Proceedings of IYSC, (2021), vol. 10

Journal homepage: http://journals.sdu.edu.kz/index.php/iysw

2021 International Young Scholars' Conference

ПРАВОВЫЕ ПРОБЛЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТ-БАНКИНГА

Елубаева Шынар Арыстанбековна
магистрант 1-го курса Университета имени Сулеймана Демиреля, email: shynare@rambler.ru

Бимбетов Асхат Болатбекович
доктор PhD, адвокат

Аннотация

В настоящей работе исследуются вопросы правового регулирования защиты персональных данных при использовании интернет-банкинга. Авторами проанализированы как законодательные, так и подзаконные акты в этой сфере, в том числе закон РК «О персональных данных и их защите». В работе раскрыта правовая сущность персональных данных, в том числе и перечень информации, составляющие персональные данные согласно законодательству Республики Казахстан и исследованиям отечественных и зарубежных ученых.

Также проведен анализ правовых способов защиты персональных данных при пользовании гражданами отечественным интернет-банкингом. В заключении авторы предложили ряд мероприятий, связанных с совершенствованием законодательства Республики Казахстан в сфере защиты персональных данных.

Ключевые слова: персональные данные, защита персональных данных, банк, интернет-банкинг, информационная безопасность.

Введение

На сегодняшний день невозможно представить сферу оказания банковских услуг без интернет-банкинга. Ежедневно огромное количество персональных данных граждан передаётся на хранение в различные информационные системы, включая интернет-банкинг.

Информационная безопасность – сложно оцениваемая вещь, в связи с этим мы не имеем ни технической, ни физической возможности определить надежность системы, пока кто-то ее не взломает. До этого времени нам не будет известно, надёжно ли защищён объект, и эффективна ли была работа уполномоченныхгосударственных органов.

Согласно исследованиям Центра анализа и расследования кибератак (далее – ЦАРКА), проведенного 28.02.2020 года, в рамках подготовки к SFO Sammit Kazakhstan,многие банки пренебрегают даже самыми распространенными и простыми в реализации советами по повышению безопасности своих веб-ресурсов. ЦАРКА отмечает, что во всех 26 банках Казахстана (на сегодняшний день 25 банков), выявлены проблемы GDPR [1, с. 19].

При изучении утечек информации ограниченного доступа в Республике Казахстан, проведенному Экспертно-аналитическим центром InfoWatch, за период 2018 - 2020 годы «зафиксировано 24 случая утечки данных из компаний и государственных органов Казахстана, опубликованных на русском языке. Всего были скомпрометированы более 11 млн. записей персональных данных и платежной информации. Более 91% утечек связано с компрометацией персональных данных». В исследовании Центра отмечаются факты, что «в результате атаки на сайт «Народного банка Казахстана» пострадали как минимум 210 клиентов». По отраслевому распределению утечек на банки и финансы приходится 12,5% всех утечек. Центр также

сообщает, что «инциденты в Республике Казахстан обладают высокой латентностью», что означает, что утечек фактически гораздо больше [2, с. 3].

При таких обстоятельствах возникают такие вопросы, как: каким образом осуществляется правовое регулирование защиты персональных данных в Казахстане; каковы правовые способы защиты персональных данных в интернет-банкинге; и какие правовые способы совершенствования норм по защите персональных данных в интернет-банкинге на сегодняшний день можно предложить.

В связи с этим, полагаем, что данная тема достаточно актуальна и требует дальнейших исследований.

1. Правовое регулирование защиты персональных данных при использовании интернет-банкинга в Республике Казахстан

Нормативная правовая база, регулирующая вопросы персональных данных при использовании интернет-банкинга представлена как общими нормами гражданского законодательства, так и специальными нормами банковского законодательства, в том числе содержащимися в подзаконных нормативных правовых актах.

Общими нормативными правовыми актами в области персональных данных являются: Конституция РК от 30.08.1995г.(статья 18); Гражданский кодекс РК (Общая часть) от 27.12.1994г. (статьи 16,115,141,144); Гражданский кодекс РК от 01.07.1999г. (Особенная часть) (статья 830); Предпринимательский кодекс РК от 29.10.2015г. (статья 111); Трудовой кодекс РК от 23.11.2015г. (статьи 16,22,23); Кодекс РК «О здоровье и системе здравоохранения» от 07.07.2020г. (статьи 57,58,60); Кодекс РК об административных правонарушениях от 05.07.2014г. (статьи 15,16,21,79,186);Уголовный кодекс РК от 03.07.2014г. (статья 147,211), Закон РК «О персональных данных и их защите» от 21.05.2013г.; Закон РК «Об информатизации»от 24.11.2015г. (статьи 6,7,14,17,18,36,56);

С целью реализации закона РК «О персональных данных и их защите» (далее – Закон о ПД), в Казахстане разработаны и действуют следующие подзаконные нормативные правовые акты:

- Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденные постановлением Правительства РК от 03.09.2013 г. № 909;

- Правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач, утвержденные постановлением Правительства РК от 12.11.2013 г. № 1214;

- Правила сбора, обработки персональных данных, утвержденные Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 21.10.2020 г. № 395/ НҚ.

Правовая защита персональных данных в банковской сфере, прежде всего, обеспечивается Законом о ПД.

К персональным данным согласно п.2 ст.1 Закона о ПД относятся «сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе» [3].

То есть, действие Закона о ПД напрямую распространяется на банки, предоставляющие услуги интернет-банкинга. При этом согласно ст.23 Закона «особенности защиты электронных информационных ресурсов, содержащих персональные данные, устанавливаются в соответствии с Законом РК «Об информатизации» [3].

Говоря о персональных данных при использовании интернет-банкинга не стоит путать понятия «персональные данные» и «банковская тайна». К банковской тайне

относятся«сведения о клиентах и корреспондентах банков, их операциях и взаимоотношениях с банками, связанных с получением банковских услуг, в том числе без ограничения: информацию о наличии, владельцах и номерах банковских счетов и корреспондентов банков, остатках и движении денег на этих счетах и счетах самого банка, ограничениях на перечисленных счетах и т.д.» (статья 50 Закона РК «Обанках и банковской деятельности») [4].

К персональным данным, приравниваются сведения, относящиеся к определенному субъекту, которые зафиксированы на электронном, бумажном или ином материальном носителе. В основном биометрические данные - ФИО, рост, вес, цвет зрачков, отпечатки пальцев и так далее.

В части защиты персональных данных в системах интернет-банкинга при осуществлении платежных операций интерес представляет п.14 ст. 13 Закона РК «О платежах и платежных системах», согласно которой «поставщик платежных услуг при оказании платежных услуг осуществляет сбор и обработку персональных данных с согласия субъекта персональных данных» и «обеспечивает конфиденциальность сведений, полученных при оказании платежных услуг, и не допускает их раскрытия третьим лицам, за исключением случаев, предусмотренных законами РК» [5].

К числу подзаконных актов, регулирующих вопросы защиты персональных данных при использовании интернет-банкинга, относятся Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденныеПостановлением Правления Национального Банка РК от 31.08.2016 г. № 212.

В этих Правилах персональные данные упоминаются только в п. 22-3, согласно которому банк проводит сеанс видеоконференции с клиентом «на основании

полученного согласия клиента на сбор, обработку,хранение и представление, в том числе при необходимости третьим лицам, его персональных данных, подтвержденного посредством идентификационного средства» [6].

Но п.24данных Правил устанавливает меры безопасности, которые обеспечивают:

«1) достоверную идентификацию клиента и его право на получение соответствующих электронных банковских услуг;

2) выявление наличия искажений и (или) изменений в содержании электронных документов, на основании которых клиенту предоставляются электронные банковские услуги;

3) защиту от несанкционированного доступа к информации, составляющей банковскую тайну, и целостность данной информации» [6].

Также банки второго уровня в соответствии с постановлением Национального банка РК от 29.02.2016 г. №66 «Об установлении перечня основных документов, подлежащих хранению, и сроках их хранения в банках второго уровня» должны хранить документы, содержащие информацию о вкладчиках, заемщиках, а также отклоненные банком заявкиграждан на получение займов в установленные этим постановлением сроки [7].

Таким образом, следует заключить, что в системе законодательства Республики Казахстан сформирован достаточно прочный правовой «фундамент» законов и подзаконных актов, направленных на регулирование защиты персональных данных при использовании интернет-банкинга в Республике Казахстан.

2. Правовые способы защиты персональных данных в интернет-банкинге

Хищение персональных данных клиентов, помимо причиненного клиентам вреда, негативно отражается на репутации банка. Одна из наиболее острых проблем интернет-банкинга касается вопросов безопасности систем интернет-банкинга.

Так, в 2017 году информационно-аналитический портал Informburo.kz сообщил, что «Государственная техническая служба Министерства информации и коммуникаций РК разослала в казахстанские банки предупреждение о вредоносном программном обеспечении, при помощи которого злоумышленники похищают персональные данные клиентов, использующих интернет-банкинг». Злоумышленники получали логины и пароли клиентов при их переходе по ссылкам на вредоносные прокси-сервера [8].

Согласно опубликованной информации от МВД РК 15 февраля 2021 года более 10 процентов всех преступлений связаны с мошенничеством. При этом, отмечается рост мошенничества в интернете: в 2020 году было зарегистрировано более 14 000 дел об интернет-мошенничестве, из них:

- 3000 фактов мошенничества связаны с хищением персональных данных граждан с последующим оформлением на них онлайн-займов;

- более 2 000 фактов мошенничества «совершены путем завладения персональными данными и реквизитами карточных счетов граждан с хищением денег через мобильный банкинг» [9].

Такая ситуация заставляет задуматься о том, какие правовые способы защиты персональных данных в интернет-банкинге существуют на сегодняшний день.

Под способами защиты гражданских прав обычно понимаются предусмотренные законодательством меры, с помощью которых можно предотвратить, устранитьнарушения прав, а также восстановить или компенсировать убытки, возникшие в результате нарушения прав.

Как отмечает Козлов С.В., риски интернет-банкинга в отношении персональных данных клиентов могут быть внутренними и внешними, а также пассивными и активными [10].

Внутренние риски возникают, когда работники банков используют в корыстных целях сведения, к которым они имеют доступ в силу выполнения должностных обязанностей, тогда как внешние риски связаны с действиями третьих лиц, как в случае упомянутых выше атак на сайт Народного банка Казахстана [10].

Пассивные риски предполагают принятие банком предусмотренных мер по защите персональных данных, и несанкционированный доступ происходит по вине клиентов. Активные риски, соответственно, связаны с тем, что банк принял недостаточно мер по защите персональных данных, не выполняет их, что приводит к возникновению негативных последствий для клиентов [10].

Правовые способы, предусмотренные нормативными правовыми актами, могут уменьшить или предотвратить внешние, внутренние и активные риски, так как устанавливают определенные требования по информационной безопасности, обязательные для соблюдения банками, а также соответствующую ответственность за их нарушение. Так, ст.55 Закона РК «Об информатизации устанавливает правовые, организационные и технические меры защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры [11].

В соответствии с Законом о ПД требования по обеспечению защиты персональных данных возлагается на собственника и/или оператора базы, содержащей персональные

данные. К понятию «оператор» исходя из данного Закона о ПД будет соответствовать каждый субъект предпринимательства (в данном случае – банк), который имеет в штате работников либо оказывает услуги населению, поскольку в процессе своей деятельности он так или иначе осуществляет сбор и обработку личной информации физических лиц.

В определенной мере можно согласиться с мнением, что законодатель не определяет перечень конкретных мер, а лишь устанавливает цели защиты (к примеру, соблюдение конфиденциальности, предотвращение законного сбора и обработки персональных данных) и общие требования к результату (например, минимизация негативных последствий несанкционированного доступа) [12].

Вместе с тем, считаем, что в условиях быстро развивающихся информационных технологий определение перечня конкретных мер, действий по защите персональных данных в информационных системах не представляется возможным, либо данный перечень будет регулярно устаревать и терять свою актуальность.

Следует отметить, что немаловажное внимание уделяется созданию внутренних документов по защите персональных данных. В частности, в банке должны быть утверждены Политика информационной безопасности, перечень защищаемой информации, включающий, в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, порядок работы с защищаемой информацией, создание бизнес-процессов и др.

Если исходить из норм Правил оценки уровня защищенности от угроз информационной безопасности, утвержденных Постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2020 г. № 110, в финансовой организации должно быть разработано порядка 22 внутренних документов, наличие которых будет свидетельствовать о соответствии третьему (наивысшему) уровню защищенности от угроз информационной безопасности.

В перечень таких документов входит Политика информационной безопасности; документ, определяющий меры информационной безопасности при предоставлении клиентам доступа к информационным системам финансовой организации; документ, содержащий правила использования электронной почты и использования сети Интернет; документ, содержащий правила управления паролями пользователей в ключевых информационных системах и многие другие [13].

Правила № 909 предусматривают в отношении персональных данных ограниченного доступа, в числе прочих, необходимость шифрования либо наличие защищенных каналов для передачи данных иным лицам; хранение данных с применением средств криптографической защиты информации; применения средств идентификации и (или) аутентификации пользователей при работе с этими данными [14].

Как отмечают Коломойцева А.И., Газизов А.Р. [15] «в банках чаще всего используются следующие виды аутентификации:

1) проверка личности по постоянному логину и паролю (введенные пользователем данные тщательно проверяются и в случае правильности ввода, осуществляется доступ в систему).

2) проверка личности по одноразовому паролю (каждый новый пароль передается по запросу клиента путем СМС - уведомлений).

3) идентификация личности по специальному техническому или электронному устройству USB - токен (это может быть мобильный телефон, смарт - карта, брелок, часы, ключи и т.д.).

4) идентификация по биометрическим данным личности (проверка происходит по отпечатку пальца, по голосу, по сканированию сетчатки глаза, по сканированию кровеносной системы и т.п.)» [15].

Указанные способы идентификации используются как по отдельности, так и в определенных сочетаниях.

В качестве дополнительных мер защиты пользователя также используются такие меры, как:

1) ограничение срока действия пароля. Задается максимальный срок действия пароля, по истечении которого пользователю необходимо получить новый пароль.

2) ограничение числа попыток входа в систему. Используется временное или постоянное блокирование возможности входа в интернет - банк в случае исчерпания допустимого количества неверного ввода логина/пароля. Например, банк установил ограничение на три попытки неверного ввода логина/пароля. После их исчерпания возможность входа пользователя в интернет - банк блокируется. При первом исчерпании доступ может блокироваться временно (например, на 40 мин.). После второго исчерпания трех попыток доступ блокируется на постоянной основе, и для его возобновления пользователю потребуется обратиться в банк с документом, удостоверяющим личность.

3) принудительный выход из системы при бездействии клиента в течение определенного времени. Например, может быть установлен порог бездействия в течение 15 мин. По истечении данного периода времени система может запросить клиента, желает ли он продолжить сеанс работы, или просто по умолчанию завершить сеанс работы с просьбой снова аутентифицироваться для входа в интернет - банк.

4) направление уведомления клиенту (по электронной почте или в виде SMS - сообщения на мобильный телефон) при входе в мобильный или интернет - банк. После

прохождения аутентификации клиента направляется уведомление, содержащее информацию об успешном входе в систему с указанием IP - адреса устройства, через которое осуществлен вход. В случае использования мобильного устройства в сообщении может быть просто отражен канал входа - SMS, WAP и т.д.» [15].

Тем самым банки проводят определенную работу по защите и обеспечению информационной безопасности. При этом также используют различные технические средства защиты, для исключения риска мошенничества, как 3DSecure –процедура, позволяющая дополнительно обезопасить платежные операции через интернет-банкинг. Как правило, банки применяют эту технологию путем установления дополнительного постоянного пароля либо одноразового пароля, высылаемого клиенту на номер мобильного телефона для возможности оплаты товаров и услуг в интернете.

В этой связи, несмотря на то, что в настоящее время на уровне законодательства предусмотрены меры по защите персональных данных при использовании интернет-банкинга, клиенты банков также должны осознавать необходимость принятия личных мер по сохранению своих персональных данных, включая логины, идентификаторы и пароли для входа в интернет-банкинг во избежание несанкционированного доступа в системы интернет-банкинга.

3. Правовые вопросы совершенствования норм по защите персональных данных в интернет-банкинге

Возрастающая угроза атак на персональные данные с развитием цифровых технологийможет вызвать проблемы, с точки зрения, обеспечения защиты прав граждан.

В частности:

1) банки обязаны обеспечивать «надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение» [16]. Тем не менее, очевидно, что обеспечение безопасности в сфере интернет-банкинга недостаточно,

поскольку банки часто подвергаются кибератакам. Необходимо вводить и развивать новые превентивные меры, закрепленные на законодательном уровне, и все это должно осуществляться в рамках государственногорегулирования банковского сектора.

2) полностью согласны с мнением, что одной из главных уязвимостей банков являются люди: это и клиенты банков (к примеру: переходят по неизвестным ссылкам, предоставляют свои данные псевдоработникам банка, устанавливают приложения из непроверенных источников и т.д.), и сотрудники банков, которые могут продатьперсональные данные либо сами похитить деньги со счетов клиентов [17].

В этой части необходима работа банка в двух направлениях:

- усиленный контроль банка за работниками, их постоянное обучение и регулярное предупреждение об ответственности, вплоть до уголовной;

- регулярное информирование клиентов о необходимости самозащиты персональных данных, учитывая низкий уровень финансовой и информационной грамотности граждан, а также постоянное совершенствование мошеннических методов социальной инженерии.

3) в России одной из мер по совершенствованию законодательства было предложено - введение обязательного для банков страхования от взлома банковских интернет-приложений (интернет-сайтов). Суть предложения состоит в том, что необходимо обязать банки осуществлять страхование на случай убытков, понесенных в результате взлома их интернет-приложений [18]. Почему бы этот вариант не рассмотреть и в Казахстане, взвесив все «за» и «против».

4) в основополагающем законе банковского сектора – «О банках и банковской деятельности в Республике Казахстан» – не содержится норм о дистанционном банковском обслуживании или об интернет-банкинге.

Было бы вполне уместно данный закон дополнить статьей «Дистанционное банковское обслуживание», где закрепить особенности дистанционного банковского обслуживания, меры по обеспечению информационной безопасности при оказании услугв интернет-банкинге.

5) Правила № 110 [13] предполагают самостоятельное проведение финансовой организацией оценки уровня защищенности от угроз информационной безопасности по запросу регулятора. Регулятор данным актом, можно сказать, отстранился от собственного проведения оценки состояния информационной безопасности в банке.

В этой части, на наш взгляд, требуется внесение изменений в законодательство, предусматривающее оценку защищенности от угроз информационной безопасности самим регулятором на определенные случаи, к примеру, на случай рассмотрения исков, связанных с утечкой персональных данных.

Заключение регулятора о состоянии информационной безопасности в банке позволило бы судам в полном объеме и объективно рассмотреть вопрос, только ли по вине клиента произошла утечка персональных данных и наступили негативные последствия, либо есть вина банка в ненадлежащем обеспечении информационной безопасности, который с помощью договорных положений, как правило, исключает свою ответственность за утечки персональных данных.

Заключение

Таким образом, на сегодняшний день нормы, регулирующие в Казахстане дистанционные банковские технологии, представлены в нормативных правовых актах различного уровня. Нормативная правовая база, регулирующая вопросы интернет-банкинга представлена как общими нормами гражданского и банковского законодательства, так и специальными нормами, содержащимися в подзаконных нормативных правовых актах.

Подводя итог, следует еще раз обратить внимание на необходимость совершенствования и развития законодательства в части регулирования интернет-банкинга, закрепления основных принципов предоставления услуг и мер по обеспечению информационной безопасности, в том числе защите персональных данных при оказании услуг интернет-банкинга.

Список использованной литературы

1. Центр анализа и расследования кибератак [Электронный ресурс] / ЦАРКА составил рейтинг сайтов банков Казахстана по уровню веб-безопасности: 2020. — Режим доступа: http://wtotem.com/files/reports/kz_banks2020.pdf/стр. 23

2. Экспертно-аналитический центр группы компаний InfoWatch [Электронный ресурс/ Исследование утечек информации ограниченного доступа в Республике Казахстан (2018-2020): 2020. —Режим доступа**:** http:// www.infowatch.ru / стр. 23**.**

3. Закон РК «О персональных данных и их защите»

4. Закон РК «О банках и банковской деятельности»

5. Закон РК «О платежах и платежных системах»

6. Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденные Постановлением Правления Национального Банка РК от 31.08.2016 г. № 212

7. Постановление Правления Национального Банка Республики Казахстан от 29.02.2016 г. № 66 «Об установлении Перечня основных документов, подлежащих хранению, и сроков их хранения в банках второго уровня»

8. Казахстанцев, использующих интернет-банкинг, предупреждают о кражах персональных данных | informburo.kz

9. На казахстанцев оформляли кредит по найденным документам – МВД | LS (lsm.kz)

10. Козлов С.В. Некоторые аспекты правового регулирования дистанционного банковского обслуживанияИсточник: Банковское право. www.sksconfidence.com № 3. 2014. С. 57-65

11. Закон РК «Об информатизации»

12. ТОП - 5 вопросов по защите персональных данных Режим доступа:

ТОП - 5 вопросов по защите персональных данных Персональные данные | Pravosite.kz

13. Правила оценки уровня защищенности от угроз информационной безопасности, утвержденные Постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2020 г. № 110

14.Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденные постановлением Правительства РК от 03.09.2013 г. № 909

15. Коломойцева А.Н., Газизов А.Р. Применение идентификации и аутентификации при защите персональных данных клиентов коммерческого банка: «Чистая наука» на службе научно - технического прогресса: Сборник статей Международной научно - практической конференции 23 декабря 2017 г. / отв. ред. Сукиасян А.А. — Уфа: ОМЕГА САЙНС,2017. — 129 с.

16. Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, утвержденные Постановлением Правления Национального Банка РК от 27.03.2018 г. № 48.

17. Насколько безопасен интернет-банкинг? (klerk.ru)

18. Правовое поле интернет-банкинга::Журнал СА 9.2017 (samag.ru)