клиентов и финансовые сведения.

Таким образом, ведение бизнеса в современных условиях невозможно без решения задач защиты информации. В том случае, когда речь идет о сегменте крупного бизнеса, данным вопросам уделяется большое внимание. Структура организации информационной системы, используемые проверенные лицензионные специализированные программные продукты, хранение данных на собственных надежных серверах, использование многофакторных средств аутентификации и идентификации пользователей с целью получения ими доступа к информации позволяют надежно защитить информацию, содержащую государственную, персональную и коммерческую тайну.

Однако в сегментах среднего и малого бизнеса данными проблемами занимаются гораздо меньше, чем требует текущая ситуация. Существует три причины подобного поведения:

1. Некомпетентность сотрудников, отвечающих за внедрение и использование информационных технологий и принимающих решения о приобретении программного и аппаратного обеспечения.

2. Неосведомленность руководителей в вопросах текущего состояния защиты информации и возможных последствий игнорирования данного вопроса, приводящая к безответственному отношению к данным проблемам.

3. Нежелание или невозможность выделения финансовых средств на обеспечение информационной безопасности, на обучение сотрудников, на приобретение современного программного и аппаратного обеспечения, использование бесплатных сервисов, программного обеспечения и облачных хранилищ данных.

Указанные выше причины редко встречаются изолированно друг от друга, чаще всего незнание руководителей организации темпов развития современных киберугроз приводит к нежеланию выделения финансовых средств на защиту информации и отсутствию внимания к уровню компетенций в области информационной безопасности сотрудников, принимаемых на работу, к непониманию необходимости обучения уже работающих в организации людей.

Подтверждением этому служат данные исследований «Лаборатории Касперского», цель которых заключалась в выявлении уровня осведомлен-

ности представителей российского бизнеса в оценке количества нового вредоносного программного обеспечения, которое появляется каждый день. Оценка руководителями и сотрудниками компаний реального существующего уровня киберугроз является главным фактором, оказывающим влияние на принимаемые меры для защиты информации.

На рис. 1 представлены полученные результаты.

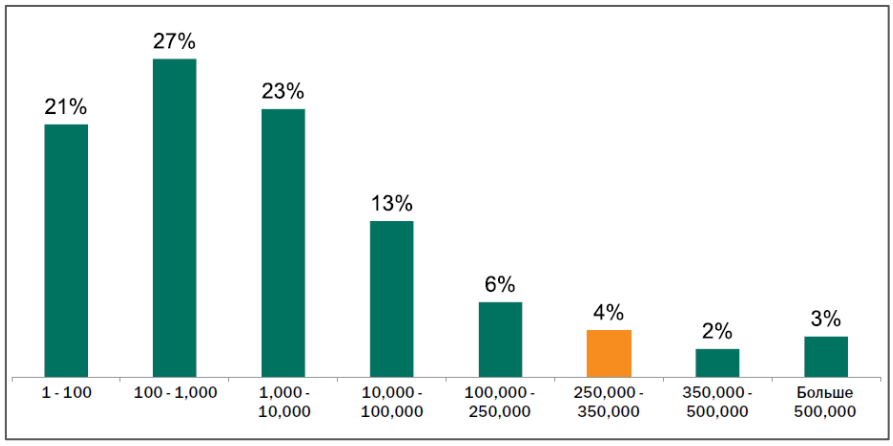

Рис. 1. Предположения сотрудников российского бизнеса относительно числа ежедневно появляющегося вредоносного программного обеспечения

На рис. 1 выделено реальное значение числа нового вредоносного программного обеспечения, которое появляется каждый день (4 %). Мы видим, что правильное предположение высказали только 4 % респондентов, при этом 91 % респондентов ее занизили.

Как известно, существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Источники угроз при этом делятся на внешние и внутренние [2]. Источниками внутренних угроз являются:

– сотрудники организации;
– программное обеспечение;
– аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;
– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;
– ошибки в работе программного обеспечения;
– отказы и сбои в работе компьютерного оборудования.

На рис. 2 представлены категории внутренних угроз, детализированные по признакам нанесения вреда компаниям (по данным «Лаборатории Касперского»).

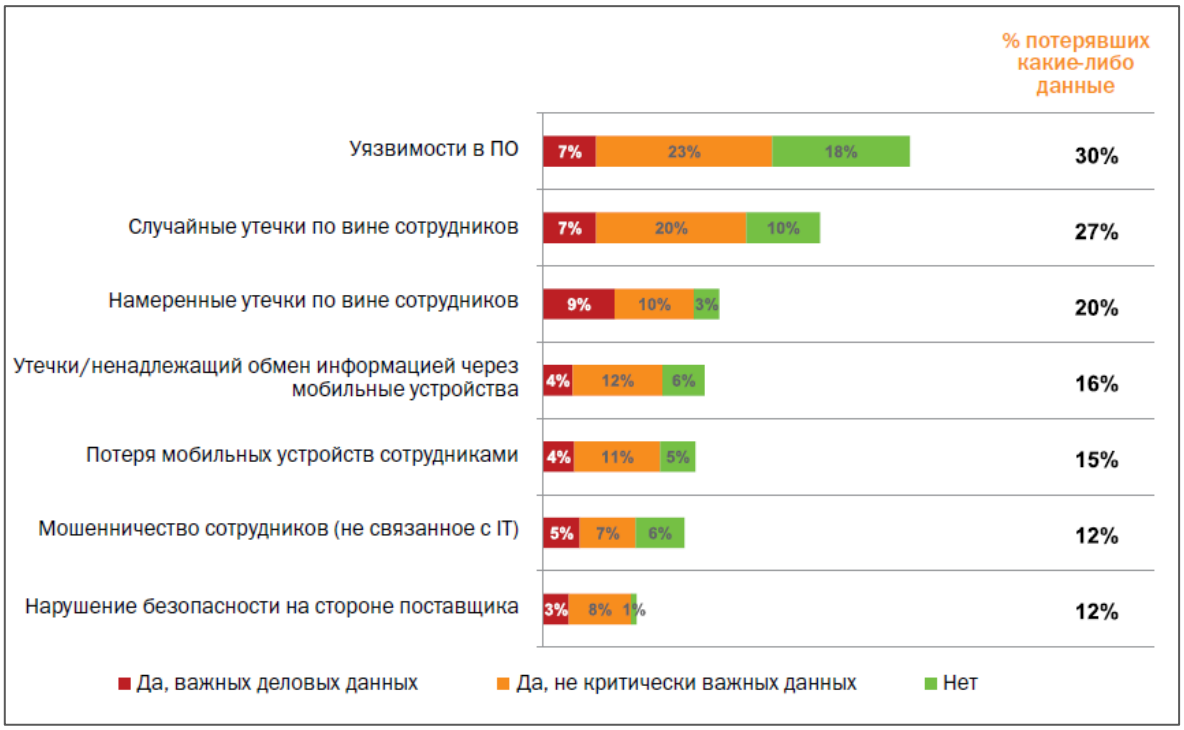

Рис. 2. Внутренние киберугрозы бизнеса

Анализ результатов показывает, что максимальный ущерб бизнесу (30 %) наносят уязвимости в программном обеспечении. Особенно остро этот вопрос стоит в случае использования бесплатного программного обеспечения, публичных облачных хранилищ данных и использования паролевой защиты для доступа к информационным ресурсам. Все указанные средства и методы не способны предоставить гарантированную защиту от компрометации и потери данных.

При установленных лицензионных информационных системах управления предприятием, электронного документооборота и рабочих мест специалистов, использовании собственных серверов для хранения информации и обеспечения многофакторной защиты доступа к информационным ресурсам, основанной на принципах биометрии или с использованием аппаратных устройств, сводят практически к нулю вероятность потерь информации по причине уязвимости в программном обеспечении. Заметим, что пункты, не требующие больших вложений материальных средств, например, утечка информации по преднамеренной или случайной вине сотрудников, потеря мобильных устройств сотрудниками, мошенничество сотрудников и т.д., одинаково вероятны и опасны как в сегменте крупного, так и среднего и мелкого бизнеса.

Высокий процент потерь данных (27 %) в компаниях вызван случайными утечками информации, возникшими по вине сотрудников. Причинами безответственного отношения к выполнению требований информационной безопасности являются отсутствие знаний в области IT-безопасности

и, соответственно, понимания важности досконального соблюдения имеющихся законов, а также правил, требований и организационных мероприятий, существующих в данной компании. К безответственному отношению к выполнению обязанностей также относится и потеря сотрудниками мобильных устройств, хранящих или использующих данные бизнеса.

Выходом из сложившейся ситуации является постоянное обучение сотрудников основам, методам и приемам защиты информации, освоение алгоритмов работы при осуществлении сбора, модификации, утечки и уничтожении информации, ознакомление с рисками и последствиями, вызванными потерей или компрометацией данных, содержащих государственную, персональную или коммерческую закрытую информацию.

В 20 % случаев наблюдалась целенаправленная утечка информации. В том случае, если правоохранительными или следственными органами будет доказана вина сотрудника, то в зависимости от типа информации, последствий и полученного правообладателем ущерба действия сотрудника подпадают под гражданскую или уголовную ответственность. Из рис. 2 видно, что 9 % похищенной информации относится к важной деловой информации.

К внешним источникам угроз относятся:

– компьютерные вирусы и вредоносные программы;
– организации и отдельные лица;
– стихийные бедствия.

Формами проявления внешних угроз являются:

– заражение компьютеров вирусами или вредоносными программами;
– несанкционированный доступ (НСД) к корпоративной информации;
– информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
– аварии, пожары, техногенные катастрофы.

На рис. 3 представлены категории внешних угроз, детализированные по признакам нанесения вреда компаниям (по данным «Лаборатории Касперского»).

На рис. 3 показано, что самой значимой внешней угрозой, с которой столкнулись 77 % компаний, является вредоносное программное обеспечение. Данная ситуация возникает в случае отсутствия установленных лицензионных полнофункциональных программных продуктов, защищающих компьютер и информационную систему в целом от вредоносных программ. Предлагаемое бесплатное или условно-бесплатное программное обеспечение никогда не будет поддерживать полный функционал средств защиты, существующих в коммерческих версиях: блокирование вирусов и шпионских программ, обеспечение безопасности покупок в Интернете, блокирование спама и фишинговых сообщений, защита конфиденциально-

сти данных, наличие брандмауэра, предотвращение хакерских атак, защита денежных операций, предупреждение о подмене доменных адресов на мошеннические и другое.

Рис. 3. Внешние киберугрозы бизнеса

Бесплатное программное обеспечение, допустимое при использовании компьютера исключительно в бытовых или развлекательных целях, не предполагающее хранение и обработку персональной и, тем более, государственной или коммерческой информации, как правило, только блокирует вирусы и шпионские программы. Поэтому использование подобных версий программного обеспечения категорически запрещено в любом сегменте бизнеса.

Высокий процент спама или нежелательных электронных писем и наличие фишинговых атак (74 % и 28 % соответственно) являются прямым следствием отсутствия установленного полнофункционального программмного обеспечения, защищающего от вредоносного программного обеспечения.

Похищаемые кибермошенниками данные (по результатам исследований «Лаборатории Касперского») имеют следующий вид (рис. 4).

Таким образом, можно сделать вывод о том, что заниженная оценка уровней существующих внутренних и внешних киберугроз, отказ или низкий уровень инвестирования в комплексные средства информационной безопасности и в обучение сотрудников в данной области может привести к значительным финансовым и репутационным потерям.

Рис. 4. Типы данных, похищаемых кибермошенниками

Убытки от произошедших инцидентов складываются из расходов на внешнее профессиональное обслуживание (приглашенные эксперты и специалисты по информационной безопасности, юристы и т.д.), из упущенных бизнес-возможностей (подорванная репутация среди коллег и доверие клиентов, расторжение или срыв контрактов и т.д.), а также ущерба от вынужденного простоя по причине блокирования IT-процессов компании и остановки деятельности на период восстановления информационных процессов и данных.

Заключение. Информация является ценнейшим ресурсом бизнеса. Защита данных, содержащих государственную тайну и персональные сведения людей, регламентируется законами Российской Федерации и обязательна для исполнения. Алгоритмы защиты коммерческой тайны необходимо задавать самостоятельно, в зависимости от специфики и величины каждого предприятия или организации.

Особенностью малого бизнеса являются ограниченные финансовые возможности, выделяемые на средства и методы защиты информации. Поэтому принимаемые решения должны позволить реализовать оптимальную защиту информационной системы и данных – обеспечить максимально возможный результат при ограниченных вложениях средств.

Библиографический список

1. Информационная безопасность бизнеса: исследование текущих тенденций в области информационной безопасности бизнеса: [Электронный ресурс]. – URL: http://www.www.kaspersky.ru.

2. Овсяницкая, Л.Ю. Актуальные вопросы защиты информации (на примере промышленных предприятий и учреждений здравоохранения г. Челябинска) / Л.Ю. Овсяницкая // Национальные интересы: приоритеты и безопасность. – 2013. – № 21(210). – С. 54–59.

3. Прохорова, И.А. Практические аспекты обучения студентов работе с данными в контексте экономического, медицинского и инженерного образования / И.А. Прохорова, Л.Ю. Овсяницкая // Сборник трудов 67-й научной конференции «Наука ЮУрГУ». – Челябинск: ЮУрГУ (НИУ), 2015. – С. 475–481.

К содержанию