М. А. Лисова,
студент II курса БГУИР
Научный руководитель:
кандидат экономических наук, доцент
Н. Н. Жилинская

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: РИСКИ И ЦЕНА УТЕЧКИ ДАННЫХ

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 ее 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 серьезную 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.

Целью данной работы является рассмотрение текущего состояния информационной безопасности как в мире, так и в Беларуси, а также анализ возможных последствий и потерь от утечек данных. Для достижения цели был выполнен ряд задач: проанализирован фактический материал, изучен характер утечек данных, выявлены их причины и последствия, сформулирован возможные проблемы и меры предотвращения кибератак.

По данным Positive Technologies, большинство кибератак (покушения на информационную безопасность) в 2018 г. предсказуемо совершалось в целях 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 г., 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 ее 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 долл. США, что выше 2017 г. на 23 % и 2016 г. на 38 %; для малого и среднего бизнеса ущерб от утечек данных вырос на 36 %: с 88 тыс. долл. США в 2017 г. до 120 тыс. долл. США в 2018 г. [3]. Как результат, средний бюджет на обеспечение безопасности увеличился в зависимости от размеров компании. Крупные корпорации тратят в среднем около 8,9 млн долл. США на информационную безопасность, в то время как малый и средний бизнес увеличили свой бюджет в среднем с 201 тыс. долл. США в 2017 г. до 246 тыс. долл. США в 2018 г. [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 (например, компании 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 украденные данные в хозяйственный оборот.

Рассмотрев уровень информационной безопасности в мире, по данным NCSI (e-Governance Academy) по состоянию на февраль 2019 г., 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 г. – 55,85, 33 место в мире) [5]. Согласно последнему опубликованному отчету ООН по Глобальному индексу кибербезопасности (GCI 2017), на 1 месте в мире находится Сингапур (0,925), на 2 – 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 г., эти показатели составили 0,33 и 0,68 соответственно, что привело к увеличению GCI Беларуси с 0,1765 (2015) до 0,592 (2018), и к благополучному смещению в мировом рейтинге [6]. Несмотря на это, сравнив результаты исследований ООН и NCSI, видно, что текущий момент в Беларуси все 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 г. составят около 1,2 % от всех расходов государственного бюджета Беларуси, эта цифра не изменялась с 2016 г. (для сравнения, расходы на здравоохранение в 2019 г. составят 4,6 %) [7].

Ближайшие практические шаги направлены на формирование правовой (институциональной среды) и технической основы для предоставления сервисов ИБ. Уже идут мероприятия по определению технических требований к центрам мониторинга информационной безопасности. В Беларуси существует оперативно-аналитический центр (ОАЦ) – государственный орган, осуществляющий регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий. Однако этого недостаточно. По мнению экспертов ООН, формирующих индекс GCI, необходимо также создание отраслевых центров информационной безопасности, а возможно, и национального центра информационной безопасности. К слову, зна-

чимые шаги уже сделаны: 18 марта 2019 г. была принята и опубликована Концепция информационной безопасности Беларуси, которая представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности, введена отдельная норма – кибербезопасность (элемент ИБ), посвящена целая глава государственно-частному партнерству, где описано взаимодействие между государством и бизнесом в целях привлечения компетенций, технологий, совместной реализации инвестиционных проектов. Данная концепция открывает новый этап в развитии информационной безопасности Беларуси, первые результаты которого, очень вероятно, мы уже сможем наблюдать в ближайшей оценке состояния информационной безопасности (ООН и NCSI).

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

1) Несмотря на увеличение расходов на ИБ, количество атак меньше не становится. Одним из возможных путей решения проблемы можно назвать необходимость учета ИБ в стратегии развития бизнеса как ее 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 проблемы и риски информационной безопасности представляют собой большую угрозу для нормального функционирования многих организаций, а в нынешних реалиях требуется не просто выявление угроз, но и, что более важно, их предотвращение.

Список использованных источников

1. Актуальные киберугрозы-2018. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/. – Дата доступа: 23.01.2019.

2. Международное исследование EY в области информационной безопасности, 2018–2019 гг. [Электронный ресурс]. – Режим доступа: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/%24FILE/ey-global-information-security-survey-rus.pdf. – Дата доступа: 02.02.2019.

3. Во сколько может обойтись потеря данных? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/economics-report-2018/20655/?utm_source=pr-media&utm_medium=partner&utm_campaign=ru_economics-report18_promo&utm_content=link&utm_term=ru_pr-media_promo_link_partner_economics-report18. – Дата доступа: 03.02.2019.

4. Месть, шпионаж и невнимательность. Как компании защититься от утечки информации? [Электронный ресурс]. – Режим доступа: https://www.kv.by/post/1054212-mest-shpionazh-i-nevnimatelnost-kak-kompanii-zashchititsya-ot-utechki-informacii. – Дата доступа: 02.02.2019.

5. National Cyber Security Index [Electronic resource]. – Mode of access: https://ncsi.ega.ee/ncsi-index/. – Date of access: 05.03.2019.

6. International Telecommunication Union [Electronic resource]. – Mode of access: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. – Date of access: 03.02.2019.

7. О республиканском бюджете на 2019 г. [Электронный ресурс] : Закон Респ. Беларусь, 30 дек. 2018 г. № 160-З // М-во финансов Респ. Беларусь. – Режим доступа: http://www.minfin.gov.by/upload/bp/act/zakon_301218_160z.pdf. – Дата доступа: 04.02.2019.