Казахстанские банки: ландшафт киберрисков в цифровом формате. Обеспечение кибербезопасности.

Р.А. Хананова[1], А.Т. Жансейтов[2]
[1]студентка 2-го года обучения по специальности «Финансы»
[2]м.н., преподаватель
rozamailru@inbox.ru

[1,2]Карагандинский государственный университет имени Е.А. Букетова, г. Караганда

Аннотация: В данной статье рассмотрена новая угроза банков Республики Казахстан такая, как «киберриск». Проанализированы актуальность проблемы, статистика и встречающиеся случаи, а также предложены пути усиления кибербезопасности. Выявлена необходимость защиты интересов, как граждан, так и самих банковских учреждений.

Ключевые слова: Казахстан, банки, кибермошенничество, киберриски, кибербезопасность, киберпространство, киберщит

Сегодня в международном сообществе вопросы и проблемы кибербезопасности входят в список наиболее важных приоритетов национальной безопасности и обозначены как одна из глобальных мировых проблем. Вследствие информатизации и цифровизации всех сфер деятельности, в том числе и государственных структур, была сформирована новая отрасль противоборства. Инциденты, связанные с утечкой данных, как правило, вызывают цепную реакцию и наносят значительный финансовый ущерб. Подсчитано, что в среднем новая вредоносная программа создается каждые четыре секунды, и урон от кибератак измеряются миллиардами долларов в мировом масштабе [1]. В связи с широким использованием современных информационных систем во всех отраслях жизнедеятельности человека, включая политику, экономику, финансы и управление, возникло совершенное иное измерение, называемо «киберпространством». Оно содержит различные виды хакерских атак, к примеру, кибермошенничество, фишинг, спам, вредоносные программы, а также корпоративный шпионаж. В последнее время в Республике Казахстан существенно активизировались мошеннические группы, жертвами которых становятся не только физические лица, но и крупные организации, среди которых банки второго уровня.

В мире, который день за днем улучшается за счет научно - технического прогресса, финансовые технологии (финтех) становятся инновационным способом достижения финансовых целей и инклюзивного роста. В частности, данные технологии расширяют доступ к финансовым услугам для населения и предприятий, уменьшают затраты на денежные переводы, повышают прозрачность государственных операций, что сопутствует уменьшению коррупции и кибератак, так как по большей части финтех работает через Интернет [2]. По этой причине зачастую киберриски затрагивают банковскую сферу страны.

Банк является коммерческой организацией, деятельность которой реализуется при постоянных рисках. Кроме традиционных финансовых и нефинансовых рисков, появился новый вид в цифровой среде и называется «киберриском». Киберриск - это риск, связанный с использованием компьютерной техники и программного обеспечения, как в локальной, так и в глобальной сети Интернет [3]. В настоящее время банковские системы большинства стран предоставляют огромные возможности онлайн управления финансовыми ресурсами. В целом это называется дистанционное банковское обслуживание (ДБО). ДБО - это сложный комплекс услуг удаленного доступа к многообразным банковским операциям, которые предоставляются банками своим пользователям. К видам ДБО можно отнести системы «клиент-банк», «телефон-банк» [4]. Прежде, чем получить доступ к электронному банкингу, клиенты обычно должны открыть счет в банке лично, это делается для смягчения рисков, так как предоставляются соответствующие документы и информация. По сведениям Национального Банка Республики Казахстан, ежеминутно через национальные платежные системы проходит около 5,4 млрд. тенге, а в день - 3,3 трлн. [5]. Сколько из них попадают под определение «мошеннические» - таких данных нет. Нидерландская аудиторская компания KPMG в результате исследования обнаружила, что каждый второй банк страдает от растущих потерь из-за мошенников [6]. Уязвимости финансовой системы к киберпреступности в значительной степени связано с недостаточной защитой банковской информации.

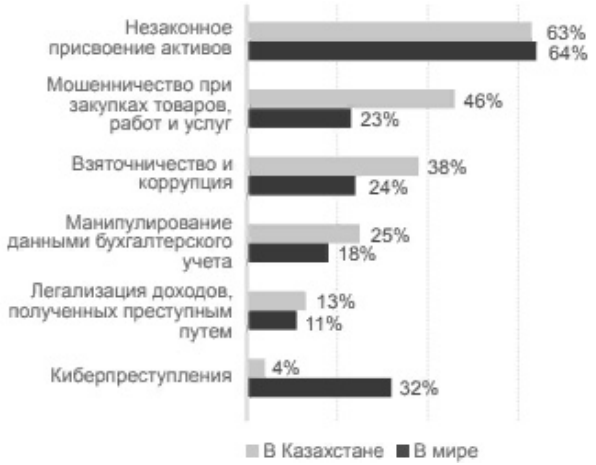

Рисунок 1. Основные виды экономических преступлений в Казахстане по сравнению с мировыми тенденциями [7]

Анализируя тенденции в области экономических преступлений, можно заметить, что среди них самый низкий удельный вес приходится на киберпреступления (рис.1), что составляет всего 4%, это существенно ниже, чем в целом по миру (32%). Следуя из этого, нужно отметить, что одним из пяти вызовов для банков стала социальная инженерия.

Социальная инженерия - это один из методов получения необходимого доступа к информации, который основан на особенностях психологии людей. Благодаря службе реагирования на компьютерные конфликты KZ-CERT удалось выявить ресурсы, моделирующие официальные интернет - сайты банков [8]. Так, в июле 2019 года в организацию KZ-CERT поступили данные о сомнительном интернет - портале, который копирует ресурс АО «Народный банк». Эксперты провели тщательный разбор и заметили наличие фишинговых форм на данной платформе. «Сайт полностью скопировал дизайн и функции официального ресурса. Для авторизации пользователям сайта предлагалось ввести номер телефона, идентификатор Homebank, логин my halyk и пароль», - говорится в службе. Специалисты зафиксировали этот случай как «мошеннический интернет - ресурс/фишинг в сети Интернет» [9].

Вслед за тем аналогичный случай был обнаружен в октябре такого же года, на этой раз пострадавшим стал АО ДБ «Альфа - банк». Проделанный тест определил, что веб - сайт имеет фишинговые формы в разделе перевода. Метод схемы афер был несложен. Для перевода валютных средств, пользователю нужно было установить данные карты с указанием номера карты, срока воздействия и CVC2/CVV2-кода, данные IBAN-счета получателя перевода и необходимую сумму валютных средств. Для удачного окончания перевода клиенту предлагалось установить семизначный цифровой код защищенности. Впоследствии ввода предоставленного кода пользователю было сообщено, что транзакция отклонена, и в это время хакерами осуществлялся сбор данных банковской карты и цифрового кода [10].

Уже в январе наступившего 2020 года кибермошенники вновь провели свои операции. «Интернет - платформа маскировалась под видом платежного ресурса, где предоставлялась возможность оплаты ипотеки, штрафов, кабельного телевидения и прочих услуг без комиссии. Вместе с тем, эксперты отмечают то, что интернет - ресурс был создан специально для Казахстана, так как возможность оплаты осуществлялась в тенге. Однако эксперты не исключают того, что злоумышленниками созданы аналогичные интернет - ресурсы для стран СНГ. Это связано с тем, что при попытке оплаты штрафов ПДД, на фишинговом интернет - ресурсе указывалось «Оплата штрафа ГИБДД». В рамках взаимодействия с международными Службами реагирования на компьютерные инциденты проведены мероприятия по оповещению страны, в которой осуществлялся хостинг данного ресурса и в течение нескольких часов данный инцидент информационной безопасности был устранен» [8],- сообщается на официальном сайте KZ-CERT.

По достоверным сведениям МВД РК за 2019 год обнаружено больше 216 случаев хищения денег с банковских карт. Официальные сведения могут отличаться от настоящих данных, так как при хищениях небольших сумм казахстанцы далеко не всякий раз обращаются с заявлением в правоохранительные органы. Во множестве случаев со счетов карт резидентов похищались суммы до 50 тысяч тенге. Однако есть и случаи, когда преступники уводили более крупные суммы - до 700 тысяч тенге [11].

Для предотвращения подобных инцидентов банкам Казахстана необходимо выдвинуть правильные задачи при создании инструмента оценки возникающих киберрисков. К этим задачам относятся:

1. Построение модели объективной оценки уровня киберрисков. Основная цель внедрения модели - не тратить ресурсы на снижение незначительных рисков, а направить усилия на обработку более высокого уровня рисков.

2. Обеспечение простого и удобного процесса оценки. Данный пункт актуален для специалистов по кибербезопасности, занимающихся процессами, разработки которых значительно ускорены.

3. Учет мнения нескольких экспертов из разных областей. Для получения объективных результатов должна быть предусмотрена возможность привлечения экспертов к оценке киберрисков для разных профилей.

4. Создание универсальной модели, подходящей для всех банков.

5. Предоставление возможности отслеживать динамику уровня киберриска при изменении внутренних и внешних факторов.

Не обращая внимания на все моменты, используемые банковскими организациями по смягчению кибератак, сам банк не должен стоять на охране беспечности его клиентов. Банковские карты предусмотрены для упрощения всевозможных процедур оплаты, переводов и обналичивания. При этом банки никоим образом не держат под контролем все операции, происходящие с картой и информацию, передаваемую пользователями третьим лицам. Впрочем, репутационные опасности для банка не бессодержательны. Ограбленные пользователи, как правило, начинают предъявлять обвинение банку в том, что не заморозил своевременно карту, не остановил операцию, которая была проведена два - три дня назад, не запустил функцию chargeback (возвратный платеж), не провел абсолютное и квалифицированное расследование. Вследствие этого банки обязаны расходовать силы на то, дабы гарантировать защищенность средств собственных клиентов [12].

Первый Президент РК Н. Назарбаев в своем Послании народу Казахстана от 31 января 2017 года отметил, что все большую значимость приобретает борьба с киберпреступностью. В соответствии с поручением Министерством оборонной и аэрокосмической промышленности Республики Казахстан с учетом Стратегии «Казахстан - 2050» по вхождению Казахстана в число 30-ти самых развитых государств мира выработан проект постановления Правительства «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» [13]. Концепция выстроена на основе интерпретации нынешней ситуации в области информатизации государственных органов, автоматизации государственных услуг, перспектив развития «цифровой» экономики и технологической модернизации производственных процессов в промышленности. Требования по безопасности банковских информационных систем обеспечиваются нормативно - правовыми актами Национального Банка Республики Казахстан с учетом отраслевых и международных требований по обеспечению безопасности информационных систем. Новая редакция Уголовного кодекса Республики Казахстан предусматривает отдельную главу, посвященную преступлениям, совершаемым в сфере информатизации и связи. Таким образом, были введены дополнения в Уголовный кодекс РК и Кодекс РК «Об административных нарушениях» [14].

В масштабах разработки Концепции кибербезопасности постановлением НБ РК от 29 октября 2018 года была согласована Стратегия кибербезопасности финансового сектора Республики Казахстан на 2018 - 2022 годы. Она содержит поставленные цели, задачи и мероприятия, достижение и реализация которых позволит гарантировать внедрение эффективно функционирующей системы кибербезопасности финансового кластера РК. Основополагающей целью Стратегии является формирование условий для безопасного оказания финансовых услуг, что необходимо для поддержания стабильного регулирования и развития финансового сектора страны. К 2023 году Нацбанк планирует создать действенную систему обеспечения кибербезопасности финансового сектора. Для достижения цели, с мониторингом текущих недостатков в области кибербезопасности финансового сектора, определены пять основных направлений [15]:

1. совершенствование регулирования систем обеспечения кибербезопасности субъектов финансового сектора

2. обеспечение кибербезопасности физических и юридических лиц при использовании финансовых услуг

3. обеспечение устойчивого и безопасного функционирования критичной информационной инфраструктуры финансового сектора, включая Национальный Банк

4. сотрудничество в сфере борьбы с киберпреступностью в национальном и глобальном масштабе

5. создание и развитие национальных технологий киберзащиты финансового сектора.

Вдобавок к этому, для усиления кибербезопасности в декабре 2018 года был предложен новый проект в области страхования «киберстрахование». Рынок киберстрахования - это небольшая, но растущая часть страхового сектора, которая помогает корпорациям защищаться от цифровых угроз. По оценкам страховой компании Allianz, киберстрахование в настоящее время составляет около 2 млрд. долларов США по всему миру, причем на рынок США приходится около 90% этой суммы. Тем не менее, по мере того, как число случаев кибератак продолжает расти и организации все чаще узнают о потере данных своих клиентов, эффективный охват кибератак становится все более важным приоритетом всех стран мира. Ожидается, что к 2025 году премии за киберстрахование во всем мире достигнут 20 млрд. долларов.

Подводя итоги, можно судить о существовании проблем в банковском секторе РК, в особенности появление киберрисков, что требует тщательного контроля и надзора со стороны НБ РК. Ключевые проблемы Казахстана в кибербезопасности вытекают из экспоненциального роста количества мобильных и интернет - пользователей, недостаточной осведомленности в области информационной безопасности граждан, а также низкой обеспеченности в системах защиты данных банковских учреждений. В настоящее время ведутся работы по улучшению безопасности и защищенности клиентов и банков, которые способствуют повышению конкурентоспособности и переходу на новый уровень.

Список использованной литературы:

1. Статья «Обеспечение кибербезопасности в Казахстане: проблемы и решения».- 2019 http://elibrary.kaznu.kz/sites/default/files/Besplatnie_resursii/weekly_e-bulletin_22.04.2019-28.04.2019_no_208.pdf
2. Рабочий документ МВФ «Финтех, инклюзивный рост и киберриски».- 2018 file:///E:/USER/Downloads/wp18201.pdf
3. Межбанковский форум по информационной безопасности «Управление рисками ИТ и ИБ в условиях современных вызовов».- 2015 https://profitday.kz/Content/files/2015/interbank/2-1.pdf
4. Веб-сайт «Бизнес Заработок» https://bizneszarabotok.ru/banki_i_kredity/dbo/#1
5. Информационное сообщение НБ РК.- 2019 https://www.nationalbank.kz/cont/%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BF%D0%BB%D0%B0%D1%82%D0%B5%D0%B6%D0%BD%D1%8B%D0%B5%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B.pdf
6. Нидерландская аудиторская компания KPMG «Глобальное исследование банковского мошенничества».- 2019 https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf
7. PWC «Казахстанский обзор экономических преступлений за 2016 год».- 2017 https://www.pwc.kz/en/publications/new-2017/crime-survey-2016-rus.pdf
8. Сайт службы реагирования на компьютерные инциденты KZ-CERT http://www.kz-cert.kz/ru
9. Новости «Sputnik Казахстан» https://ru.sputniknews.kz/society/20190711/10908362/narodnyi-bank-kazakhstan-poyavilsya-klon-moshennik-v-seti.html
10. Новостной портал Агентства «Хабар» https://24.kz/ru/news/economyc/item/351499-kazakhstanskij-bank-stal-zhertvoj-internet-moshennikov
11. Новости «Tengri News» https://tengrinews.kz/kazakhstan_news/kak-u-kazahstantsev-voruyut-dengi-s-kart-rasskazali-v-mvd-381538/
12. Новостной портал «InBusiness» https://inbusiness.kz/ru/news/lzhebankiry-i-prostachki-pochemu-v-kazakhstane-rastet-oborot-rynka-moshennicheskikh-operatsiy-20713
13. Официальный интернет-ресурс Министерства юстиции РК http://www.adilet.gov.kz/ru/leaflet/kibershchit-kazahstana
14. Постановление Правительства РК «Об утверждении Концепции кибербезопасности» http://adilet.zan.kz/rus/docs/P1700000407
15. Постановление Правления НБ РК «Об утверждении Стратегии кибербезопасности финансового сектора Республики Казахстан на 2018-2022 годы» https://online.zakon.kz/Document/?doc_id=34451945#pos=1;-123