Декабрь 2021

БЕЗОПАСНОСТЬ

В поисках цифрового равновесия

КУРСИВ | GUIDE

Приложение к республиканскому деловому еженедельнику «Курсив»

Александр Левин,
ответственный редактор
Kursiv.Guide

Что гражданам и бизнесу нужно знать о финансовой безопасности?

Каждое четвертое уголовное правонарушение в Казахстане – мошенничество. За 9 месяцев 2021 года ущерб от таких преступлений составил 47,4 млрд тенге. Это «письма счастья», объявления о продаже неких чудодейственных медицинских гаджетов, обещания о списании долгов, сбор на «благотворительные» цели или ставшие едва ли не анекдотичными звонки от «службы безопасности банка».

При этом пресс-службы и настоящие службы безопасности банков говорят: нет никаких «зеркальных счетов» или «страховых ячеек». Настоящие сотрудники банка никогда не просят клиента куда-то перевести деньги для того, чтобы их уберечь. Да, в банках действительно есть система, которая отслеживает подозрительные операции. Например, человек сменил пароль и тут же снимает все средства с депозита – у банка могут возникнуть вопросы. СБ звонит клиенту и уточняет, сам он это делает или нет. Мошенники знают об этом и предупреждают: «Если вас спросят, скажите, что сами». Не должно ли такое предупреждение выглядеть подозрительно? Даже без специальных знаний.

Мошенники не первый (и не десятый) год пользуются низкой финансовой грамотностью населения, жаждой быстрой наживы или тяжелым экономическим положением в регионе или стране. Казалось бы, что может быть проще, чем не называть незнакомым людям конфиденциальные данные пластиковых карт (например, CVV-код, PIN-код, пароль от карты и от банковских онлайн-кабинетов, коды подтверждения из SMS-сообщений, кодовые слова), но, как показывает практика, злоумышленники могут быть чертовски убедительны. Ну, или им просто удается попасть в нерв, предложить решение денежных проблем в семье, проблем с трудоустройством. Так, с поправкой на новую, «карантинную» реальность появились сайты фиктивных кадровых агентств, предлагающих трудоустройство на удаленном режиме за плату или сценарии с возвратом налога на добавленную стоимость, когда жертвы сами переводят деньги преступникам, выполняя по указанию последних те или иные операции на счетах.

И, конечно, финансовые пирамиды. Только за последние пять лет в Казахстане было зарегистрировано более шестисот уголовных дел, связанных с созданием финансовых пирамид. Около трети из них пришлось на прошлый год, а ущерб от их деятельности в Генпрокуратуре оценили в 6 млрд тенге. В конце 2020 года Институт общественной политики провел социологическое исследование на эту тему. Согласно его результатам, только 39,9% из 6,8 тысяч опрошенных казахстанцев изучают сайты финансовых организаций для выбора наиболее оптимального финансового продукта или услуги.

В том, что в кризисный 2020 год количество мошенников увеличилось, нет ничего удивительного. И дело не только в наивности людей или действительно низкой финансовой грамотности. Причем речь идет не только о физических лицах, но и о бизнесе. Стресс, выгорание, новые правила жизни, перенапряженный информационный фон, срыв планов – у многих людей не остается сил к критическому восприятию предложений. Что делать? Как обезопасить себя, свой бизнес, родных? Именно об этом мы поговорим в рамках нового бизнес-гайда «Безопасность». Разбираемся, какие виды мошенничества на финансовых рынках существуют и как не попасться на уловки преступников.

Генеральный директор/главный редактор: Сергей ДОМНИН s.domnin@kursiv.kz, редакционный директор: Александр ВОРОТИЛОВ a.vorotilov@kursiv.kz, выпускающий редактор «Курсив Guide»: Александр ЛЕВИН a.levin@kursiv.kz, бильд-редактор, фотограф: Илья КИМ i.kim@kursiv.kz, верстка: Мадина НИЯЗБАЕВА, дизайнер: Данара АХМУРЗИНА, коммерческий директор: Ирина КУРБАНОВА, тел. +7 (777) 257 49 88, i.kurbanova@kursiv.kz, руководитель по рекламе и PR: Сабир АГАБЕК-ЗАДЕ, тел. +7 (707) 950 88 88, s.agabek-zade@kursiv.kz, нач. отдела распространения: Ренат ГИМАДДИНОВ, тел. +7 (707) 766 91 99, r.gimaddinov@kursiv.kz, А15P1M9, РК, г. Алматы, ул. Розыбакиева, 127, тел./факс +7 (727) 339 84 41, e-mail: kursiv@kursiv.kz, представительство в Нур-Султане: пр. Кунаева, д. 12/1, БЦ «На Водно-зеленом бульваре», ВП-80, 2-й этаж, оф. 203, тел. +7 (7172) 28 00 42, e-mail: astana@kursiv.kz. Подписные индексы: для юридических лиц – 15138, для физических лиц – 65138. Газета зарегистрирована в Министерстве информации и коммуникаций Республики Казахстан. Свидетельство о постановке на учет No 17442-Г, выдано 9 января 2019 г. Приложение отпечатано в типографии «Print House Gerona», г. Алматы, ул. Сатпаева, 30а/3, офис 124. Тираж 8 000 экз.
Информационная продукция данного печатного издания предназначена для лиц, достигших 18 лет и старше. Дизайн обложки: Гамаль СЕЙТКУЖАНОВ.

Победа над мошенниками – в финансовой грамотности клиентов

Крупнейшие игроки казахстанского банковского сектора говорят о мошенничестве и дают советы, которые помогут сберечь деньги граждан. Зачастую, говорят представители банков, клиенты сами передают мошенникам персональные данные – злоумышленникам проще «взломать» человека с помощью социальной инженерии, чем многоуровневые системы защиты финансовых институтов.

ForteBank

В последние годы мошенники часто атакуют клиентов казахстанских и российских банков. К сожалению, даже учитывая все профилактические уведомления от банков (предупреждения в SMS-сообщениях, информация на сайте и в социальных сетях) о такой активности, многие граждане все еще попадают под влияние социальной инженерии, предоставляя доступ к своим счетам, оформляя кредиты онлайн и оставаясь обманутыми. Даже хорошо осведомленные люди периодически оказываются в такой ситуации – среди них есть и пожилые, и предприниматели, и даже сотрудники банков.

Большая сложность в том, что мошенники профессионально подготовлены и владеют алгоритмами для получения контроля над людьми. А клиенты банков, напротив, никогда не тренировались противостоять мошенническим действиям, и мало кто имеет положительный опыт ухода от подобных атак. Тем не менее, со временем таких людей становится больше.

Клиенты нашего банка не являются исключением, и некоторые из них попадаются на мошеннические звонки, но, к счастью, их не так много.

Мошенники постоянно занимаются сбором данных из различных источников. В большинстве случаев из интернета: с сайтов объявлений, сервисов доставки, госуслуг, интернет-магазинов – то есть везде, где человек может ввести данные своей карты либо раскрыть информацию о своем банке.

Затем они занимаются обзвоном и следуют подготовленным сценариям диалога – например, представляются службами безопасности банков, рассказывают, что нужно подтвердить некоторые данные, чтобы избежать кражи денег с карт. В ходе диалога направляют клиента по работающему алгоритму, завладевают персональными данными и кодами подтверждения из сообщений с одноразовыми паролями. Таким образом получают доступ к банкингу клиента.

Важно помнить, что мошенники точно понимают и следят за обновлениями антимошеннических инструментов, составляя схемы перевода и вывода денег так, чтобы не быть замеченными системой и избегать блокировок подозрительной активности клиентов.

В сфере борьбы с мошенничеством есть несколько важных вопросов. Первое – это финансовая грамотность населения. Учитывая развитие digital-каналов для обслуживания, требуется постоянное проведение доступной и, самое главное, понятной информационной работы с физическими лицами, старшим поколением – на уровне СМИ, рекламных буклетов на улицах, то есть в общедоступных местах, чтобы все знали о видах мошенничества и были готовы им противостоять. Многие, к сожалению, о мошенничестве, социальной инженерии узнают, только став их жертвами.

Также важно проводить работу на межгосударственном уровне при взаимодействии банков, правоохранительных органов на более тесном уровне, действуя превентивно.

ДБ АО «Сбербанк»

С каждым годом происходит рост интернет– и телефонного мошенничества. Мошенники на постоянной основе совершенствуют свои методы атак, и неподготовленному клиенту становится сложнее определить звонок от мошенника. Для защиты клиентов банк использует лучшие решения с рынка для противодействия мошенничеству, а работники постоянно проходят обучение по противодействию мошенничеству.

Статистика показывает, что количество атак увеличилось на 37% в сравнении с 2020 годом. Но, учитывая развитие финансовых институтов в борьбе с мошенничеством, число реализованных фактов мошенничества в 2021-м снизилось на четверть.

Сейчас социальная инженерия стала более подготовленной. Например, один из распространенных видов мошенничества таков: обычно мошенники звонят потенциальным жертвам под видом банковских сотрудников, представителей иных финансовых организаций или правоохранительных органов.

Они сообщают о том, что по карте якобы совершена подозрительная операция или на карту оформлен кредит. Для «предотвращения операции и сохранения средств» мошенники выманивают данные карты, убеждают жертву перевести деньги на «безопасный счет» или установить специальное приложение для «усиленной защиты телефона», которое на самом деле оказывается программой удаленного доступа к мобильному телефону.

Есть и другой способ: злоумышленники запугивают жертву недобросовестным работником банка, который пытается оформить на клиента кредит. Далее обманным путем оформляют «предодобренный кредит» (убеждают жертву это сделать или получают доступ в мобильный банк и сами проводят операцию).

Одна из проблем в этой сфере – операторы связи не блокируют звонки с подменой номеров. Это когда клиенту звонят из другой страны, а у клиента отображается звонок от казахстанского номера телефона. Зачастую при атаке мошенники подделывают номера местного телефонного оператора. Полагаем, что при реализации блокировки звонков с подменных номеров уровень мошенничества может снизиться до 70%.

Важным остается и повышение финансовой грамотности. Наш банк регулярно размещает обучающие посты, уведомляет своих клиентов о возможных способах мошеннических операций по всем возможным каналам – от социальных сетей и памяток на сайте банка до обучающих роликов в отделениях и на YouTube.

Jusan Bank

Масштабный переход в условиях карантина в онлайн многих денежных операций, невысокий уровень финансовой грамотности у новых пользователей дистанционных сервисов создают благоприятные условия для мошенников.

Наиболее распространенным методом у них является телефонное мошенничество, которое, как правило, связано с незаконным сбором персональных данных и социальной инженерией. В подобных случаях мошенник звонит потенциальной жертве и представляется сотрудником службы безопасности банка либо работником вымышленных организаций, например, ассоциации банков или каких-либо других, которые могут вызвать доверие у потенциальной жертвы, чтобы получить те или иные персональные данные и в последующем воспользоваться ими.

Чаще всего лжеработник банка звонит с предупреждением о якобы случившейся блокировке карты, ошибочном открытии кредита, взломе личного кабинета в интернет-банкинге, подозрительной транзакции. Например, наиболее частый сценарий сейчас – звонок или серия звонков с целью проверки по якобы оформляемому на потенциальную жертву кредиту в другом городе.

Во время разговора потенциальную жертву могут уговаривать, пугать, угрожать, чтобы лишить эмоционального равновесия, не дать времени на раздумья и подтолкнуть к спонтанным действиям. Злоумышленники стараются убедить жертву в том, что могут ей «помочь» не потерять свои деньги или предотвратить открытие кредита, только если им очень срочно сообщить, например, ИИН, код из SMS, данные карты или иную персональную информацию. Также могут предложить до выяснения обстоятельств перевести имеющиеся на карте деньги на другой счет.

Еще один способ, которым сегодня все чаще пользуются мошенники – получение удаленного доступа к устройствам банковских клиентов. Например, с помощью таких распространенных программ, как AnyDesk или TeamViewer, мошенники могут получить удаленный доступ к смартфонам, планшетам и компьютерам, чтобы через интернет-банкинг открыть кредит или перевести деньги клиента на свои счета. Чтобы не попасться на эту уловку, не следует устанавливать сторонние приложения на смартфон или компьютер по инициативе незнакомого человека.

Важно помнить, что сотрудники банка никогда не звонят с предложением установить стороннее программное обеспечение на ваше устройство, не предлагают оформить кредит для перевода денег на другие счета или перевести деньги на какой-либо «безопасный счет» при возникновении якобы подозрительных транзакций на ваших счетах.

Мошенники также активно осваивают цифровые методы. Например, клоны банковских сайтов и аккаунтов в социальных сетях, электронные рассылки с розыгрышем призов – на любом этапе и под любым предлогом потенциальной жертве может быть предложено ввести данные банковской карты. Это называется фишингом.

Чтобы на него не попасться, следует внимательно проверять последовательность букв в адресной строке сайта или наименовании аккаунта и его внешнее оформление – малейшая неточность в цвете или неаккуратность в структуре должны насторожить. Также не следует вводить данные карты на посторонних ресурсах, а информацию о розыгрышах и акциях всегда можно уточнить в контакт-центре.

В течение 10 месяцев 2021 года было зафиксировано около 150 фактов мошенничества, и все они связаны с передачей самими же клиентами персональной информации мошенникам.

Безопасность клиентов – приоритет в работе Jusan Bank. Для поддержания безопасности банк использует современные цифровые решения, например, при регистрации в нашем мобильном приложении пользователи проходят аутентификацию по биометрии.

В то же время это не освобождает пользователей банковских продуктов от необходимости самим соблюдать простые правила, которые с большой долей вероятности могут помочь защитить себя от мошенников. На практике мошенникам легче «взломать» клиента, чем многоуровневую банковскую систему безопасности.

Риски мошеннических операций возможны только в тех случаях, когда пользователь сам делится с незнакомцами конфиденциальной информацией, пусть даже делает это неосознанно. Именно поэтому в подавляющем большинстве схемы аферистов основаны на методах социальной инженерии, или, другими словами, на психологическом манипулировании.

ДО АО Банк ВТБ (Казахстан)

Проблема мошенничества со счетами клиентов банков актуальна, поэтому Банк ВТБ уделяет повышенное внимание вопросам безопасности данных и средств клиентов, вкладывая материальные и кадровые ресурсы в развитие этого направления. Параллельно с этим банк уделяет внимание вопросам финансовой грамотности клиентов, распространяя через публичные каналы коммуникаций информацию о методах защиты от мошенничества.

Современное мошенничество чаще всего направлено именно на получение конфиденциальной информации у пострадавшей стороны – в результате таких действий человек сам предоставляет злоумышленникам личные данные. В таких случаях ответственность за сохранность сбережений полностью лежит на владельце счета.

Сегодня наиболее распространенным видом мошенничества на рынке является социальная инженерия, когда человек, сам того не осознавая, передает мошенникам конфиденциальную информацию. Например, если взять фишинг, то он бывает голосовым и SMS.

Первый подразумевает телефонное мошенничество, когда под видом сотрудников банка злоумышленники пытаются заставить клиента озвучить свои данные. Более того, имеют место быть и «Caller ID spoofing attacks», когда недобросовестные личности звонят потребителям финансовых услуг с подмененного идентификатора входящего номера. В результате клиент думает, что звонок поступает из банка, и доверительно относится к собеседнику.

Фишинг через SMS можно определить в виде сообщения, в котором человека просят перейти по ссылке на фишинговый сайт, установить вредоносное программное обеспечение или под различными предлогами самостоятельно отправить персональные данные ответным сообщением.

Если клиент банка сталкивается с мошенническими действиями, в первую очередь необходимо незамедлительно сообщить об инциденте в банк и заблокировать карту, предотвратив дальнейшие потери.

Далее следует обратиться в банк с заявлением о пропаже денег со счета. Банк, в свою очередь, должен провести служебное расследование. Если банк убедится, что вы не нарушали правила использования карты и не сообщали третьим лицам свои личные данные, при этом вовремя опротестовали операцию, вам вернут деньги.

Фото: Depositphotos

Как банки защищают данные и борются с внешними угрозами

Мобильный банкинг – повседневная реальность. Но чем удобнее сервис, тем больше угроз безопасности.

Банковскими услугами через смартфон люди пользуются во всем мире. К примеру, согласно опросу Американской банковской ассоциации 2019 года, 73% американцев получают доступ к своим банковским счетам онлайн или через мобильные устройства. В Казахстане в одном только банкинге Kaspi в 2020 году количество ежемесячных активных пользователей составило 9,1 млн (+59% в годовом выражении), а по итогам шести месяцев этого года достигло 10,2 млн – более 50% всего населения страны.

Алимхан Адилов

Должен создаваться механизм мониторинга и оперативного реагирования на все отклонения от стандартной работы системы.

Тренд не появился сам по себе. Онлайн и мобильный банкинг делают управление финансами простым и удобным. Прошли те времена, когда приходилось посещать отделения для решения рутинных банковских задач. Но есть и обратная сторона – безопасность. В режиме онлайн на нее покушаются чаще, чем при физических походах в банк. Банки, в свою очередь, полагаются на различные меры безопасности, такие как, например, 128-битное или 256-битное шифрование данных. Разбираемся, что это значит, как в целом устроена защита информации в банках и какие угрозы существуют.

Нормы и нормативы

Для начала стоит разделить два вида угроз для потребителя банковских услуг. Первый – когда попытки взлома/обмана направлены на сам банк, его сотрудников или онлайн-платформы. Второй – атака направлена на потребителей, то есть физических лиц. Это самый уязвимый, и, соответственно, распространенный вид мошенничества, поскольку строится он исключительно на инструментах социальной инженерии.

Опытному мошеннику достаточно пары звонков, чтобы как минимум один из ста человек по собственной воле отдал персональные данные преступнику. В первом же случае злоумышленникам приходится сталкиваться со сложно устроенной системой банковской защиты.

По данным российского разработчика средств информационной безопасности SearchInform, в коммерческих банках построение системы информационной безопасности базируется на следующих принципах: во-первых, это безопасность узлов системы и информационных ресурсов, она должна обеспечиваться на всех этапах жизненного цикла данных, при любых внешних и внутренних обстоятельствах. Во-вторых, информация должна ранжироваться по степени важности, конфиденциальности, отнесению к защищаемым ресурсам согласно требованиям законодательства и регулятора. В-третьих, должен создаваться механизм мониторинга и оперативного реагирования на все отклонения от стандартной работы системы, выявляющий внешние подключения, подмену кода, работу вредоносных программ.

По словам Романа Кузьменко, начальника службы информационной и внутренней безопасности Fortebank, с 2015 года число угроз в сфере информационной безопасности выросло значительно. «В открытом доступе появилось много кибероружия. Угрозы стали эволюционировать быстрее, вместе с ними и мы», – отмечает он.

Эксперт объясняет: чтобы противостоять угрозам – в каждом банке существует такое понятие, как СУИБ. «Это система управления информационной безопасностью. Участниками этой системы почти все – от советников директоров банка до департаментов GR или риск-менеджмента. Это огромная командная работа. Такие подразделения – это локомотив, который двигает процессы обеспечения информационной безопасности», – говорит он.

При этом, продолжает Кузьменко, сфера информационной безопасности в банках ввиду своей важности крайне зарегулирована, и принцип ее строительства основан не только на национальных, но и на международных регламентах.

«Существует огромное количество документов. Часть из них – международные, которые мы не можем игнорировать. Это группа стандартов ISO27000, стандарты ISO9000, генеральный регламент обработки персональных данных граждан ЕС GDPR. И это международный стандарт индустрии платежных карт PCI DSS – под него попадают почти все в этой индустрии: эквайринги, а также другие специалисты, которые обрабатывают платежные и персональные данные», – подчеркивает Кузьменко.

Кроме того, есть большая линейка требований к обеспечению информационной безопасности согласно национальным стандартам.

«Основные для банков второго уровня – сорок восьмые требования об обеспечении безопасности в банках (Постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года №48). Это наша настольная книга, но мы ожидаем новую редакцию», – говорит эксперт.

По его словам, есть также правила организации системы управления рисками внутреннего контроля, там тоже прописан функционал для обеспечения информационной безопасности. С 2021 года также действуют новые нормативы, которые, помимо прочего, касаются компетенции сотрудников служб безопасности, а также методики построения систем безопасности и возможных рисков.

«В общем, это широкий спектр документов, и регулятор очень сильно озабочен состоянием информационной безопасности. Наша деятельность регулируется больше, чем какая-либо другая», – говорит Кузьменко.

Социальный щит

Но кроме правил регулирования и методик, по которым действуют службы безопасности, есть также и другой уровень защиты – это механизмы, которые должны обеспечивать безопасность банковских сервисов с клиентами. Они бывают разные, но работают синхронно – данные клиентов должны быть в безопасности на каждом этапе, в том числе на самом уязвимом – социальном.

К примеру, согласно данным Tadviser, 75% банков уязвимы для атак методами социальной инженерии. Поэтому в банках налажена работа систем-скоринга. Эта система применяется для оценки платежеспособности заемщика. Клиент банка при оформлении кредита, например, проходит обязательное анкетирование. Его профессиональные, демографические и социальные характеристики имеют определенный балл. Сухие цифры и данные подтвердят личность без всяких нареканий и упростят работу сотрудников банка. Потому что первые – машины, а вторые – люди, которым свойственно ошибаться.

75% банков уязвимы для атак методами социальной инженерии

Также стараются обезопасить и мобильные банкинги. К примеру, казахстанские банки и их приложения работают по механизму двухфакторной аутентификации (2FA) – это частный случай многофакторной верификации доступа к конфиденциальным данным. Личность, зашедшая в банкинг, должна подтвердить право доступа не только паролем, но и SMS-кодом. Так же работают и операционные системы самих мобильных устройств. К примеру, пользователи IOS могут заходить в банкинг только при подтверждении FaceID (система распознавания лиц).

Евгений Белов, директор департамента защиты информационных ресурсов Halyk, отмечает, что чем больше и удобнее сервисов, тем больше будет попыток их использовать вне правовой схемы.

«Сервис нужно сделать настолько надежным, чтобы даже клиент не понимал, когда его защищают. Это реально. Те системы, которые работают в казахстанских банках, позволяют достаточно комплексно защищать клиента. К примеру, раньше была схема удаленного доступа, когда злоумышленники ставили программы удаленного доступа к устройству, а затем с устройства клиента проводили манипуляции без его участия. На сегодняшний день хорошо работает схема отслеживания, можно понять, что установлен сервис удаленного управления, и далее заблокировать активность», – говорит Белов.

По его словам, возможности обеспечения информационной безопасности и дальше будут развиваться. Важно защищать клиента, вне зависимости от того, насколько он подвержен схемам мошенничества, подчеркивает он. «Мы к этому стремимся – делать клиентский сервис, и при этом крайне защищенный. К примеру, тренд на суперприложения – это же выбор в пользу клиента и его потребностей. Но когда ты называешься суперприложением, то и безопасность должна быть супер», – говорит эксперт.

Фото: Depositphotos

Что для борьбы с мошенничеством на финансовых рынках делает АРРФР РК

Заместитель председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка Нурлан Абдрахманов рассказал о шести стратегических мерах АРРФР РК по борьбе с финансовым мошенничеством и финансовыми пирамидами.

Фото: Depositphotos

Особенно актуальной проблема финансового мошенничества стала в конце 2019 – начале 2020 года, когда наблюдалась значительная активность финансовых пирамид, которые либо регистрировались как ломбарды, кредитные товарищества или кооперативы, либо незаконно использовали в описании деятельности ссылки на известные финансовые организации. Так, в начале февраля 2020 года жители городов Нур-Султан, Актобе, Атырау и других регионов начали жаловаться на то, что не могут вернуть вложенные средства в ломбарды «Гарант 24», «Estate Ломбард», «Home Avto Invest» и другие. При этом многие люди для того, чтобы вложиться в финансовую пирамиду, продавали недвижимость. Правоохранительными органами заведено несколько уголовных дел, организаторы финансовых пирамид арестованы, по ним ведутся следственные мероприятия.

В этой связи, главой государства в феврале 2020 года было дано поручение выработать эффективные меры по противодействию финансовому мошенничеству и финансовым пирамидам.

Что сделало АРРФР РК

1 Ввиду того, что некоторые мошеннические организации маскировались под ломбарды, в марте 2020 года агентством совместно с органами прокуратуры, МВД РК и министерством финансов РК были начаты проверки учреждений такого типа. Под проверку попали более 597 ломбардов, около 50 субъектов онлайн-кредитования и около 200 микрофинансовых организаций.

В периметр вопросов проверки входили:

- противодействие отмыванию доходов и финансированию терроризма;
- противодействие организации финансовых пирамид;
- требования к коэффициенту долговой нагрузки, размеру годовой эффективной ставки вознаграждения и значению предельного вознаграждения по микрозаймам, правильности начисления вознаграждения, штрафов и пени, порядку очередности погашения задолженности по микрокредиту.

По итогам проверок Генеральной прокуратурой РК в отношении недобросовестных организаций возбуждено 910 дел об административных правонарушениях с наложением штрафа на сумму свыше 70 млн тенге. Агентством в отношении 204 кредитных организаций составлено 1000 административных протоколов и выставлено штрафов в размере 152 млн тенге.

2 Дополнительно в отношении ломбардов, МФО, кредитных товариществ и компаний онлайн-кредитования проведена учетная регистрация. Кроме того, агентством был ужесточен ряд требований к ним.

Так, к примеру, были установлены квалификационные требования к акционерам и менеджменту компаний. В частности, требования к наличию безупречной деловой репутации, наличию опыта работы, отсутствию непогашенной судимости. В целях обеспечения устойчивости субъектов повышены пруденциальные стандарты по минимальному размеру капитала. Минимальный размер собственного капитала для действующей микрофинансовой организации установлен на уровне 50 млн тенге с увеличением к 2023 году до 100 млн тенге, для кредитного товарищества – с 30 до 50 млн тенге, для ломбарда – с 30 до 70 млн тенге.

Кроме того были установлены требования по обеспечению безопасности и технической укрепленности помещений, процедуры хранения имущества, разработаны меры по противодействию обороту незаконно добытых вещей. Ранее ломбарды зачастую осуществляли деятельность в неприспособленных помещениях, которые не обеспечивали сохранность заложенного имущества.

3 Для усиления контроля над деятельностью всех микрофинансовых организаций в рамках исполнения поручений главы государства с 1 января 2021 года было введено обязательное лицензирование микрофинансовой деятельности. Теперь все субъекты микрофинансового сектора, включая ломбарды, подлежат лицензированию и усиленному надзору.

Лицензии получили 1064 организации, осуществляющие микрофинансовую деятельность, в том числе 235 микрофинансовых организаций, 218 кредитных товариществ и 611 ломбардов. Остальные более 3,5 тыс. субъектов кредитования, из которых более 1,5 тысяч – ломбарды, были ликвидированы добровольно или в судебном порядке.

4 В период пандемии МФО активизировали выдачу микрокредитов дистанционно, без физического присутствия клиента. Вместе с тем, на рынке микрофинансирования получила распространение практика выдачи фиктивных микрокредитов с незаконным использованием персональных данных граждан. Для недопущения мошенничества, связанного с выдачей онлайн-микрокредитов и защиты потребителей микрофинансовых услуг, в апреле 2021 года регуляторно ужесточен порядок идентификации заемщиков.

В целях предотвращения интернет-мошенничества с микрокредитами, агентством совместно с правоохранительными органами в октябре текущего года подписан меморандум «О взаимопонимании и сотрудничестве», которым установлен алгоритм оперативного списания задолженности заемщиков по фиктивным займам, выданным электронным способом.

В соответствии с данным алгоритмом, агентство, с учетом полученной от министерства внутренних дел информации по фактам оформления микрокредитов мошенническим способом, осуществляет мониторинг за принятием МФО мер по приостановлению начисления вознаграждения по фиктивному микрокредиту, прекращению претензионно-исковой работы в отношении потерпевшего-заемщика МФО.

На основании информации органов внутренних дел и иных сведений, подтверждающих неполучение потерпевшим микрокредита, агентство осуществляет контроль за внесением корректировки в кредитную историю, принятием МФО решения о списании задолженности заемщиков по оформленным на них микрокредитам мошенническим способом.


Фото: Depositphotos

Для недопущения мошенничества, связанного с выдачей онлайн микрокредитов и защиты потребителей микрофинансовых услуг постановлением правления агентства от 30 апреля 2021 г. №63 введен новый порядок идентификации заемщиков при выдаче онлайн-микрокредитов. Теперь для удаленного получения микрокредита требуется обязательное проведение идентификации заемщика одним из трех способов:

1. посредством электронно-цифровой подписи;
2. соответствия биометрическим параметрам заемщика с использованием сервиса ЦОИД (Центр обмена идентификационными данными) КЦМР Национального Банка;
3. посредством двухфакторной проверки персональных данных и изображения заемщика в режиме реального времени.

В связи с введением новых требований количество жалоб на оформление фиктивных микрокредитов резко уменьшилось. Так, за 2021 год выявлено только 475 фиктивных микрокредитов, из которых 469 случаев произошли до ужесточения регуляторных требований по идентификации заемщиков при выдаче онлайн-микрокредитов.

Возбуждено 910 дел об административных правонарушениях

Дополнительно для снижения рисков, связанных с оформлением микрокредита на другое лицо, агентством в октябре текущего года также разработаны требования по аутентификации клиента при получении микрокредита электронным способом, в том числе путем использования механизма осуществления идентификации клиента при выдаче микрокредита посредством сверки его персональных данных с базами операторов мобильной связи, обеспечивающей проверку принадлежности клиенту данного абонентского номера.

В целом, вышеуказанные меры позволили повысить прозрачность рынка микрофинансирования, обеспечить защиту прав потребителей финансовых услуг, снизить системные риски и вывести с рынка недобросовестных участников.

5 Однако проблема финансовых пирамид остается актуальной. Мошенники теперь выбирают различные способы маскировки, выдавая свою деятельность за инвестиционную, посредническую либо формируя «клубы по интересам», туристические клубы и даже якобы букмекерские конторы.

Для выявления и пресечения деятельности финансовых пирамид и оперативной передачи информации о них в правоохранительные органы в 2020 году по поручению помощника президента – пекретаря Совета безопасности РК А. О. Исекешева создана Межведомственная рабочая группа (МВРГ), в которую, помимо агентства, входят МВД РК, ГП РК, МИОР РК, АФМ РК и НБРК. Деятельность МВРГ в первую очередь направлена на выработку эффективных мер по выявлению финансовых пирамид и прекращению их деятельности.

Работы МВРГ пресечена деятельность 12 финансовых пирамид на начальном этапе. В рамках межведомственного взаимодействия агентством совместно с государственными органами был сформирован и утвержден перечень из 39 признаков финансовых пирамид. Из них ключевыми являются: отсутствие лицензии и учетной регистрации агентства; массированная реклама в СМИ, интернет-ресурсах, в том числе в социальных сетях, с обещанием высокой доходности; организация бизнеса на принципах сетевого маркетинга, когда доход вкладчика формируется за счет вложений новых привлекаемых им участников, и др.

МВРГ на основе утвержденных признаков финансовых пирамид и коллегиальных решений сформирован список организаций, имеющих признаки финансовых пирамид и нелицензированной инвестиционной деятельности. На сегодня в списке значатся 121 субъект: 65 нелицензированных инвестиционных посредников и 56 финансовых пирамид. Вышеуказанный список опубликован на официальном интернет-ресурсе агентства.

В случае, если граждане столкнулись с деятельностью финансовых пирамид или вложили в них средства, им следует незамедлительно обратиться в правоохранительные органы.

Другим видом интернет-мошенничества является мошенничество с банковскими картами и счетами. По данным платежных систем Visa и Mastercard, в более 90 процентах фактов мошенничества присутствует вина самого пользователя финансовой услуги. Обычно потребитель самостоятельно передает преступникам свои личные данные, SMS-коды или пароли от личных кабинетов. Нередки случаи фишинга, ввода личных данных на сайтах, копирующих оригинальные, либо установки вирусных программ, которые собирают данные пользователя (в том числе пароли) и передают их злоумышленникам.

Агентством совместно с финансовыми организациями ведется системная работа по обнаружению и устранению уязвимостей в информационной защите как самих организаций, так и потенциальных угроз для потребителей. Для предотвращения кибератак в 2020-2021 годах, агентством приняты меры по блокировке 20 мошеннических интернет-ресурсов, в том числе 13 – с признаками финансовой пирамиды. В банки направлено более 400 предупреждений об угрозах информационной безопасности и обработано более 300 карт информационных инцидентов от БВУ. Для автоматизации процессов взаимодействия по вопросам информационной безопасности и повышения оперативности реагирования в пилотную эксплуатацию запущена автоматизированная система обработки информации по событиям и инцидентам информационной безопасности на финансовом рынке – АСОИ «Qainar». Данная система фиксирует события, сигналы и инциденты информационной безопасности, предупреждает об угрозах и уязвимостях.

На данный момент все 22 банка подключены к «Qainar». При этом 8 банков (АО «Евразийский банк»; ДБ АО «Сбербанк России»; АО «Банк ЦентрКредит»; АО «ForteBank»; АО ДБ «Альфа-Банк»; АО «Банк «Bank RBK», АО «Halyk Bank», АО «Altyn Bank») используют автоматизированный механизм взаимодействия.

Что для борьбы с финансовым мошенничеством делает МВД РК

Рассказывает Канат Нурмагамбетов, заместитель начальника департамента криминальной полиции министерства внутренних дел.

Развитие цифровых технологий привело к росту мошенничества с их использованием. В последнее время широкий общественный резонанс вызывают именно факты интернет-мошенничества. Если в 2019 году в Казахстане их число составляло 7,7 тысячи, то по итогам 2020 года зафиксировано более 14 тысяч таких преступлений. И только за 10 месяцев 2021-го в сравнении с аналогичным периодом прошлого года их число выросло на 80% – до 17,8 тысячи.

Самые распространенные способы совершения интернет-мошенничества – это получение предоплаты за товар или услугу по объявлениям (на них приходится половина всех преступлений), оформление онлайн-займов на сайтах микрокредитных организаций, а также хищение денег с банковских счетов после получения персональных данных владельцев.

Есть и другие распространенные среди мошенников способы. Например, почти 2 тысячи преступлений совершены под предлогом выгодного вложения денег в разные проекты, игры, инвестиции и ставки.

Что делает министерство внутренних дел, чтобы бороться с этим явлением?

С начала 2021 года заработала программа по противодействию киберпреступности на 2021-2022 годы, в регионах созданы специальные следственно-оперативные группы по их расследованию, каждый квартал проходят оперативно-профилактические мероприятия по предупреждению киберпреступности.

Например, с 8 по 14 ноября 2021 года по всей стране прошло ОПМ «Хай-тэк». Его цель – профилактика интернет-мошенничества и раскрытие преступлений, задержание совершающих их лиц. Мероприятие принесло результаты: за семь дней зарегистрировано около 300 и раскрыто 440 ранее совершенных киберпреступлений.

Всего за период проведения ОПМ установлено 261 лицо, совершившее такие преступления, задержаны 34 мошенника, совершившие более двух преступлений.

Приведу несколько примеров. Сотрудники полиции Атырауской области задержали жителя Семея, который в социальных сетях находил объявления о пропаже документов и по ним подавал заявки на получение микрозаймов. Граждане даже не подозревали об этих займах до получения уведомлений о просрочке. Установлены 320 граждан, которым причинен ущерб на сумму более 10 млн тенге.

Еще один случай: жительница Павлодарской области на сайтах размещала объявления о сдаче квартир в аренду по заниженной цене. В ходе разговора с потенциальными клиентами мошенница просила перевести задаток на различные счета, а после получения денег отключала номера телефонов и удаляла объявления. Установлена ее причастность к 30 преступлениям, причиненный ущерб – свыше 800 тысяч тенге.

Третий случай – задержан житель Туркестанской области, который в социальной сети Instagram занимался мошенничеством, обещая «раскрутить» денежные средства. Злоумышленник уверял граждан, что при внесении 25 тысяч тенге на его банковскую карту в течение суток деньги будут возвращены в двух– или трехкратном размере. Идет досудебное расследование.

Что делать, чтобы уберечь себя от интернет-мошенников?

Есть несколько простых мер безопасности.

Никому не сообщайте персональные данные, реквизиты банковских карт и не передавайте квитанции о переводах и, тем более, коды и кодовые слова. Их нельзя предоставлять даже лицам, которые говорят, что являются сотрудниками банка или полиции.

Нельзя доверять персональные данные неизвестным и непроверенным сайтам, производить предоплату без проверки, делать денежные переводы по сомнительным сделкам, а также нужно остерегаться финансовых схем без прозрачного источника дохода.

Если собираетесь установить какое-то приложение на смартфон, пользуйтесь только официальными магазинами – AppStore, PlayMarket и другими, которые верифицированы официальными разработчиками.

Регулярно меняйте пароли доступа к сервисам банков, используйте 3D-защиту и другие меры безопасности, предлагаемые финансовыми институтами, регулярно проверяйте движение денег на счетах.

Ни в коем случае не переходите по ссылкам, которые вам отправляют для оплаты чего-либо, или ссылкам, что содержатся в спам-рассылках от неизвестных контактов или во всплывающих окнах. Часто мошенники предлагают для оплаты перейти по ссылке, которая на самом деле является фишинговой и имитирует настоящий сайт объявлений или сайт банкинга.

Эти простые меры помогут избежать мошенников и сохранить свои деньги и личные данные.

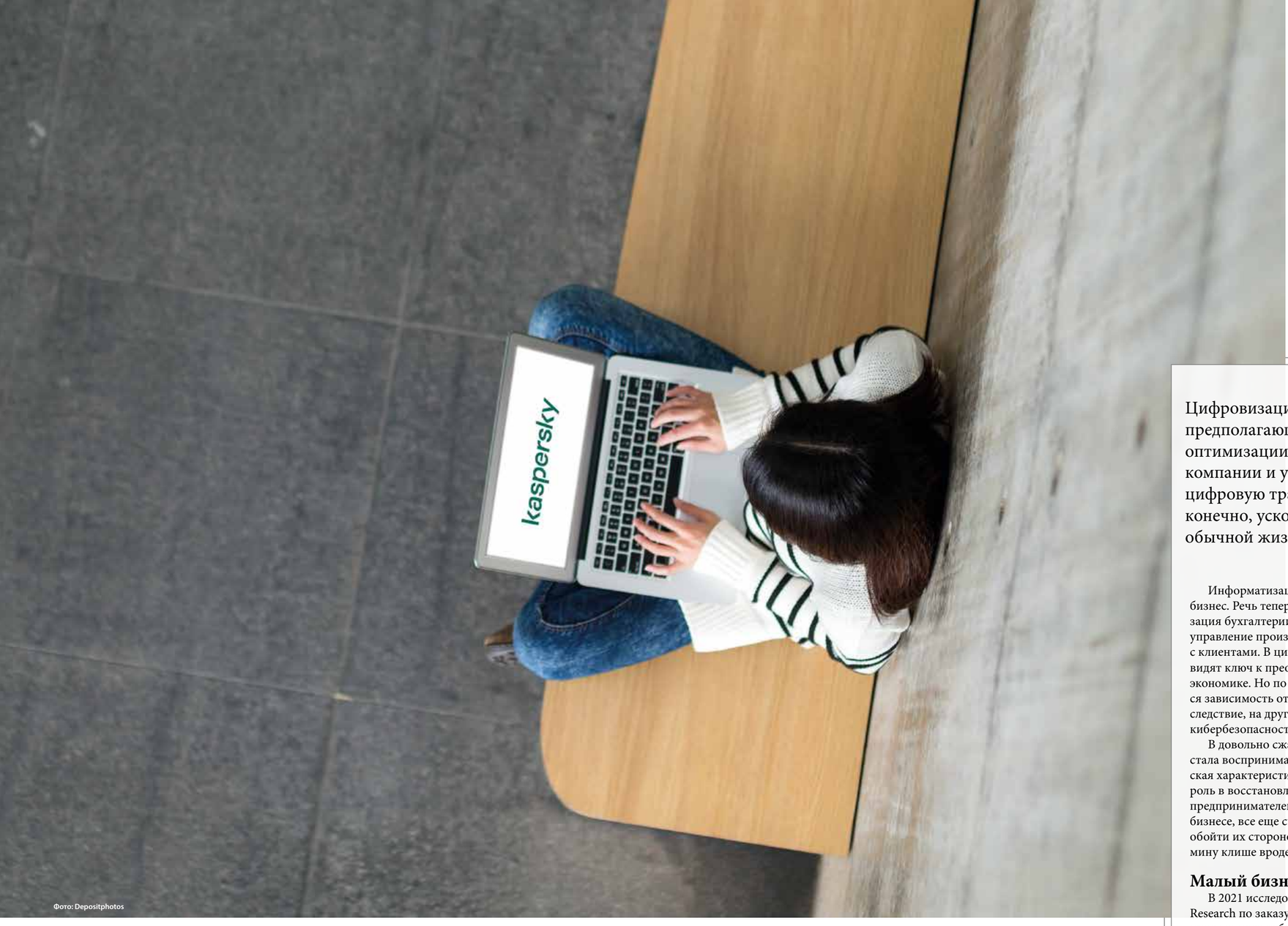


Фото: Depositphotos

Влияние современных цифровых угроз на бизнес в Казахстане

Разбираемся вместе с «Лабораторией Касперского»

Цифровизация бизнеса – это глубокая трансформация, предполагающая использование цифровых технологий для оптимизации бизнес-процессов, повышения производительности компании и улучшения взаимодействия с клиентами. Тренд на цифровую трансформацию появился не вчера, но пандемия его, конечно, ускорила. То, что произошло всего за несколько месяцев, в обычной жизни развивалось бы пять-шесть лет.

Информатизация все глубже проникает в бизнес. Речь теперь идет не только об автоматизация бухгалтерии, например, оцифровывается управление производством, весь цикл отношений с клиентами. В цифровизации предприниматели видят ключ к преодолению турбулентности в экономике. Но по этой же причине формируется зависимость от цифровых технологий и, как следствие, на другой уровень выходит угроза кибербезопасности.

В довольно сжатые сроки кибербезопасность стала восприниматься как базовая и критическая характеристика, которая сыграет ключевую роль в восстановлении экономики. Однако часть предпринимателей, особенно в малом и среднем бизнесе, все еще считает, что новые угрозы могут обойти их стороной, размышляя набившим оскомину клише вроде «да и красть у нас нечего».

Малый бизнес

В 2021 исследовательское агентство Arlington Research по заказу «Лаборатории Касперского» провело масштабное исследование (22 страны по всему миру) на тему «Как малый и средний бизнес переживает пандемию». Согласно результатам этого исследования, более 51% предпринимателей в Казахстане назвали внедрение новых технологий наиболее приоритетной задачей для стабильного функционирования их бизнеса во время пандемии.

В список необходимых мер вошли обеспечение персонала новыми технологиями и оборудованием, сервисами коммуникации и совместной работы, позволяющими перевести бизнес в онлайн, а сотрудникам – работать удаленно или в гибридном формате.

В тройку наиболее значимых активностей в сложный для бизнеса период вошли сохранение рабочих мест (об этом сообщили 46% респондентов) и поддержание бизнеса любой ценой (59%). Однако для этого собственникам бизнеса пришлось принимать непростые решения. Так, в 36% компаний был сокращен бюджет, в 33% – временно закрыты некоторые или все офисы и другие физические площади (например, торговые точки или склады). В то же время были и те, кто увидел в сложной ситуации новые возможности. Так, в каждой пятой небольшой компании были запущены новые продукты или услуги.

Исследования не раз доказывали, что на эффективность бизнеса напрямую влияет удовлетворенность персонала. Предприниматели осознают ценность сотрудников. В результате опроса выяснилось, что удержание сотрудников стало приоритетом для компаний, даже несмотря на вынужденное сокращение бюджета. Так, в следующие 12 месяцев казахстанские предприниматели планируют повышать зарплаты (32%).

«Мы видим, что вызванные пандемией сложности породили у бизнеса новые потребности в технологиях. Особую актуальность приобрели онлайн-сервисы, и те предприятия, род деятельности которых позволял запустить их, оказались в более выгодном положении по сравнению с теми, для которых цифровизация по тем или иным причинам была невозможна. К счастью, существует множество простых в управлении сервисов, включая бесплатные, для установки, управления и обслуживания которых не нужен выделенный IT-администратор. Однако еще раз хочется отметить, что такая цифровизация должна быть безопасной для бизнеса», – прокомментировал Валерий Зубанов, коммерческий директор «Лаборатории Касперского» в Центральной Азии.

Основные киберугрозы для МСБ

Небольшие компании сталкиваются с разными проблемами кибербезопасности. Почти в трети казахстанских компаний (36%) возникают вопросы, как защищать корпоративные данные на личных устройствах сотрудников, 34% испытывают трудности с обеспечением безопасности в связи с тем, что на одного сотрудника приходится несколько рабочих устройств, 24% называют проблемой недостаток цифровой грамотности среди сотрудников. 28% компаний сталкиваются с тем, что сотрудники не соблюдают правила информационной безопасности при ведении переписки по электронной почте, а каждая пятая (20%) – с тем, что они не всегда используют собственный отдельный логин и пароль для входа в системы. Для 22% компаний одна из основных проблем в области информационной безопасности – обеспечить соответствие своих IT-систем законодательным требованиям.

Результаты исследования показывают, что представители небольших казахстанских компаний нуждаются в советах по кибербезопасности. Так, 45% хотели бы понимать, как бороться с утечками, 34% – как избежать атак программ-вымогателей и что делать, если столкнулись с этой проблемой, 29% – как обеспечивать безопасность облачных сервисов.

«У всех, вне зависимости от размера компаний, есть очень ценная информация для злоумышленников. Это и интеллектуальная собственность, и финансовые или персональные данные. Но, в отличие от крупных корпораций, малый и средний бизнес в Казахстане особенно подвержен целевым атакам, так как эти компании менее защищены с точки зрения кибербезопасности. И это еще не все: злоумышленники стремятся использовать доступ к сетям МСБ в рамках многоэтапных операций по проникновению в сети более крупных организаций. Бизнесу угрожают не только целевые атаки, очень часто заражение происходит в ходе массовых рассылок вредоносного ПО, нацеленных на случайных жертв», – комментирует Валерий Зубанов.

Крупный бизнес

В мае-июне 2021 года «Лаборатория Касперского» провела опрос «Информационная безопасность бизнеса». В нем приняли участие 4 303 специалиста из компаний с более чем 50 сотрудниками из 31 страны. По данным этого опроса, в 2021 году крупные компании в Казахстане и России теряли в среднем около $900 тысяч долларов в результате киберпреступлений.

Самыми дорогими видами киберинцидентов для крупного бизнеса в России и Казахстане стали (в порядке убывания): утечки данных из электронных систем (ущерб от одного такого инцидента превышает $1 млн долларов), целевые атаки (около $900 тысяч) и атаки на цепочки поставок (более $700 тысяч). Для МСБ-сектора самыми дорогими стали инциденты, произошедшие в результате нарушения сотрудниками политик кибербезопасности, атаки криптомайнеров и инциденты, в ходе которых были атакованы сторонние поставщики, с которыми компания обменивается данными.

Последний тип атак оказался наиболее дорогостоящим среди компаний по глобальной статистике. Средняя сумма ущерба составила $1,4 млн долларов, а в целом с такими утечками столкнулись 32% организаций по всему миру. При этом средняя сумма ущерба от одной утечки данных от атак любого типа для крупных компаний во всем мире составляет $926 тысяч долларов.

«В ходе нового исследования мы выяснили, что самые сложные задачи с точки зрения кибербезопасности, стоящие перед бизнесом, – это вопросы защиты данных, соответствия законодательным нормам, а также повышение уровня цифровой грамотности сотрудников. Кроме того, бизнес беспокоит растущая сложность IT-инфраструктуры, поскольку это приводит к необходимости увеличивать соответствующий бюджет, – комментирует Валерий Зубанов. – Чтобы свести к минимуму риск кибератак и утечек данных, мы рекомендуем компаниям регулярно проводить для сотрудников тренинги по информационной безопасности, использовать защитные решения для конечных устройств в сочетании с инструментами для обнаружения угроз, обходящих традиционные антивирусные средства».

Такое сочетание доступно, например, в рамках трёхуровневого подхода «Лаборатории Касперского» к кибербезопасности. Самый продвинутый уровень – это Kaspersky Expert Security. Он предназначен для корпораций и промышленных предприятий. На нём доступны платформа для обнаружения продвинутых угроз на уровне сети Kaspersky Anti Targeted Attack и Kaspersky EDR – мощная система, которая предоставляет ИБ-специалистам полную картину событий в инфраструктуре рабочих мест и серверов и обеспечивает их эффективную защиту от сложных угроз и APT-атак. Кроме того, на этом уровне предлагается доступ к аналитическим данным портала Kaspersky Threat Intelligence и тренингам для ИБ-специалистов.

Информационная безопасность бизнеса и как ее обеспечить

Информационная безопасность – меры, предпринимаемые для защиты конфиденциальных данных, разработок, идей, технологий и денег компании. «Информационная безопасность» понятие настолько широкое, что все ее аспекты частенько не укладываются в одну картину и не воспринимаются, как части одной проблемы, поэтому ей частенько пренебрегают. Чего, конечно, делать не стоит. Обеспечение информационной безопасности предприятия, вопреки распространенному заблуждению, часто не сопряжено с каким-то огромными затратами. Значительно повысить качество IT-инфраструктуры можно соблюдая ряд достаточно простых правил. Самое главное в этом вопросе – системность.

Информационная безопасность включает в себя сохранение конфиденциальности данных, создание иерархии доступа к информации, обеспечение бесперебойной работы программного обеспечения, в том числе корректное зеркалирование и бэкапирование критичных данных, а также контроль над банковскими счетами и другими финансовыми инструментами. Так, абсолютно любые запрашиваемые сведения могут быть доступны только тем пользователям, которые могут в них нуждаться по долгу службы. К примеру, только сотрудники отдела закупок могут получить сведения о поставщиках, при это покупателей им знать не обязательно. Это поможет обезопасить базу данных, ведь уволенный сотрудник, имеющий доступ ко всем базам данных, а не только по профилю, может продать их конкурентам.

Фото: Depositphotos

Фото: Depositphotos

Главная брешь в информационной безопасности – человеческий фактор. Важно создать иерархию доступа к данным и не отклоняться от правил. После того, как сотрудник переводится на другую позицию в компании или покидает команду, нужно менять пароли, а также конфисковать электронные ключи. Кроме того, важно проводить тренинги по повышению компьютерной грамотности, потому что человеческий фактор – это не только обида или злой умысел. Часто это невнимательность, отсутствие нужного уровня понимания процессов, любопытство, переработки.

Так, одна из основных хакерских атак на бизнес, фишинг, – это чаще всего не виртуозный взлом ПО, а игра на эмоциях недостаточно подкованных сотрудников. Фишинг – это создание почти точной копии определенного сайта с целью получения личных данных пользователя, данные карты, пароли от CMS-систем сайтов предприятий или от аккаунтов в социальных сетях. Невнимательный пользователь отзывается на эмоциональный призыв срочно написать данные карты или пароли – в ином случае фишинговый сайт грозится что-то удалить или куда-то отправить – и теряет доступы, деньги, репутацию.

Угрозы информационной безопасности бывают внешние и внутренние. Внутренние – это отсутствие или несоблюдение правил и регламентов, иерархии доступа к данным, неосторожность сотрудников или безответственное отношение к работе. Внешние угрозы – это последствия политических событий (например, изъятие техники), стихийные бедствия, форс-мажоры в офисных центрах и хакерские атаки, Вирусы-шифровальщики, DDoS-атаки, фишинг, собственно, и другие.

«Лаборатория Касперского» рекомендует организациям придерживаться следующих мер для обеспечения кибербезопасности:

- убедитесь, что устройства сотрудников, программное обеспечение, приложения и сервисы регулярно обновляются;
- принимайте ключевые меры для защиты корпоративных данных и устройств, включая установку пароля, шифрование рабочих устройств и обеспечение резервного копирования данных;
- убедитесь, что ваши сотрудники знают, к кому обратиться, если у них возникнут проблемы с IT или кибербезопасностью. Уделяйте особое внимание тем, кому приходится работать с личных устройств: дайте им специальные рекомендации по безопасности и предоставьте соответствующие политики;
- запланируйте тренинги для сотрудников для повышения их цифровой грамотности, в том числе онлайн. Это позволит научить их управлять учетными записями и паролями, обеспечивать безопасность электронной почты и конечных устройств;
- установите проверенное защитное ПО для бизнеса на все конечные устройства, включая мобильные девайсы.

Как распознать финансовую пирамиду

Казахстанцы вновь и вновь попадаются на уловки мошенников. Как не оказаться в их числе?

С первой финансовой пирамидой мир столкнулся в 1716-1720 годах, когда во Францию приехал шотландский экономист Джоном Ло. Заручившись поддержкой регента короля, экономист создал «Западную компанию», затем распустил слухи о небывалом успехе компании, а после начал продавать акции. Однако вскоре выяснилось, что никакой серьезной деятельности она не ведет. Экономист бежал в Италию, оставив одураченных французов. За 300 лет мир сильно изменился, не изменились только «шотландские экономисты» и люди, попадающие на их уловки.

Алимхан Адилов

В августе этого года МВД РК выступило с докладом. Как выяснилось, в Казахстане по-прежнему растет количество преступлений, связанных с финансовыми пирамидами. Только с начала 2021 года министерством внутренних дел расследовано 330 уголовных дел о финансовых пирамидах (для сравнения, в 2020 году их было 218). Под следствием находятся 62 человека, из них 55 арестованы, 177 дел направлено в суд в 2021 году. Совокупно, по данным профильного министерства, общее количество потерпевших по уголовным делам о финансовых пирамидах (находящимся в производстве) составляет свыше 19 тыс. человек, которые заявили об ущербе на общую сумму более 21 млрд тенге. В октябре этого года Агентство по регулированию и развитию финансового рынка даже внесло в список 56 организаций с признаками финансовой пирамиды и 65 лжеброкеров и разместило у себя на сайте.

Кто виноват

В Казахстане расследованием дел, связанных с финансовыми пирамидами, занимаются правоохранительные структуры. Работают они, чаще всего, в связке с Агентством РК по регулированию и развитию финансового рынка. Вторые ведут мониторинг информационного пространства в интернете, отслеживают социальные сети, блоги, форумы, видеохостинги и мессенджеры, а также работают с обращениями физических и юридических лиц. Для более эффективной осведомленности агентство информирует все субъекты финансового рынка о подозрительных компаниях, а также взаимодействует с уполномоченными органами для проведения дальнейшей проверки и блокировки сайтов таких компаний.

Однако все эти списки и регулярное информирование профильных ведомств не останавливают казахстанцев в порывах нести деньги мошенникам. Официальный представитель столичного департамента экономических расследований Айнур Хамзаева подчеркивает, что дело здесь по-прежнему в вере населения в легкие деньги, а также в низком уровне финансовой грамотности.

Что делать

Во-первых, говорит Хамзаева, стоит с подозрением отнестись к тому, что вас просят вложить крупную сумму денежных средств. Далее следует обратить внимание на очень высокие проценты, которые финансовые пирамиды «гарантируют» на вложенный капитал. Главная задача мошенников, говорит эксперт, – привлечь как можно больше людей.

«Самый главный мотив – это жадность и желание больших денег. Поэтому устроители пирамид не скупятся на обещание больших доходностей, и 20, и 30% в месяц для них не предел. Если же сравнить с обычными инвестиционными фондами, то там даже нет и намека на обещание дохода в будущем», – говорит Хамзаева.

Также один из характерных сигналов – условия возврата денег: в пирамиде, чтобы вернуть и/или преумножить деньги, нужно привлечь своих друзей или знакомых.

Чаще всего финансовая пирамида – это компания которая зарегистрирована недавно, у нее минимальный уставный капитал и единственный учредитель. «Отличительные черты финансовых пирамид - это активная и навязчивая реклама в социальных сетях, различные презентации, розыгрыши всевозможных призов, подарков, путевок, массовая раздача листовок, почтовые и e-mail рассылки», – говорит Хамзаева.

Еще одна важная деталь – в заключаемых договорах почти никогда не прописывается ответственность.

Компания, подчеркивает эксперт, чаще всего может работать под видом МФО, кредитного бюро, центра финансовых услуг.

«А еще такие компании принимают наличные деньги либо используют различные системы интернет-платежей и переводов без применения специальных расчетных счетов компании в банках. И главное – они не имеют лицензии Агентства по регулированию и развитию финансового рынка на привлечение денег от граждан», – резюмирует Хамзаева.

Какие бывают пирамиды

Чтобы не оказаться вкладчиком в очередной финансовой пирамиде, стоит знать, какими они в принципе бывают. Агентство по финансовому мониторингу РК выделяет четыре вида пирамид.

Первый тип – многоуровневая пирамида. Такая мошенническая организация вменяет в обязанность каждому участнику сделать выгодный вклад при вступлении, распределяемый между пригласившим новичка и другими, более поздними участниками. Далее каждый прибывший обязательно должен пригласить n-ое число участников, вклады которых пойдут новичку и пригласившему его ранее. Причиной краха таким образом организованной пирамиды является нехватка новых участников.

Схема Понци – еще один вид финансовой пирамиды. Изобретатель этой схемы Чарльз Понци организовал первую финансовую пирамиду на территории США. Для получения дохода первоначальным вкладчикам нет нужды привлекать новичков. Первопроходцы получают доход за счет собственных средств организатора этой схемы, привлечение новых вкладчиков основывается на распространении информации об ультрасовременной супердоходной инвестиционной разработке организатора, которая подкрепляется словами вкладчиков, получивших прибыль.

Третий тип – маскирующаяся пирамида. «Такие пирамиды маскируются под многоуровневый маркетинг, то есть это пирамиды, продающие какой-либо товар или услугу. Участники вступают в данную пирамиду и находят человека, приобретающего данный товар или услугу. После чего участник получает комиссионное вознаграждение. Товар – это своего рода прикрытие организации для снятия с себя подозрения в деятельности обычной финансовой пирамиды», – говорится в сообщении Агентства.

Четвертый тип – это матричная пирамида. Вышеперечисленные пирамиды могут быть еще и матричного типа. Это значит, что каждому новому участнику необходимо заполнить ряды участников под собой, и только лишь после заполнения рядов второго и третьего порядка он сможет получить прибыль.

В агентстве также отмечают, что отличительная особенность работы финансовых пирамид – это довольно сильное психологическое и эмоциональное давление на сознание клиента. «Это и навязчивая реклама, и стимулирование привлечения новых клиентов, и прочие психологические приемы, главной целью которых является не только удержание клиента, но и вовлечение новых участников», – отмечается в сообщении Агентства.

Вымышленные инвестиции. Как социальная инженерия работает в финпирамидах

Финансовые пирамиды – уязвимое место общества, и Казахстан не исключение

По данным Комитета по правовой статистике и специальным учетам Генпрокуратуры РК, на 1 ноября 2021 года в производстве находилось около 400 уголовных дел по статье 217 (Создание и руководство финансовой (инвестиционной) пирамидой). Установленная сумма ущерба, причиненного физическим лицам, составила 87,4 млрд тенге.

Динара Бекмагамбетова

Вымышленные инвестиции

Крупнейшая в истории независимого Казахстана пирамида была раскрыта в 2017 году. Правоохранительные органы в ходе досудебного расследования установили, что с марта 2016-го по июнь 2017 года граждане Испании, Кабо-Верде и России создали на территории Казахстана финансовую пирамиду Questra World и руководили ею в составе транснациональной организованной преступной группы.

Как сообщал журналистам официальный представитель МВД Нурдильда Ораз, руководители пирамиды обещали вкладчикам доходность в размере до 336% от инвестиций. Гражданам предлагали приобрести вымышленные инвестиционные портфели стоимостью от 90 до 500 тыс. евро с использованием виртуальной валюты. Полученные средства руководители пирамиды распределяли между собой.

От действий мошенников пострадали тысячи казахстанцев. Некоторые граждане для участия в пирамиде продали квартиры. Общая сумма ущерба, по данным МВД, превысила 1 млрд тенге.

Досудебное расследование по этому делу завершилось только в этом году, и в начале ноября материалы были переданы в суд. Однако 19 ноября информационное агентство Tengrinews сообщило, что специализированный суд по уголовным делам Нур-Султана вернул материалы дела прокурору города для устранения «существенных нарушений уголовно-процессуального законодательства, препятствующих назначению главного судебного разбирательства».

Одну из создательниц финансовой пирамиды Questra World Ольгу Клейнард экстрадировали из Беларуси в Казахстан в августе 2020 года. По данным правоохранительных органов, Клейнард курировала действия мошенников на территории Казахстана.

Отметим, создание финансовой пирамиды, согласно Уголовному кодексу РК, наказывается штрафом в размере до 3 тыс. МРП, привлечением к общественным работам на срок до 800 часов либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок и с конфискацией имущества.

Если же это деяние совершено группой лиц по предварительному сговору, неоднократно, лицом с использованием служебного положения или с привлечением денег или иного имущества в крупном размере, срок ограничения/лишения свободы вырастает до семи лет, также с конфискацией имущества и лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.


Фото: Depositphotos

Обман на криптовалюте

Расследование в отношении крупнейшей российской пирамиды в современной истории также все еще продолжается. Компания «Финико», по данным прокуратуры Татарстана, вела деятельность с июня 2018 по декабрь 2020 года.


Фото: Depositphotos

Организаторы схемы сулили инвесторам ежемесячный доход до 25% годовых за счет вложения средств в криптовалюту и фондовые рынки. Сначала предполагалось, что пирамида действовала только в России, но впоследствии нашлись пострадавшие и в Казахстане.

По оценкам независимых экспертов, совокупный ущерб от деятельности «Финико» превышает $4 млрд, число пострадавших составило не менее 850 тыс. человек.

Уголовное дело против компании «Финико» было открыто в декабре 2020 года, а в феврале 2021 года Центральный банк России добавил организацию в список компаний с признаками финансовой пирамиды. Однако схема продолжала работать вплоть до июля текущего года, когда организаторы внезапно приостановили выплаты вкладчикам.

В конце июля правоохранительные органы Татарстана задержали одного из основателей «Финико» Кирилла Доронина. Позже под стражу водворили еще трех организаторов мошеннической схемы – Ильгиза Шакирова, Лилию Нуриеву и Дину Габдуллину.

Но это вряд ли поможет потерпевшим вернуть деньги. Доронин утверждает, что потерял доступ к личным кабинетам вкладчиков. По данным портала Forklog, соучредители «Финико», оставшиеся на свободе, записали ответное видеообращение, в котором заявили, что в начале июля перевели все деньги вкладчиков пирамиды самому Доронину по его просьбе.

В начале ноября Forklog сообщил о том, что неизвестные вывели оставшиеся на одном из кошельков «Финико» средства на общую сумму 750 BTC (на тот момент около $48,8 млн).

Бисерные аферы

Довольно необычную форму финансовые пирамиды принимали в соседних странах Центральной Азии. В 2003 году в Кыргызстане, а затем и в Таджикистане прогремели дела о так называемых бисерных пирамидах. Организаторы предлагали желающим возможность легкой работы на дому. Гражданам под денежный залог предлагались бисер и леска. Бисер нужно было нанизать на леску, а готовые бусы вернуть организаторам две недели спустя. За усилия участники получали обратно вложенные средства плюс гонорар за проделанную работу.

В Кыргызстане компания «Уорлд Энтерпрайз» предоставляла вкладчикам два пакетика бисера и леску себестоимостью 5-10 сомов (20-30 тенге по курсу 2003 года), размер залога же составлял 300 сомов (почти тысячу тенге). Первое время компания действительно возвращала участникам денежный залог и выплачивала вознаграждение за работу. Существующих «работников» призывали приводить в компанию и других желающих легко заработать. Несколько месяцев спустя пирамида закрылась, а кыргызстанцы потеряли несколько десятков тысяч долларов сбережений.

В Таджикистане аналогичная бисерная пирамида носила название «Джамал и Ко». Организаторов в этом случае задержали, и все они понесли наказание. Глава компании Джамшед Сияев был приговорен к 11 годам лишения свободы, его заместитель Зафар Камолов и главный бухгалтер Вячеслав Цой получили по восемь лет. Генпрокуратуре Таджикистана удалось даже вернуть часть денег пострадавшим. Однако в большинстве случаев компенсация не превышала тысячи долларов, в то время как убытки многих вкладчиков исчислялись в десятках тысяч. В августе 2005 года местные СМИ сообщали, что около 54 тыс. вкладчиков так и не получили свои деньги обратно. Сумма ущерба составила 77 млн сомони (примерно $25 млн).

Мавроди и в Африке Мавроди

Печально известный на постсоветском пространстве основатель финпирамиды МММ Сергей Мавроди не прекратил деятельность и после освобождения из тюрьмы в 2007 году. В 2011 году он пытался запустить новые пирамиды в России, Казахстане и Беларуси, но из этого ничего не вышло. Тогда Мавроди переключился на другие страны. Новая пирамида получила название MMM Global и обещала вкладчикам 30% годовых. Пирамида маскировалась под так называемый клуб взаимопомощи, члены которого могли занимать друг другу деньги. Каждый новый член пирамиды обязан был внести вступительный взнос.

Неожиданных успехов Мавроди удалось добиться в странах Африки – в новую MMM вступили миллионы людей из Нигерии, ЮАР, Зимбабве, Кении, Египта и Марокко. Особенно пострадали нигерийцы – по данным компании Nigeria Deposit Insurance Corporation (NDIC), в MMM Nigeria вложили сбережения около 3 млн граждан. Для многих из них участие в финпирамиде было единственным источником дохода. Однако схема проработала в Нигерии всего год. В декабре 2016 года все счета вкладчиков были заморожены, а сотрудники MMM Nigeria объявили о временных неполадках. Однако деньги вкладчикам так и не вернули. Общая сумма ущерба составила около $60 млн.

США

Самое суровое за последние несколько лет наказание за создание финансовой пирамиды понес 80-летний Уильям Нил Галлахер из Техаса, известный под прозвищем Money Doctor. 31 августа 2021 года он признал вину по обвинениям в вымогательстве миллионов долларов у пожилых людей с помощью схемы Понци. 1 ноября этого года Галлахер был приговорен к трем пожизненным срокам тюремного заключения.

Галлахер работал ведущим на нескольких христианских радиостанциях. В своих радиопередачах он призывал слушателей инвестировать в принадлежащую ему компанию Gallagher Financial Group. Полученные деньги, однако, никуда не инвестировались. Таким образом Галлахер вымогал деньги в течение десяти лет.

Одним из отягчающих обстоятельств в деле Галахера стал тот факт, что его жертвами были в основном пенсионеры, регулярно слушающие христианское радио. Более 12 потерпевших преклонного возраста выступили в суде с показаниями против Галлахера. Они вложили в его схему от $50 тыс. до $600 тыс.

Конфиденциальность перестала быть темой для гиков

О прогнозах и трендах в сфере конфиденциальности на 2022 год рассказывает коммерческий директор «Лаборатории Касперского» в Казахстане и Центральной Азии Валерий Зубанов.

Глобальная сеть сегодня обеспечивает такие базовые потребности общества, как логистика, работа государственных служб и банковских сервисов. Потребители общаются с компаниями в мессенджерах и заказывают доставку еды вместо того, чтобы ходить по магазинам, научные конференции проходят на виртуальных платформах, а число отраслей, в которых удаленная работа стала нормой, продолжает расти.

Все эти процессы сказываются на сфере конфиденциальности – необходимости предотвращения разглашения, утечки какой-либо информации в цифровой среде. Сегодня компании хотят получать больше информации о действиях своих клиентов в интернете, чтобы повышать качество обслуживания, и одновременно с этим усложняют процедуры авторизации, чтобы противостоять мошенникам. Власти многих стран стремятся упростить идентификацию пользователей в целях борьбы с киберпреступниками и «традиционными» группировками, которые координируют свою деятельность онлайн. Граждан, в свою очередь, все больше беспокоят «надзорный капитализм», недостаток приватности и зависимость от онлайн-сервисов.

Можно отметить, что большинство из прошлых наших прогнозов относительно трендов конфиденциальности в этом году действительно сбылись и превратились в глобальные тенденции. Технологии сохранения конфиденциальности стали одной из самых обсуждаемых тем в сфере технического прогресса. Стоит признать: такие нововведения, как локальная обработка звука для Siri или частное вычислительное ядро Android, – это большой шаг в сторону повышения конфиденциальности пользователей. Кроме того, в этой сфере появилось множество новых сервисов, созданных молодыми компаниями, которые только начинают монетизировать свои услуги. Мы также наблюдаем усиление тенденции к защите конфиденциальности (которое отражается и в маркетинге, и в технологиях) среди разработчиков приложений для iOS и Android. Facebook (сейчас Meta) тоже старается обеспечить больший уровень приватности своих пользователей: компания ввела сквозное шифрование резервных копий в WhatsApp и избавилась от технологии распознавания лиц в Facebook.

Мы надеемся, что 2022 год будет последним годом пандемии, однако тенденции в сфере конфиденциальности вряд ли изменятся. Какими будут последствия этих процессов? Ниже мы расскажем об основных действующих силах, которые, по нашему мнению, будут формировать ландшафт конфиденциальности в 2022 году.

1. Технологические гиганты предоставят людям больше инструментов для контроля конфиденциальности – в определенных пределах.

Поскольку компании по всему миру вынуждены соблюдать множество строгих нормативов по защите данных, они будут предоставлять клиентам своих сервисов все больше инструментов для контроля конфиденциальности. Возможно, с помощью новых кнопок и переключателей опытные пользователи и правда смогут установить уровень приватности, соответствующий их потребностям. Однако тем, кто разбирается в компьютерах немного хуже, не стоит думать, что их конфиденциальность будет защищена по умолчанию. Даже если по закону компании обязаны сделать это, они все равно продолжат искать лазейки, чтобы заставить людей выбирать настройки с меньшим уровнем приватности, поскольку их прибыль непосредственно зависит от сбора данных.

2. Власти обеспокоены растущим влиянием технологических гигантов и объемами данных, которые они собирают. Это приведет к конфликтам – и компромиссам.

Власти создают собственную цифровую инфраструктуру, чтобы упростить доступ к государственным службам и, хотелось бы верить, сделать их работу более прозрачной. Кроме того, таким образом они рассчитывают получать больше информации о гражданах, чтобы лучше контролировать их. Неудивительно, что их все больше интересуют данные пользователей, циркулирующие в больших коммерческих экосистемах. Это приведет к появлению новых нормативов – законов о защите, локализации данных, а также требований, определяющих, какая информация и в каких случаях должна быть доступна правоохранительным органам. Ситуация с внедрением Apple системы CSAM отлично показала, как сложно найти баланс между шифрованием данных и конфиденциальностью пользователей с одной стороны – и выявлением преступных действий с другой.

3. Машинное обучение – это, конечно, хорошо, но скоро станет больше разговоров о машинном «разучении».

Современное машинное обучение обычно подразумевает тренировки огромных нейросетей с использованием колоссального списка параметров, которые иногда исчисляются миллиардами (некоторые считают их аналогами мозговых нейронов, хотя это не совсем верно). Нейросети можно научить не только поддерживать простые взаимодействия с пользователями, но и запоминать целые фрагменты данных, что в свою очередь может привести к утечкам конфиденциальной информации и материалов, защищенных авторским правом, или закреплению социальных предрассудков. Кроме того, возникает интересный правовой вопрос: если модель машинного обучения тренировали с использованием моих данных, могу ли я, ссылаясь, например, на регламент GDPR, потребовать полностью удалить результаты этих тренировок из системы? И если да, чем это обернется для компаний, работающих на основе данных? Все просто: им придется переобучить модели с нуля, что может стоить недешево. В связи с этим могут появиться новые интересные технологии, которые не только будут препятствовать запоминанию (как, например, обучение с использованием методов дифференциальной приватности), но и позволят исследователям удалять данные из уже обученных систем.

4. Пользователи и регулирующие органы потребуют сделать алгоритмы более прозрачными.

Сложные алгоритмы, такие как машинное обучение, все чаще используются для принятия решений в самых разных ситуациях – от оценки кредитоспособности заемщиков до распознавания лиц при показе рекламных объявлений. И пока одни люди наслаждаются прелестями персонализации, для других она может стать источником неприятных ситуаций или даже дискриминации. Представьте интернет-магазин, который делит пользователей на более и менее ценных с помощью некоего алгоритма, определяющего показатель LTV (пожизненной ценности клиента). Перспективные покупатели могут общаться с сотрудниками службы поддержки в живом чате, а менее удачливых ждет далекий от совершенства чатбот. Если бы компьютер посчитал вас второсортным клиентом, вы бы хотели узнать, почему? А что, если бы на этом основании вам отказали в выдаче кредитной карты? В ипотеке? В пересадке почки? Алгоритмы используются во многих сферах, поэтому в будущем нас ждет еще больше дискуссий и новых правил вокруг объяснения, опровержения и корректировки решений, принятых автоматизированными системами. Появятся и новые исследования, призванные сделать методы машинного обучения более понятными.

5. Благодаря работе из дома люди станут больше внимания уделять защите конфиденциальности – не без помощи своих работодателей.

Работая из дома в период пандемии, вы наверняка расширили свое знание IT-сленга: такие выражения, как «инфраструктура виртуальных рабочих столов», «одноразовый пароль», «двухфакторные ключи безопасности» и т.д., стали известны даже продавцам и банковским служащим. Пандемия закончится, но культура работы из дома может остаться с нами надолго. Когда сотрудники используют одни и те же устройства для рабочих и личных нужд, периметр корпоративной сети расширяется. Чтобы защитить его, службам безопасности придется позаботиться о повышении информированности персонала. Это значит, что все больше людей будут участвовать в тренингах по кибербезопасности и защите конфиденциальности и применять рабочие навыки, такие как использование двухфакторной авторизации, в обычной жизни.

Подводя итог: конфиденциальность перестала быть темой для гиков и шифропанков и превратилась в один из главных предметов дискуссии о правах личности и человека, безопасности и деловой этике – между обществом, бизнесом и властями. Мы надеемся, что результатом этой дискуссии станет более прозрачное, честное и разумное использование персональных данных, а ответы на самые острые юридические, социальные и технологические вопросы, связанные с защитой конфиденциальности, будут найдены.

Технологические гиганты предоставят людям больше инструментов для контроля конфиденциальности - в определенных пределах

1

Возможно, с помощью новых кнопок и переключателей опытные пользователи и правда смогут установить уровень приватности, соответствующий их потребностям. Однако тем, кто разбирается в компьютерах немного хуже, не стоит думать, что их конфиденциальность будет защищена по умолчанию

Даже если по закону компании обязаны сделать это, они все равно продолжат искать лазейки, чтобы заставить людей выбирать настройки с меньшим уровнем приватности, поскольку их прибыль непосредственно зависит от сбора данных

Поскольку компании по всему миру вынуждены соблюдать множество строгих нормативов по защите данных, они будут предоставлять клиентам своих сервисов все больше инструментов для контроля конфиденциальности

Машинное обучение - это, конечно, хорошо, но скоро станет больше разговоров о машинном «разучении»

2

В связи с этим могут появиться новые интересные технологии, которые не только будут препятствовать запоминанию (как, например, обучение с использованием методов дифференциальной приватности), но и позволят исследователям удалять данные из уже обученных систем

Нейросети можно научить не только поддерживать простые взаимодействия с пользователями, но и запоминать целые фрагменты данных, что в свою очередь может привести к утечкам конфиденциальной информации и материалов, защищенных авторским правом, или закреплению социальных предрассудков

Кроме того, возникает интересный правовой вопрос: если модель машинного обучения тренировали с использованием моих данных, могу ли я, ссылаясь, например, на регламент GDPR, потребовать полностью удалить результаты этих тренировок из системы? И если да, чем это обернется для компаний, работающих на основе данных? Все просто: им придется переобучить модели с нуля, что может стоить недешево

Современное машинное обучение обычно подразумевает тренировки огромных нейросетей с использованием колоссального списка параметров, которые иногда исчисляются миллиардами (некоторые считают их аналогами мозговых нейронов, хотя это не совсем верно)

Благодаря работе из дома люди станут больше внимания уделять защите конфиденциальности - не без помощи своих работодателей

3

Чтобы защитить его, службам безопасности придется позаботиться о повышении информированности персонала. Это значит, что все больше людей будут участвовать в тренингах по кибербезопасности и защите конфиденциальности и применять рабочие навыки, такие как использование двухфакторной авторизации, в обычной жизни

Пандемия закончится, но культура работы из дома может остаться с нами надолго. Когда сотрудники используют одни и те же устройства для рабочих и личных нужд, периметр корпоративной сети расширяется

Работая из дома в период пандемии, вы наверняка расширили свое знание IT-сленга: такие выражения, как «инфраструктура виртуальных рабочих столов», «одноразовый пароль», «двухфакторные ключи безопасности» и т.д., стали известны даже продавцам и банковским служащим

Власти обеспокоены растущим влиянием технологических гигантов и объемами данных, которые они собирают. Это приведет к конфликтам - и компромиссам

4

Неудивительно, что их все больше интересуют данные пользователей, циркулирующие в больших коммерческих экосистемах. Это приведет к появлению новых нормативов - законов о защите, локализации данных, а также требований, определяющих, какая информация и в каких случаях должна быть доступна правоохранительным органам.

Власти создают собственную цифровую инфраструктуру, чтобы упростить доступ к государственным службам и, хотелось бы верить, сделать их работу более прозрачной. Кроме того, таким образом они рассчитывают получать больше информации о гражданах, чтобы лучше контролировать их

Ситуация с внедрением Apple системы CSAM отлично показала, как сложно найти баланс между шифрованием данных и конфиденциальностью пользователей с одной стороны - и выявлением преступных действий с другой

Пользователи и регулирующие органы потребуют сделать алгоритмы более прозрачными

5

Сложные алгоритмы, такие как машинное обучение, все чаще используются для принятия решений в самых разных ситуациях - от оценки кредитоспособности заемщиков до распознавания лиц при показе рекламных объявлений. И пока одни люди наслаждаются прелестями персонализации, для других она может стать источником неприятных ситуаций или даже дискриминации. Представьте интернет-магазин, который делит пользователей на более и менее ценных с помощью некоего алгоритма, определяющего показатель LTV (пожизненной ценности клиента)

Перспективные покупатели могут общаться с сотрудниками службы поддержки в живом чате, а менее удачливых ждет далекий от совершенства чатбот. Если бы компьютер посчитал вас второсортным клиентом, вы бы хотели узнать, почему? А что, если бы на этом основании вам отказали в выдаче кредитной карты? В ипотеке? В пересадке почки? Алгоритмы используются во многих сферах, поэтому в будущем нас ждет еще больше дискуссий и новых правил вокруг объяснения, опровержения и корректировки решений, принятых автоматизированными системами. Появятся и новые исследования, призванные сделать методы машинного обучения более понятными

Как мошенничество рушит доверие добросовестных инвесторов к фондовому рынку

Не так много случаев мошенничества выявляют на фондовом рынке, но те, которые уже обнаружили, являются довольно изощренными и оперируют огромными суммами. Одна из главных проблем в борьбе с мошенничеством – недостаточная финансовая грамотность населения, которой и пользуются злоумышленники.

АО «Фридом Финанс»

Биржа и надзорный орган постоянно совершенствуют системы контроля и предотвращения мошеннических действий со стороны инвесторов и профессиональных участников рынка. Если сравнивать механизмы контроля 2015 года и текущие, то можно увидеть значительную разницу в работе с базами данных.

Комплаенс профессиональных участников может предотвратить совершение сделок с признаками манипулирования еще на первичных этапах, когда инвестор отправляет к брокеру приказ. К примеру, одним из критериев манипулирования является многократное увеличение средств на брокерском счете за очень короткие сроки и сделки между своими счетами.

Проблема мошенничества будет присутствовать на рынке всегда, но в нынешних реалиях биржа и надзорный орган предпринимают действия для того, чтобы добросовестные участники не понесли экономического убытка. Сейчас выявляется не так много случаев мошенничества на фондовом рынке, но выявленные случаи являются довольно изощренными и оперируют огромными суммами. В целом, это все безусловно рушит репутацию и доверие ко всему фондовому рынку.

В последнее время злоумышленники обзванивают граждан и, представляясь сотрудниками известных брокерских компаний, предлагают установить на компьютер или мобильный телефон программу для удаленного управления устройством, маскируя эти действия под демонстрационный продукт возможностей инвестирования.

На самом деле цель преступников – похищение паролей и хищение средств казахстанцев. Мы призываем инвесторов внимательно проверять корректность адресов посещаемых сайтов и не вводить на сомнительных страницах персональную информацию, данные банковских карт, логины и пароли для входа в торговые платформы, которыми они пользуются.

Уже была информация от коллег из другой брокерской компании об активизации мошенников в интернете. В частности, в поисковых системах и мессенджерах распространялась контекстная реклама и осуществлялась рассылка с упоминанием брокерской компании, призывом участвовать в IPO и приобретать акции казахстанских и иностранных эмитентов.

В дальнейшем получатели переходили по интернет-ссылке для ввода персональных данных и перевода денежных средств, якобы в целях приобретения ценных бумаг.

В нашу компанию официальных обращений о мошеннических действиях не поступало, но есть информация, что злоумышленники обзванивают граждан и представляются сотрудниками известных брокерских компаний.

Чтобы бороться со злоумышленниками, мы усиливаем систему внутреннего контроля и совершенствуем информационные системы для устранения рисков еще на стадии подачи приказов клиентами. Например, компания не дает возможность купить клиентам ценные бумаги, если у них нет денег или обеспечения. В дальнейшем мошеннические действия могут предприниматься клиентами, так как на рынке присутствует много неликвидных инструментов, но со временем и приходом новых инвесторов эта проблема станет неактуальной.

Бывают случаи, когда из-за отсутствия ликвидности на рынке по многим инструментам крупному инвестору не составляет труда снизить цену. Для снижения подобных рисков для других участников торгов мы выступаем в качестве маркет-мейкера по многим инструментам и в некоторых случаях становимся им на добровольной основе.

Мы часто сталкиваемся с ситуацией, когда клиент хочет купить или продать по цене, значительно отличающейся от рыночной. В этих ситуациях мы не позволяем отправлять заявку на рынок и уведомляем клиента о том, что такая цена приведет к манипулированию. Мы каждый день усиливаем контрольные функции, чтобы наши клиенты не совершали манипуляций на рынке.

Финансовая грамотность населения в указанных вопросах носит основополагающее значение, поскольку знания позволяют инвестору не быть вовлеченным в данный процесс и избежать совершения сделок, связанных с манипулированием на рынке ценных бумаг, а также сделок, совершаемых в результате манипулирования рынком в результате действий других субъектов.

Для этого компания на своем официальном интернет-ресурсе разместила уведомление, информирующее клиентов об ограничениях и запретах, связанных со сделками, связанными с манипулированием на рынке ценных бумаг, а также внутренние правила, регулирующие условия распоряжения и использования инсайдерской информацией.

При работе с клиентами мы в обязательном порядке озвучиваем условия, по которым клиент может покупать или продавать ценные бумаги. При этом мы проводим обучающие семинары, где затрагиваем тему, связанную с отклонением цены и доходности, для принятия правильных и взвешенных решений по управлению личным или семейным бюджетом.

АО «Евразийский капитал»

До 2021 года наша компания не сталкивалась со случаями мошенничества, но в этом году наши клиенты неоднократно сообщали нам, что им звонили, представляясь сотрудниками «Евразийского капитала», и предлагали вкладывать деньги под очень высокие проценты. После этого мы оповестили клиентов о таких возможных мошеннических действиях третьих лиц и проинструктировали, как отличить мошенников от настоящих сотрудников компании.

Главная проблема в борьбе с мошенничеством – это недостаточная финансовая грамотность населения, именно этим пользуются злоумышленники. Чтобы избежать обмана, в первую очередь нужно помнить, что гарантировать высокие прибыли на фондовом рынке не может никто, и любые предложения получить гарантированный доход либо определенный процент в месяц заведомо являются обманом.

Чтобы повысить финграмотность населения, брокерским компаниям нужно проводить активную разъяснительную работу через свои сайты и популярные социальные сети – наша компания, например, сейчас активно этим занимается. Биржа KASE давно работает в этом направлении и сейчас занялась разработкой эффективных обучающих программ для розничных инвесторов, планирует привлечь к сотрудничеству многих участников рынка – это очень хорошо.

АО «Halyk Global Markets»

Фондовый рынок ассоциируется у людей с быстрым и легким заработком – именно это эксплуатируют мошенники. Поскольку всегда есть люди, желающие получить много денег легко и быстро, всегда будут существовать и злоумышленники, желающие этим воспользоваться. Со времени финансовой пирамиды, созданной Чарльзом Понци в 1919 году, прошло более 100 лет, но поведение людей не изменилось.

Вопрос не в том, насколько велика проблема мошенничества в сфере торговли на фондовых рынках. Убытки могут быть колоссальными, как в случае с Бернардом Мэдоффом (был обвинен в основании, возможно, крупнейшей в истории финансовой пирамиды – пострадало до 3 млн человек, а финансовые потери составили около $17,5 млрд), а могут быть и небольшими, если речь идет о мелких мошенниках, которые еще не успели развернуть свою деятельность.

Вопрос в том, что проблема мошенничества существовала, существует и будет существовать, пока есть спрос на легкий заработок.

Если мы говорим о профессиональных участниках рынка ценных бумаг, о компаниях, имеющих лицензию, о компаниях, регулируемых АРРФР, то проблемы мошенничества нет – работа ведется в строгом правовом поле. В этом сегменте рынка меры борьбы с мошенничеством со стороны участников рынка и государства очень эффективны.

Если мы говорим о нерегулируемом сегменте рынка, то бороться с мошенничеством крайне тяжело. Если сегодня закрыть одну подозрительную компанию без лицензии, завтра появится другая. Можно только повышать финансовую грамотность населения, что и делает регулятор и профессиональные участники рынка.

Мошенникам крайне сложно пройти процедуру KYC и стать клиентом компании. Наша компания уже отказывала в установлении деловых отношений, если имела основания полагать, что мы имеем дело с мошенниками. Обращения от клиентов по поводу мошеннических действий к нам не поступали.

Нам, как инвесторам, иногда приходят предложения инвестировать в различные проекты, инструменты с высокой доходностью. Как правило, мошенников достаточно легко вычислить. Я думаю, что многие получали «письма счастья» из африканских или других стран о том, что вам некто оставил несколько миллионов долларов в наследство. Мошенники, как правило, пишут с подозрительных электронных адресов, про их компанию ничего не известно (нет сайта и лицензий, нет информации на сайте регулятора той страны, откуда пишут, а сами проекты весьма туманные и непонятные). При этом всегда обещают баснословные доходы.

В целом мошенники наносят урон репутации всему рынку ценных бумаг. Бороться с этим можно, повышая финансовую грамотность населения.

Это очень важное направление, и потому наша компания запустила проект с одним из информационных порталов по публикации серии статей, направленных на объяснение принципов рынка ценных бумаг простым языком. Это наш вклад в повышение финансовой грамотности населения.

АО «Инвестиционный дом «Астана-Инвест»

Проблема мошенничества действительно становится заметной и с каждым годом набирает более высокие обороты. Это видно по реакции клиента на входящую информацию по предлагаемым с нашей стороны возможностям и погруженности самого клиента в то, как работают финансовые рынки.

Эффективность каждого участника сейчас разная, так как мы все работаем в одиночку и у каждого свои ограничения бюджета для борьбы с мошенничеством. При этом важным моментом и очень часто возникающим является проблема отсутствия комплексного подхода. Это как у аграриев – если твой сосед не обработает участок от вредителей, то эффективность твоей обработки со временем стремится к нулю.

Наша компания постоянно наблюдает неправомерные действия со стороны мошенников, направленные не только на наших клиентов, но и людей, которые проявили большую бдительность и обратились в наш call-центр для разъяснения какой-либо ситуации.

Сейчас очень часто мы слышим, что мошенники, используя бренд инвестиционного дома «Астана-Инвест», предлагают какие-то невероятно выгодные вложения, показывают нашу лицензию и представляются нашими сотрудниками. Целью этих действий является перечисление клиентом денег на телефон или карту, которые, как правило, находятся за пределами Казахстана. Причем клиент это должен сделать срочно, пока находится под влиянием полученной информации, и, как правило, без подписания договора или иного документа.

К сожалению, это нынешняя реальность и, возможно, не мы одни сталкиваемся сейчас с подменой фактов. Мошенничество на фондовых рынках значительно выросло в масштабах и с каждым разом становится более адаптированным под ситуацию. Этому очень сильно способствовали различные ограничения, карантины и переход множества операций в онлайн-режим.

2020 год был для нашей компании входом и периодом адаптации к новой реальности. Поэтому многие вопросы «решались с колес» – нужно было быстро перестроить бизнес, выстроить системы защиты и научиться работать дистанционно. Поэтому мы не наблюдали повышения активности мошенников, а новые виды обмана только зарождались.

Приростом мошеннических действий отмечен 2021 год. Например, только по call-центру нашей компании мы сейчас фиксируем до 10 обращений в месяц. Это высокая цифра, если смотреть конкретно по нашему случаю.

Одна из главных проблем в борьбе с мошенничеством – то, что компании занимаются этим в одиночестве. Но, как говорится, один в поле не воин. При этом, борьба эта всегда требует значительных финансовых ресурсов. Решить данную проблему вмиг невозможно, но стремится к этому всегда необходимо.

В этом плане очень радует подключение к решению вопросов мошенничества руководства страны. Так появляется шанс для реализации комплексных мер, что, в свою очередь, снизит масштабы пострадавших лиц. Проблемы уже вышли за рамки индивидуальный кейсов и начинают угрожать национальным интересам. Возможно, именно поэтому в последние годы мы часто слышим о необходимости усиливать профилактику правонарушений.

Манипуляция рынком используется мошенниками как фактор к действию и, если в моменте они попадают в сферу интересов клиента, то обман получается – цель мошенника выполнена, деньги отправлены, из документов на руках у клиента только вымышленное имя и перевод на реквизиты иностранного счета. Раньше очень часто диалог начинался с «А вы видели, как выросла цена биткоина…» или «Вы еще не зарабатываете на Forex-рынке…» Сейчас это уже отработанные фразы, и мошенники двигаются дальше.

Методы нашей борьбы во многом сводятся к обучению. Мы объясняем, что в основу работы на фондовом рынке нужно закладывать официальные взаимоотношения. Они основаны на наличии лицензии регулятора, обязательного договора и прозрачных данных всех сторон сделки.

Повышение финансовой грамотности населения – это очень важный фактор для снижения угроз мошенничества. Этот инструмент – один из немногих, который эффективно работает как общая стерилизация мошенничества. Часто люди пренебрегают элементарными средствами защиты, такими как проверка сайтов и отзывов, звонок на официальный номер, консультация у знакомого специалиста.

Фото: Depositphotos

Чем опасны манипуляции рынком для добросовестных инвесторов

Только за 2019 год зарубежные регуляторы наложили штрафов за манипулирование рынком ценных бумаг почти на $1,8 млрд

Манипуляции на фондовом рынке – явление не новое, ущерб от него исчисляется миллиардами долларов. По данным консалтинговой компании Deloitte, за 2019 год регуляторы наложили штрафы на сумму в $1,78 млрд по 160 инцидентам с манипуляциями в США, Великобритании, Австралии и странах Азии.

Сергей Лукьянов,
Председатель Правления
АО «Фридом Финанс»

Чем плохи манипуляции?

Всего с 2016-го по 2020 год в США штрафы за манипулирование на рынке ценных бумаг (РЦБ) составили $7,8 млрд, в Великобритании – $2 млрд, а в Китае – около $7,4 млрд. Также в топе Гонконг со $160 млн штрафов, Австралия – $101 млн и Канада с $70 млн.

Это показывает масштаб проблемы на развитых фондовых рынках. И несмотря на попытки лучше контролировать торговлю на РЦБ, сохраняется большое число попыток им манипулировать. В 2020 году пандемия создала больше возможностей для неправомерных действий и манипуляций из-за перехода на удаленную работу и высокой динамики на рынках (в связи с увеличением объемов торгов и сделок).

Манипуляции на рынке ценных бумаг наносят ущерб добросовестным инвесторам, поскольку необъективное установление или поддержание отдельными субъектами цен на ценные бумаги может подтолкнуть инвестора к совершению убыточных сделок – например, заставить вынужденно покупать по искусственно завышенным ценам либо продавать по заниженным.

Такие обстоятельства приводят к утрате доверия инвесторов к рынку ценных бумаг, а также неспособности регулятора, бирж своевременно выявлять и не допускать таких ситуаций.

Игроки наращивают цифровую безопасность

Еще один важный вопрос в борьбе с мошенничеством на фондовом рынке – это информационная безопасность. По мере внедрения цифровизации во все сферы нашей жизни растет и разновидность хакерских атак.

Теперь серьезные кибератаки могут быть выполнены злоумышленниками разного уровня подготовки – это работает как сервис. За небольшую сумму можно купить разные виды услуг взлома, которые предоставляются подготовленными хакерскими группировками.

Но в теории, даже если мошенники получат доступ к личному кабинету инвестора, продадут его бумаги, то все равно не смогут вывести эти средства на сторонний счет, так как вывод осуществляется только на счет инвестора.

В нашей компании, например, используется двухфакторная аутентификация, которую невозможно скомпрометировать. Логины и пароли у людей на разных ресурсах, как правило, одинаковые, поэтому, взломав один ресурс, можно получить доступ и к другим – в том числе и к инвестиционным счетам. В связи с этим компании дополнительно используют одноразовые пароли, которые действуют только 30 секунд и могут быть доставлены клиенту разными способами (обычно через SMS-сообщения), что снижает риски. Такую систему невозможно взломать.

Клиенты брокерских компаний должны помнить, что нельзя передавать логины и пароли третьим лицам, даже если они представляются сотрудниками вашего брокера – они никогда такую информацию не запрашивают. Если же мы выявляем факт передачи личных данных сторонним лицам, то немедленно блокируем счета клиента в целях его безопасности.

Определенного тренда в сфере информационной безопасности в брокерском бизнесе пока нет – атаки происходят по-разному, их число огромно. Поэтому игроки рынка делают упор на сферу информационной безопасности в целом, чтобы минимизировать риски по всем направлениям.

Фото: Depositphotos

Мошенничество на фондовом рынке. Как это работает?

Главным методом борьбы со злоумышленниками остается повышение финансовой грамотности населения

Рассказываем, как рынок борется с мошенничеством и почему в этом вопросе крайне важно повышать финансовую грамотность населения.

Юрий Масанов

Мошенничество в мире

Мошенничество на фондовом рынке существовало, возможно, с самого появления бирж. Один из ярких примеров – афера Бернарда Мэдоффа из США, в результате которой пострадало до 3 млн человек, а финансовые потери оцениваются примерно в $17,5 млрд. Компания Бернарда Мэдоффа проработала более 40 лет. Эта афера считается крупнейшей в истории.

Madoff Investment Securities считалась одним из самых надежных инвестфондов в Штатах, вклады приносили инвесторам около 12-13% годовых. В числе клиентов были банки, хедж-фонды и розничные инвесторы – к 2008 году, когда аферу раскрыли, у Madoff Investment Securities было $17 млрд. Оказалось, что компания в реальности не занималась инвестициями, а действовала по классической пирамидальной схеме Понци, расплачиваясь с инвесторами деньгами, которые приходили от новых клиентов.

Мошенничество на фондовых рынках продолжает существовать, даже несмотря на совершенствование регулирования со стороны госорганов и систем защиты профессиональных игроков. По данным консалтинговой компании Deloitte, только за 2019 год регуляторы в странах Северной Америки, Европе, Азии и Австралии наложили штрафы на сумму почти в $1,8 млрд по 160 инцидентам с манипуляциями на рынке ценных бумаг.

«В 2020 году тренд продолжился – пандемия дала возможность для правонарушений и манипуляций на фондовых рынках из-за перехода на удаленную работу и динамичные условия на рынках, связанные с увеличением объемов торгов и волатильностью», – пишут эксперты Deloitte.

В казахстанском законодательстве тоже прописаны уголовные статьи за мошеннические действия на фондовом рынке. Помимо самого мошенничества, есть и статьи за манипулирование рынком, под которым понимают действия для установления или поддержания цен на ценные бумаги выше или ниже рыночных.

Если манипулирование будет доказано, то физлицу грозит штраф в 200 МРП (это 583,4 тыс тенге в 2021-м). В случае с юридическими лицами штраф для малого бизнеса составляет 300 МРП (или 875,1 тыс тенге), среднего – 400 МРП (1,166 млн тенге) и крупного – 500 МРП (почти 1,5 млн тенге).

Для физлица штраф могут заменить на исправительные работы сроком до 200 часов либо арестом вплоть до 50 суток. Виновного также могут лишить права занимать определенные должности или работать в определенной сфере на срок до трех лет.

Уголовная ответственность может наступить, если манипулирование совершали неоднократно, если оно было совершено группой лиц и причинило ущерб свыше 58,3 млн тенге (на 2021 год). Здесь наказание растет до двух лет с конфискацией имущества и лишением права занимать определенные должности. Если суд признает обвиняемых преступной группой, то сроки растут до ограничения или лишения свободы до пяти лет. Такое же наказание можно получить и за незаконную инсайдерскую торговлю.

Мошенничество в Казахстане

В Казахстане фондовый рынок развит не так сильно, как за рубежом. Потому и случаев мошенничества выявляется немного. В основном они связаны с попытками украсть личные данные инвесторов и вывести деньги с их счетов либо с попытками сделать граждан клиентами «инвесткомпании» или «брокера» без лицензии для последующей кражи денег.

«Фондовый рынок ассоциируется у людей с быстрым и легким заработком – именно это эксплуатируют мошенники. Поскольку всегда есть люди, желающие получить много денег легко и быстро, всегда будут существовать и злоумышленники, желающие этим воспользоваться. Со времени финансовой пирамиды, созданной Чарльзом Понци в 1919 году, прошло более 100 лет, но поведение людей не изменилось», – говорят в компании Halyk Global Markets.

Убытки могут быть колоссальными, а могут быть и небольшими. «Вопрос в том, что проблема мошенничества существовала, существует и будет существовать, пока есть спрос на легкий заработок», – отметили в компании.

В АО «Фридом Финанс» также считают, что проблема мошенничества будет присутствовать на рынке всегда. Но в нынешних реалиях биржа и надзорный орган предпринимают действия для того, чтобы добросовестные участники не понесли экономического убытка.

«Выявляется не так много случаев мошенничества на фондовом рынке, но выявленные случаи являются довольно изощренными и оперируют огромными суммами», – рассказывают в компании.

В целом, подчеркивают во «Фридом Финанс», это «все безусловно рушит репутацию и доверие ко всему фондовому рынку». Также в компании отметили, что в последнее время злоумышленники обзванивают граждан и, представляясь сотрудниками известных брокерских компаний, предлагают установить на компьютер или мобильный телефон программу для удаленного управления устройством, маскируя это под демонстрационный продукт возможностей инвестирования.

На самом деле цель преступников – похитить пароли и деньги казахстанцев. Поэтому важно внимательно проверять корректность адресов посещаемых сайтов и не вводить на сомнительных страницах персональную информацию, данные карт, логины и пароли для входа в торговые платформы.

«Была информация от коллег из другой брокерской компании об активизации мошенников в интернете. В частности, в поисковых системах и мессенджерах распространялась контекстная реклама и осуществлялась рассылка с упоминанием брокерской компании, призывом участвовать в IPO и приобретать акции казахстанских и иностранных эмитентов», – говорят во «Фридом Финанс».

В дальнейшем получившие сообщения граждане переходили по ссылкам для ввода персональных данных и перевода денег, якобы в целях покупки ценных бумаг.

Также бывают случаи, когда из-за отсутствия ликвидности на рынке по многим инструментам крупному инвестору не составляет труда снизить цену. Для снижения подобных рисков для других участников торгов «Фридом Финанс» выступает маркет-мейкером по многим инструментам и в некоторых случаях становится им добровольно.

«Мы часто сталкиваемся с ситуацией, когда клиент хочет купить или продать по цене, значительно отличающейся от рыночной, в этих ситуациях мы не позволяем отправлять заявку на рынок и уведомляем клиента о том, что такая цена приведет к манипулированию. Мы каждый день усиливаем контрольные функции, чтобы наши клиенты не совершали манипуляций на рынке», – пояснили в компании.

В «Евразийском капитале» говорят, что до 2021 года не сталкивались со случаями мошенничества. Но в нынешнем году клиенты компании неоднократно сообщали, что им звонили, представляясь сотрудниками «Евразийского капитала» и предлагали вкладывать деньги под высокие проценты.

«После этого мы оповестили клиентов о возможных мошеннических действиях третьих лиц и проинструктировали, как отличить мошенников от наших настоящих сотрудников», – рассказали в компании.

Со схожей проблемой сталкиваются в «Инвестиционном доме «Астана-Инвест». Там объяснили, что часто слышат – мошенники, используя их бренд, предлагают «какие-то невероятно выгодные вложения», показывают лицензию компании и представляются ее сотрудниками.

«Целью этих действий является перечисление клиентом денег на телефон или карту, которые, как правило, находятся за пределами Казахстана. Причем клиент это должен сделать срочно, пока находится под влиянием полученной информации, и, как правило, без подписания договора или иного документа», – отметили в инвестдоме «Астана-Инвест».

Мошенничество на фондовых рынках, рассказал собеседник «Курсива», «значительно выросло в масштабах и с каждым разом становится более адаптированным под ситуацию». Этому, помимо прочего, помогли карантинные ограничения и переход множества операций в онлайн-режим.

Финграмотность – важный инструмент борьбы

Важным способом борьбы с мошенничеством остается повышение финансовой грамотности населения, считают опрошенные «Курсивом» участники рынка. Так, во «Фридом Финанс» говорят: профессиональные знания позволяют инвестору не быть вовлеченным в этот процесс и избежать совершения сделок, связанных с манипулированием на рынке ценных бумаг, а также сделок, совершаемых в результате манипулирования рынком в результате действий других субъектов.

В «Евразийском капитале» также отметили, что главная проблема в борьбе с мошенничеством – это недостаточная финансовая грамотность населения, чем и пользуются злоумышленники. Чтобы избежать обмана, говорят в компании, нужно помнить, что «гарантировать высокие прибыли на фондовом рынке не может никто, а любые предложения получить гарантированный доход определенный процент в месяц заведомо являются обманом».

В «Инвестиционном доме «Астана-Инвест» говорят, что повышение финграмотности – это важный фактор для снижения угроз мошенничества и один из немногих инструментов, который эффективно работает как общая стерилизация мошенничества.

В компании заявили, что поддерживают все инициативы Агентства по регулированию и развитию финансового рынка в этой сфере. Во исполнение поручений главы государства АРРФР разработало и утвердило «Концепцию повышения финансовой грамотности на 2020-2024 годы», которая разработана по рекомендациям ОЭСР. Эта работа, говорят в «Астана-Инвест», направлена на разъяснение возможностей рынка, ориентиров доходности, преимуществ и рисков и при этом всегда акцентирует внимание – любые отношения должны строиться на юридической основе.

Фото: Depositphotos

Фальсификация и манипуляция

Истории мошенников, которые находили лазейки даже в самых стабильных на первый взгляд системах


Фото: Depositphotos

Мошенничество появилось вместе с деньгами. Развитие фальшивомонетничества и изготовления поддельных бланков не отставало от развития системы наличного денежного обращения и документарных ценных бумаг. Искусно подделывая монеты, а потом и бумажные ассигнации, бланки векселей и других ценных бумаг, мошенники наносили колоссальный ущерб как государству, так и частным компаниям, рядовым гражданам. Рынки меняются – мошенники остаются. Рассказываем, как они работают на биржах.

Алимхан Адилов

Как обмануть рынок

Существует два основных способа обмануть рынок. Первый – фальсификация или манипуляция новостями. К примеру, можно вспомнить Twitter-аккаунт миллиардера Илона Маска, которого финрегулятор не раз упрекал в игре с фондовым рынком из-за постов о компании Tesla. Из-за этого в 2019 году Комиссия по ценным бумагам и биржам США (SEC) перечислила ряд тем, которые не должны освещаться Маском в социальных сетях или «иным образом сообщаться в письменной форме без предварительного согласия юриста Tesla».

Второй и самый распространенный способ – технические манипуляции. Они заставляют цены двигаться в нужную для манипулятора сторону и требуют хорошего знания технической стороны вопроса. Манипуляции обычно рассчитаны на краткосрочный эффект, поэтому страдают от них в основном краткосрочные инвесторы и дей-трейдеры (биржевые спекулянты, которые совершают сделки в пределах одного дня).

Кто обманывал рынок

В 2008 году французский трейдер Жером Кервьель чуть не уничтожил один из крупнейших банков Европы Societe Generale, нанеся ему фантастический ущерб в 5 млрд евро махинациями на рынке. Сам Кервель работал в бэк-офисе этого же банка, и почти всегда он был под контролем служб безопасности: у него и его коллег был лимит на сделки, открывать позиции можно было лишь с рабочих компьютеров, а все данные передавались контролерам в реальном времени. Но за пять лет работы в банке он смог изучить систему безопасности вдоль и поперек, а после разработал собственную схему. Действовала она следующим образом: Жером открывал превышающие лимит позиции на огромные суммы в расчете на рост или падение рынков, а перед проверками открывал фиктивные страховочные позиции, которые после закрывал. В свою очередь, люди, которые осуществляли контроль, не видели рискованных позиций. Также он фальсифицировал документооборот, пользуясь паролями бывших коллег. Кроме того, для фиктивных сделок он использовал счета клиентов Societe Generale. В итоге в 2008 году, когда мошенника раскрыли, выяснилось, что он открыл позиций на почти 50 млрд евро, при том, что рыночная капитализация Societe Generale тогда составляла всего 35 млрд евро. Банк решил закрывать позиции – на это ушло два дня, обернувшиеся убытком в 4,9 млрд евро.

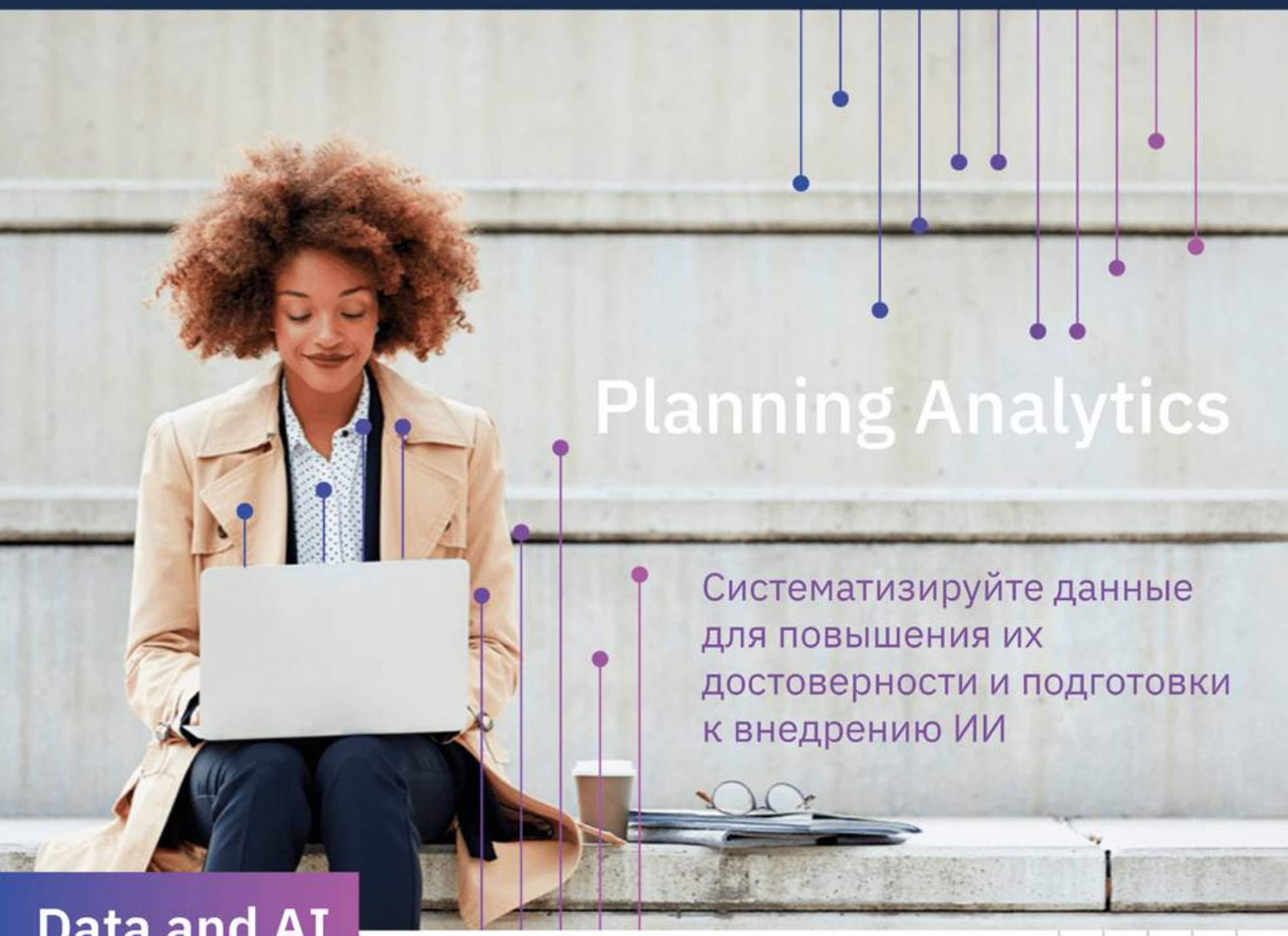
Но это не самый крупный ущерб для рынка. От мальчика-аутиста до угрозы мирового фондового рынка – именно так можно описать историю Навиндера Сингха Сарао. Торгуя на бирже, он использовал специальную программу для автоматического трейдинга, которая размещала тысячи заявок на крупные суммы, а затем сразу их отменяла. Такой метод торговли называется «спуфинг» (имитация заявки). Фальшивые ордеры сильно влияют на котировки: они создают ложное впечатление об уровне спроса и предложения. Трейдеры и алгоритмы фиксируют их и стремятся выставлять заявки на примерно том же уровне, что приводит к естественному росту или падению цен. С июня 2010 года спуфинг запрещен законодательством США.

Навиндер Сингх Сарао работал исключительно с контрактами E-mini S&P 500 – индекса, в корзину которого входят 500 публичных компаний США с наибольшей капитализацией. Предвидя реакцию трейдеров на его ложные заявки, он с помощью софта проводил сделки за миллисекунды и получал прибыль, когда котировки возвращались к естественному уровню. 6 мая 2010 года Сарао выставил на продажу одну из крупных заявок, которая вызвала кратковременное сумасшествие. Денежный объем заявок составил около $200 млн (20–29% от всех ордеров на тот момент), поставленных на скорое падение индекса. Это спровоцировало дисбаланс на рынке и привело к обвалу. Этот день назвали «черный четверг», индекс Dow Jones за пять минут рухнул на 600 пунктов.

Мошенничество на фондовых рынках совершенствуется в ногу с развитием самих рынков. В последние пару лет в Казахстане наблюдается биржевой бум: ежемесячно на фондовый рынок приходят тысячи новичков. При этом многие не до конца понимают, как все устроено изнутри. Такие люди становятся добычей разного рода проходимцев – от «экспертов» с платными курсами до аферистов, которые сливают в офшоры миллионы тенге. Наиболее эффективным способом защитить себя является повышение собственной финансовой грамотности. Именно осведомленность о принципах работы того или иного финансового инструмента, четкое представление о собственных правах и обязанностях позволяет отличить добросовестного участника рынка от мошенника и сохранить деньги.

DIGITALISM

Platinum Business Partner IBM



Planning Analytics

Систематизируйте данные для повышения их достоверности и подготовки к внедрению ИИ

Data and AI

Решение для координации действий пользователей, процессов и технологий с целью предоставления проверенных, готовых к использованию данных субъектам, операционным подразделениям и приложениям на всех этапах жизненного цикла данных.

Правильное управление данными позволяет организациям соблюдать сложные нормативные правила и требования, а также обеспечивать конфиденциальность данных и точность модели искусственного интеллекта (ИИ) благодаря контролю качества данных.

+7 (727) 327-47-00 | info@digitalism.kz | digitalism.kz