1. Электронный бизнес и электронная коммерция // MARKET-PAGES.RU. Информационный бизнес портал [Электронный ресурс]. URL: http://market-pages.ru/inmark/4.html
2. Предпринимательство. Электронный бизнес // Пуск!by [Электронный ресурс]. URL: http://refu.ru/refs/66/33933/1.html

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лисова М.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жилинская Н.Н. – к.э.н.,доцент

Под риском информационной безопасности понимается возможность того, что данная угроза будет использовать уязвимости информационного актива (группы активов) и, тем самым, нанесет вред организации. Он измеряется комбинацией вероятности нежелательного события и его последствий (возможного ущерба). В последние годы проблема рисков информационной безопасности стала как нельзя актуальной, причиной тому послужил серьезный ущерб, влияющий не только на финансовую составляющую.

Для эффективной деятельности организации необходимо обладать полной, достоверной, актуальной информацией, благодаря которой можно получить определенные преимущества в процессе её функционирования. В связи с современными условиями развития информационных технологий, все чаще используются автоматизированные информационные системы, которые позволяют значительно повысить уровень управления организацией. Однако использование информационных систем и технологий связано с определенным количеством рисков, представляющих серьёзную угрозу для эффективного функционирования любого бизнеса. А сегодня, обладая определенными знаниями и навыками, практически не составляет труда завладеть какими-либо данными. Все более актуальным становится риск потери контроля и, как следствие, утечки конфиденциальной информации.

По данным Positive Technologies, большинство кибератак (покушения на информационную безопасность) в 2018 году предсказуемо совершалось с целью обогащения (получения финансовых выгод) или получения конфиденциальных данных. При этом атаки, направленные на получение информации, зачастую также содержат финансовый подтекст: украденные данные затем используются для кражи денег, шантажа или размещаются для продажи на теневом рынке [1]. Проанализировав кибератаки на отдельные отрасли, которые чаще всего становились целью злоумышленников в 2018 году, имеем: 23% кибератак затронули частных лиц; среди юридических лиц в 19% инцидентов жертвами стали государственные учреждения, еще в 11% случаев пострадали медицинские учреждения, а в 10% — финансовые организации, на IT-компании же пришлось 5% от всех атак, 4% - в торговли, в сфере услуг, на криптовалютных биржах [1]. Согласно опросу, проведенному в рамках международного исследования компанией EY, многие компании не уверены, что они успешно выявляют все инциденты и случаи нарушения информационной безопасности (ИБ). Среди тех, кто стал жертвой инцидента за последний год, менее трети указывают, что взлом системы был выявлен их центром безопасности. Как отмечается в исследовании компании EY, 76% организаций повысили расходы на информационную безопасность уже после её серьезного нарушения [2].

Ущерб от утечки информации, по данным Лаборатории Каперского 2018, составляет: для крупных корпораций во всем мире средняя стоимость утечки данных сейчас составляет чуть более $1,23 млн., что выше 2017 года на 23% и 2016г. на 38%; для малого и среднего бизнеса ущерб от утечек данных вырос на 36%: с $88 тыс. в 2017 году до $120 тыс. в 2018 году [3]. Как результат, средний бюджет на обеспечение безопасности увеличился в зависимости от размеров компании. Крупные корпорации тратят в среднем около $8,9 млн. на информационную безопасность, в то время как малый и средний бизнес увеличили свой бюджет в среднем с $201 тыс. в 2017 году до $246 тыс. в 2018 году [3]. Проанализировав множество результатов исследований в области информационной безопасности, можно отметить, что одной из основных причин увеличения ущерба от утечек данных является отсутствие надежного плана действий (стратегии) на случай нарушения информационной безопасности. Последствиями утечек данных в организациях зачастую являются крупные финансовые потери или даже банкротство, риски репутации, потери ноу-хау. В частности, по статистике Ponemon Institute, 2/3 малых и средних компаний закрываются в течение полугода после утечки данных. Крупные компании в целом переживают подобные инциденты, но несут существенные финансовые потери [4].

Пользователи - это своего рода актив какой-либо компании, такой же, как и здания, сырье, технологии (взяв, например, компанию Facebook или Google, для которых пользователи

есть не что иное, как актив, источник получения прибыли). Следовательно, утечки данных могут привести не только к крупным финансовым потерям, как отмечалось выше, но и к потере репутации, сказаться на котировке акций и капитализации компании. Если размышлять о том, кто получает выгоды от утечки данных, можно уверенно утверждать: никаких выгод не получают законопослушные граждане и компании. Таким образом, получает выгоды тот, кто в дальнейшем вовлекает эти данные в хозяйственный оборот.

Рассмотрев уровень информационной безопасности в мире по данным NCSI (e-Governance Academy) по состоянию на февраль 2019 года, имеем: на первом месте по уровню национальной кибербезопасности находится Чехия с индексом в 90.91 (в июне 2018 г. этот показатель составлял 75.03, 10 место); в России данный индекс составил 64.94, 22 место; США – 63.64, и 28 место; Беларусь же занимает 41 место с индексом в 53.25 (в 2018 году – 55.85, 33 место в мире) [5]. Согласно последнему опубликованному отчету ООН по Глобальному индексу кибербезопасности (GCI 2017), на первом месте в мире находится Сингапур (0,925), на втором – США (0,919), Россия - 10 место (0,788), Беларусь - 39 место с индексом 0,592 (83 место в 2015 г.) [6].

В частности, анализируя состояние информационной безопасности в Беларуси по GCI 2015 и 2017 гг., заметно, что страна сделала значительный скачок по ряду показателей. Например, в 2015 г. критерии «Организационные вопросы» и «Создание потенциала» были оценены нулевыми баллами, однако уже через два года, в 2017 году, эти показатели составили 0,33 и 0,68 соответственно, что привело к увеличению GCI Беларуси с 0,1765 (в 2015г.) до 0,592 (в 2018 г.) и к благополучному смещению в мировом рейтинге [6]. Несмотря на это, сравнив результаты исследований ООН и NCSI, видно, что на сегодняшний день в Беларуси всё же существует ряд серьезных проблем в области ИБ. Главными проблемами Беларуси является отсутствие плана по укреплению стратегии реализации ИБ в стране, законодательства по защите персональных данных, а также ответственности по ИБ для поставщиков цифровых услуг. Как показывает мировой опыт, решение этих проблем возможно только благодаря совместной работе бизнеса и государства. Сейчас государство остро заинтересовано во взаимодействии с ИТ-компаниями, сотовыми операторами, провайдерами, экспертным сообществом через мониторинг, аудит, различные варианты взаимодействия. К слову, расходы на ИБ в 2019 году составят около 1,2% от всех расходов государственного бюджета Беларуси, эта цифра не изменялась с 2016 г. (для сравнения, расходы на здравоохранение в 2019 составят 4,6%) [7].

Изучив исследование международной компании EY, можно выделить ряд общих для всех стран и организаций проблем и возможных мер для их устранения. Например [5]:

1) Несмотря на увеличение расходов на ИБ, количество атак меньше не становится. Одним из возможных путей решения проблемы можно назвать необходимость учёта ИБ в стратегии развития бизнеса как её неотъемлемую часть.

2) Компании имеют огромное количество партнеров, следовательно, они находятся в зависимости от мер безопасности, которые применяют их партнеры, по этой причине нужно разрабатывать программу по обеспечению ИБ для всей корпоративной системы или же определить для себя, насколько утечка данных ваших партнеров скажется на вашем бизнесе.

3) Зачастую функции по обеспечению ИБ и функции центров ИБ часто передаются на аутсорсинг, что также может стать причиной недостаточного уровня обеспечения, поэтому следует инвестировать в то, где инвестиции способны принести максимальный эффект, и искать оптимальный баланс между имеющимися ресурсами и возможностями внешних поставщиков.

Сейчас в мире существует ряд инструментов (мер) для борьбы с утечками информации в организации, однако эффективную защиту можно выстроить только благодаря двум действиям: 1) выявление ценных ресурсов и концентрирование инвестиций на защиту именно их; 2) использование современных продвинутых инструментов защиты (Threat Intelligence, Security Operations Centres; продвинутая стратификация, в том числе использование поведенческих профилей пользователей; средства аутентификации и прогнозирования угроз уязвимостей, тестирование защищенности). В то же время своего рода тренды в области ИБ приводят к повышению спроса на такие технологии как SIEM, NBAD, IRP, SOC, BI, с важной составляющей в сторону визуализации, метрик результативности и процессов информационной безопасности, что в свою очередь требует высококвалифицированных кадров и даже появления целого ряда новых должностей. Однако единственной технологии, способной защитить от всех современных угроз и атак, не существует. Для каждой организации актуален свой набор механизмов защиты в зависимости от критичности бизнеса, ИТ-технологий, размера инфраструктуры, наличия прямого взаимодействия с бизнес-партнерами и конечными пользователями с использованием веб- и мобильных технологий и т.д.

Подводя итог всему вышеизложенному, можно с уверенностью сказать, что на данный момент риски информационной безопасности представляют собой большую угрозу для нор-

мального функционирования многих организаций и в нынешних реалиях требуется не просто выявление угроз, но и, что более важно, их предотвращение.

Список использованных источников:

1. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
2. https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/%24FILE/ey-global-information-security-survey-rus.pdf
3. https://securelist.ru/ksb-threat-predictions-for-2018/88032/
4. https://www.kv.by/post/1054212-mest-shpionazh-i-nevnimatelnost-kak-kompanii-zashchititsya-ot-utechki-informacii
5. https://ncsi.ega.ee/ncsi-index/
6. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
7. http://www.minfin.gov.by/upload/bp/act/zakon_301218_160z.pdf

МИРОВОЙ ОПЫТ ЭЛЕКТРОННОЙ ТОРГОВЛИ

Сеидов Д.

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Карпук А.А. – к.т.н., доцент

Приведена краткая история развития электронной торговли в мире. Рассмотрено текущее состояние электронной торговли в Китае, США, Великобритании, Японии, Германии и Канаде.

Активное развитие информационных технологий и сети Интернет создают принципиально новые условия для развития бизнеса, постоянно происходит формирование новых рынков, возникновение спроса на новые товары и услуги, создание принципиально новых предложений. Одним из активно развивающихся направлений электронного бизнеса является электронная коммерция и ее составная часть - электронная торговля. Под электронной торговлей понимается оптовая или розничная торговля, характеризующаяся заказом, покупкой, продажей товаров с использованием информационных систем и сетей. В настоящее время электронная торговля наиболее развита в Китае, США, Великобритании, Японии и Германии.

По ряду причин в Туркменистане темпы развития электронной торговли пока отстают от многих стран. Целью научных исследований автора является разработка предложений по дальнейшему развитию электронной торговли в Туркменистане на основе мирового опыта. На первом этапе исследований был проведен анализ мирового опыта электронной торговли, результаты которого изложены в настоящей работе.

В 1960 г. в США были разработаны первые системы для ведения электронного бизнеса. При этом сделки проводились с помощью специальных протоколов обмена данными, что тормозило скорость обработки. С целью развития электронной коммерции были разработаны и внедрены более современные стандарты, например EDI. Эта система представляет собой набор правил и норм, касающихся электронного оформления различных бумаг – таможенных деклараций, заказов, накладных документов и т. д. Немного позже подобные стандарты появились и в Европе, в первую очередь, в Великобритании. В 1980 г. началась активная деятельность по объединению американских и европейских технологий, был разработан новый стандарт – EDIFACT, использующий протокол X400.

С 1995 г. начинается активное ведение электронных сделок. При этом к концу 1996 г. с использованием стандарта EDI было совершено сделок более чем на 300 млрд долл. США. С 2000 по 2001 г. темпы развития электронной предпринимательской деятельности немного спали. Это было вызвано общей ситуацией в мировой экономике. Чрезмерное финансирование глобальной сети и активное развитие аудитории привело к обвалу на 214 пунктов индекса NASDAQ. Итог – затяжной спад в экономике не только США, но и в странах всего мира. Основной причиной было отсутствие достаточного опыта у людей, которые впервые стали у руля такого бизнеса. По статистике почти 2/3 таких компаний оказались убыточными и потянули на «дно» экономику своих стран [1].

С 2001 по 2007 г. ситуация стабилизировалась и интернет-индустрия снова набрала темп. Появились специалисты в этой отрасли, бизнес в Интернете стал более продуманным. Многие предприниматели считали делом принципа открыть новый магазин и занять свою «ячейку» в глобальной мировой сети. При этом бизнесмены часто брали средства взаймы для создания собственного бизнеса. В течение 6 лет объем интернет-магазинов вырос почти на 17%. Людей привлекала в этот бизнес невероятная перспектива заработка и огромный рынок клиентов. Потенциальная прибыль исчислялась триллионами долларов.