УДК 336.71.078.3

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ФИНАНСОВОГО СЕКТОРА: ЗАРУБЕЖНАЯ И ОТЕЧЕСТВЕННАЯ ПРАКТИКА

Бүркітбаева Айғаным Маратқызы
burkitbayevaai@gmail.com
Студент ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель – ст. преподаватель Кодашева Г.С.

Развитие технологий в современном мире происходит в ускоренном темпе. Все большую массовость приобретают социальные сети, онлайн транзакции, облачные хранилища и автоматизированные процессы. Но наряду с технологической эволюцией происходит и развитие киберпреступности, которая постоянно разрабатывает новые типы атак, инструментов и методов, позволяющих хакерам проникать в наиболее сложные или

наиболее контролируемые среды, при этом наносить большой урон, особенно в финансовой сфере.

Под киберпреступлениями подразумеваются противоправные действия с использованием высоких технологий с целью извлечения экономической, политической или иной выгоды. Преступления производятся посредством кибератак, то есть покушения на информационную безопасность компьютерных систем. Одними из наиболее популярных мишеней среди киберпреступников являются кредитные организации, в частности коммерческие банки.

Принято считать, что главные угрозы для банков появляются из внешней среды, например действия конкурентов, хакерские атаки, утечки и другие неприятности, а отделы информбезопасности сталкиваются с ними ежедневно.

Самое ценное в наши дни – это информация. С ростом ценности информации в мире эволюционировали и способы ее защиты. Сегодня такие компании, как Google или Facebook, куда лучше оберегают данные миллионов своих пользователей, чем банки. В крупных IT-компаниях безопасность буквально «встроена» внутрь самих продуктов и является обязательной их составляющей [1].

В Казахстане Национальный банк РК принял Стратегию кибербезопасности финансового сектора на 2018-2022 годы (далее – Стратегия), которая утверждена в рамках реализации Концепции кибербезопасности («Киберщит Казахстан»). Данная Стратегия включает в себя комплекс целей, задач и мероприятий, достижение, решение и реализация которых позволит обеспечить создание эффективно функционирующей системы кибербезопасности финансового сектора РК. Основной целью Стратегии является создание условий для безопасного предоставления финансовых услуг, что необходимо для обеспечения стабильного функционирования и развития финансового сектора страны.

Концепция кибербезопасности («Киберщит Казахстана») разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира. Концепция «Киберщит Казахстан» призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

При разработке Концепции изучен международный опыт в области формирования подходов к защите национальной информационно-коммуникационной инфраструктуры государств-лидеров в сфере разработки и использования информационно-коммуникационных технологий, так и стран, стремящихся расширить сферу их применения для достижения целей социально-экономического развития.

Целями Концепции являются достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.

Задачи Концепции:

1. Формирование необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно-технического воздействия и защищенного телекоммуникационного оборудования.

2. Совершенствование правоприменительной практики, методологической базы, нормативно-правового и организационно-технического обеспечения безопасного

использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами.

3. Создание высоко адаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно-коммуникационной инфраструктуры.

Ожидаемые результаты:

1) глобальный индекс кибербезопасности Казахстана к 2017 году составит 0,200, к 2018 году – 0,300, к 2019 году – 0,400, к 2020 году – 0,500, к 2021 году – 0,550, к 2022 году – 0,600;

2) повышение осведомленности об угрозах информационной безопасности к базовому периоду 2018 года в 2019 году – на 5%, в 2020 году – на 10%, в 2021 году – на 15%, в 2022 году – на 20%;

3) количество переподготовленных специалистов в сфере информационной безопасности в 2018 году – 300, в 2019 году – 500, в 2020 году – 600, в 2021 году – 700, в 2022 году – 800;

4) увеличение доли отечественных программных продуктов в сфере информатизации и связи, используемых в государственном и квазигосударственном секторах к базовому периоду 2017 года в 2018 году – на 10%, в 2019 году – на 20%, в 2020 году – 30%, в 2021 году – 40%, в 2022 году – 50%;

5) доля использования отечественных сертификатов безопасности при шифрованной передачи данных Интернет-ресурсами с доменом .KZ и .ҚАЗ в 2018 году составит 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, в 2022 году – 100%;

6) доля информационных систем государственных органов, негосударственных информационных систем, интегрируемых с государственными, информационных систем критически важных объектов информационно-коммуникационной инфраструктуры, подключенных к центрам мониторинга информационной безопасности, в 2018 году – 20%, в 2019 году – 40%, в 2020 году – 60%, в 2021 году – 80%, к 2022 году – 100%.

Период реализации Концепции включает два этапа:

1) первый этап 2017-2018 годы;

2) второй этап 2019-2022 годы.

На первом этапе будут:

- сформирована развернутая правоприменительная практика соблюдения уже установленных требований в сфере обеспечения информационной безопасности, по результатам которого будут внесены необходимые изменения в законодательство;

- проведена ревизия образовательных программ и профессиональных стандартов, увеличено количество и качество подготавливаемых специалистов в области информационной безопасности, обеспечено повышение квалификации действующих работников, занятых в этой сфере;

- выстроена эффективная схема взаимодействия и кооперации между промышленностью и наукой в создании отечественных разработок, что создаст основу для развития национального и отраслевых оперативных центров информационной безопасности, что позволит на втором этапе обеспечить:

- ключевое участие казахстанских IT-компаний в обеспечении национальной информационно-коммуникационной инфраструктуры системами информационной безопасности;

- загрузку отечественных предприятий электронной промышленности заказами на приобретение государственными органами и квазигосударственным сектором телекоммуникационного оборудования, произведенного и прошедшего процедуры сертификации на соответствие требованиям информационной безопасности на территории страны.

Начиная с 2015 года, Нацбанк РК регулярно получает информацию по понесенным банками убыткам, связанным с реализацией рисков информационной безопасности. Так, на

2015 год заявленный ущерб банков составил около 61 миллиона тенге, в 2016 году более 2 миллиардов тенге и за первое полугодие 2017 года ущерб составил более 11 миллионов тенге. Между тем популярность приобретения и использования электронных денег растет. Так, в 2017 году по сравнению с 2016 годом количество операций с электронными деньгами выросло на 88,1%, объем возрос в 2,3 раза. На конец 2017 года выпуск электронных денег осуществляли 13 банков, при этом для населения на рынке было представлено 17 систем электронных денег. С учетом общемировых тенденций, ожидается, что потребность в данном инструменте будет и дальше возрастать. Доля мошеннических операций от общего объема операций с использованием платежных карточек в 2017 году, по данным банков, составила 0,002% (в 2016 году доля составляла 0,003%) [2].

С учетом глобальных тенденций по переходу на электронные банковские услуги безналичные платежи с использованием платежных карточек казахстанских эмитентов в 2017 году по сравнению с 2016 годом выросли по количеству на 92,5%, по сумме на 88,2%, составив 232 млн операций на сумму Т3 048,5 млрд. За 2017 год посредством интернет и мобильного банкинга с использованием платежных карточек было совершено 91,8 млн операций на сумму Т1,2 трлн. В Казахстане на 1 января 2018 года 73% банков второго уровня (24 банка) предоставляют услуги мобильного банкинга для физических лиц [3].

В Нацбанке РК отмечают, что из-за отсутствия на государственном уровне утвержденных стандартов, требований и порядков по обеспечению кибербезопасности, «реализация мер и контроля по защите производится исходя из опыта отдельных работников и возможностей, заложенных разработчиками информационных систем, программного и аппаратного обеспечения». Крупные банки, по данным финрегулятора, «самостоятельно создают и успешно эксплуатируют центры и службы реагирования на инциденты кибербезопасности» [4].

Термин «кибербезопасность» и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

В тоже время на уровне ООН имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно-коммуникационных технологий в вопросах обеспечения (1) неприкосновенности частной жизни, (2) конфиденциальности, целостности и доступности информации в электронной форме, (3) защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно-техническими методами.

При этом многие страны не рассматривают в руководящих документах вопросы защиты от вредной или незаконной информации, распространяемой с использованием ИКТ в контексте понимания кибербезопасности из-за опасений в чрезмерном ограничении права на доступ и свободное распространение информации.

Рассматривая международный опыт по кибербезопасности Annual Fraud Indicator отмечает, что интернет-мошенничество обошлось Великобритании в 2016 году в £193 млрд. Это означает, что каждую секунду убыток составлял £6 тыс. В 2016 году у 9000 клиентов Tesco Bank были украдены средства на общую сумму £2,5 млн. В США в ушедшем году многочисленным атакам подвергался банк JP Morgan Chase. Несмотря на это, по некоторым данным, внимание банков к вопросам безопасности оставляет желать лучшего [5].

Так, например в Центральном банке Бангладеша, заметив признаки неполадок, банк выявил проблему, связанную с печатью. Пришедшие утром в офис сотрудники обнаружили, что лотки для бумаг, которые всегда в течение ночи наполняются печатными

материалами с подтверждениями проведения международных транзакций в системе SWIFT, были пусты. Сначала сотрудники решили, что проблема обусловлена сбоем в работе принтера, однако позже было выяснено, что банк стал жертвой интернет-взлома. К тому времени как банк определил, что причина гораздо глубже простой неисправности оборудования, он уже потерял в регионе $101 млн [6].

Ранее стало известно о том, что хакерская группа Cobalt в 2017 году провела 11 успешных атак вируса Cobalt Strike на российские банки и похитила 1,156 млрд рублей. Группа Cobalt атакует российские, европейские и азиатские банки в разных странах мира. Cobalt проникает в банковскую сеть через рассылку фишинговых писем – от имени государственных регуляторов, производителей банкоматов или партнерских банков. После открытия писем активируется вирус, и хакеры через внутреннюю сеть банка получают доступ к банкоматам или SWIFT.

ФинЦЕРТ – Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России – выпустил отчет о ситуации с кибербезопасностью финансовой сферы России. Из него следует, что успешных хакерских атак на банки в 2018-м стало по сравнению с предыдущим годом заметно меньше, а вот юридическим лицам и индивидуальным предпринимателям стоит срочно укреплять защиту от хакеров.

Как отмечают «Ведомости», за первые восемь месяцев текущего года атаки на российские банки принесли злоумышленникам 76,5 млн рублей, в то время как за те же месяцы 2017-го – 1,08 млрд рублей. И это несмотря на рост числа атак с 20 до 22.

Причиной того, что хакерам все реже удается похитить у кредитно-финансовых организаций заметные суммы, стало повышение общего уровня кибербезопасности банков. Например, более эффективно фильтруются фишинговые письма – основной механизм заражения компьютерных систем вредоносным ПО.

По мнению ФинЦЕРТа, киберпреступники будут постепенно переключаться с атак против самих банков на их клиентов, куда менее защищенные юридические лица. Киберэксперты ЦБ предупреждают, что число хищений у бизнеса, особенно малого и среднего, а также у индивидуальных предпринимателей может возрасти. Такие цели почти всегда более уязвимы, так как в компаниях, как правило, относятся к кибербезопасности далеко не так серьезно, как в банках.

Более трети банков оценивает свои потери от одного дня кибератаки в сумму до 2 млн рублей. Об этом говорится в исследовании Positive Technologies, специализирующейся на вопросах кибербезопасности. При этом большинство кредитных организаций тратит на защиту от взлома до 50 млн рублей. В прошлом году все эти показатели были на 10–15% ниже, подсчитали в компании Zecurion, разрабатывающей системы безопасности для банков. Расходы растут из-за активизации хакерских группировок и ужесточения требований ЦБ, отмечают эксперты. Компания Positive Technologies впервые провела исследование с целью выяснить, какой ущерб хакеры могут нанести кредитной организации за один день кибератаки (исследование есть у «Известий»). В опросе приняло участие 170 организаций. По итогам этого года оказалось, что большинство (38%) оценили свои потери от действий кибермошенников в 0,5–2 млн рублей. 30% оценили потери в 50 млн рублей, четверть банков – в 2–10 млн, а 7% – в 10–50 млн.

В компании пояснили, что работа инфраструктуры банка может быть нарушена, если хакеры получат полный контроль над его доменами и сетевым оборудованием. Это возможно за счет отправки вирусного программного обеспечения и фишинговых рассылок.

Чтобы восстановить поврежденную инфраструктуру, каждый третий банк – 33% – готов потратить на восстановление работы после кибератаки 2–10 млн рублей. То есть расходы на нормализацию ситуации фактически в несколько раз превышают размер причиненного ущерба. 12% банков тратит 10–50 млн рублей. Остальные банкиры не стали раскрывать свои издержки на устранение вреда от хакеров.

Всего же на кибербезопасность большинство банков (70%) тратит 10–50 млн рублей в год, указали в Positive Technologies. Расходы 27,5% банков на это направление достигают 300 млн [7].

Таким образом, кибербезопасность в современном мире имеет огромное значение. Компьютерная сеть со дня её создания была подвержена атакам злоумышленников, и похоже, что угроза кибератак будет только расти по мере роста сети. Но с необходимым уровнем подготовки оборудования и специалистов вполне возможно контролировать ущерб, и восстанавливать потери от кибератак.

Список использованных источников

1. Сквозь пальцы. Пять главных ошибок банков в сфере кибербезопасности. https://www.forbes.ru/finansy-i-investicii/372009-skvoz-palcy-pyat-glavnyh-oshibok-bankov-v-sfere-kiberbezopasnosti
2. Стратегия кибербезопасности финансового сектора Республики Казахстан на 2018-2022 годы https://nationalbank.kz/cont/ Информсообщение% 20ПП%20Стратегия%20КБ%20ФС%20рус.pdf
3. В РК утверждена Стратегия кибербезопасности финансового сектора http://ru.zhambylnews.kz/lentanews/56506-v-rk-utverzhdena-strategiya-kiberbezopasnosti-finansovogo-sektora.html
4. Нацбанк РК утвердил стратегию кибербезопасности финансового сектора на 2018-2022 годы. https://wfin.kz/novosti/finansy/item/21038-natsbank-rk-utverdil-strategiyu-kiberbezopasnosti-finansovogo-sektora-na-2018-2022-gody.html
5. 8 советов для кибербезопасности банков. http://profinance.kz/news/novosti_dlya_koshelka/8_sovetov_dlya_kiberbezopasnosti
6. Кибербезопасность в финансовой сфере. https://www.it-world.ru/cionews/manage_secure/115701.html
7. Банки увеличили на 15% расходы на кибербезопасность. https://iz.ru/687793/anastasiia-alekseevskikh/banki-uvelichili-na-15-raskhody-na-kiberbezopasnost