Министерство образования и науки Республики Казахстан

Университет имени Сулеймана Демиреля

Елубаева Ш.А.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТ-БАНКИНГА

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Специальность 7М04202– «Право информационных технологий»

Каскелен, 2022

Министерство образования и науки Республики Казахстан

Университет имени Сулеймана Демиреля

Кафедра Право

«Допущена к защите»
Директор магистерских программ
Факультета «Права и социальных наук»,
Орынбасаров Д.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема: «Правовое регулирование интернет-банкинга»

по специальности 7М04202– «Право информационных технологий»

Выполнил: Елубаева Ш.А.

Научный руководитель
к.ю.н., ассоциированный профессор: Омарова А.

Каскелен, 2022

КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК

выполнения и представления магистерской диссертации на тему **«Правовое регулирование интернет-банкинга»**

магистранта 2 курса Елубаева Шынар

7М04202– «Право информационных технологий»

№	Наименование разделов	Сроки предоставления руководителю	Отметка о выполнении	Подпись научного руководителя
1	Выбор и утверждение темы магистерской диссертации. Назначение научного руководителя.	*(Выберите дату между 01.10.2021-15.10.2021)*	✓	
2	Получение и разработка задания на выполнение магистерской диссертации	*(Выберите дату между 01.11.2021-15.11.2021)*	✓	
3	Подбор теоретического материала и представление руководителю	*(Выберите дату между 15.11.2021-30.11.2021)*	✓	
4	Подбор практического материала, систематизация теоретического и практического материала и представление руководителю	*(Выберите дату между 13.12.2021-17.1.2022)*	✓	
5	Написание 1 главы магистерской диссертации/проекта	*(пример. 18.01.2022-4.03.2022)*	✓	
6	Написание 2 главы магистерской диссертации/проекта	*(прим. 5.03.2022-.19.05.2022)*	✓	
7	Написание 3 главы магистерской диссертации/проекта (при ее наличии)	*(прим. 1.09.2022-.14.11.2022)*	✓	
8	Оформление магистерской диссертации/проекта	*(прим. 28.11.2022)*	✓	
9	Направление магистерской диссертации на проверку на предмет наличия или отсутствия плагиата	*(прим. 03.04.2023)*	✓	

10	Направление магистерской диссертации нормоконтролеру	*(прим. 10.04.2023)*	✓	
11	Направление магистерской диссертации/проекта научному руководителю для написания отзыва	*(прим. 29.04.2023)*	✓	
12	Процедура предварительной защиты магистерской диссертации/проекта	*(прим. 02.05.2023)*	✓	
13	Направление магистерской диссертации/проекта на рецензию	*(прим. 22.05.2023)*	✓	
14	Направление магистерской диссертации/проекта с отзывом и рецензией в ГАК	*(прим. 01.06.2023)*	✓	
15	Защита магистерской диссертации/проекта	*(прим. 19.06.2023)*	✓	

Дата выдачи задания «30» 11 2022 г.

Директор магистратуры Орынбасаров Д. _____
подпись

Научный руководитель Омарова А _____
ФИО подпись

Задание принял к исполнению

Магистрант(ка) Елубаева Ш _____
ФИО подпись

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы. Информационно – коммуникативные технологии все больше проникают в обычную жизнь людей и влияют на финансовую индустрию, внедряя новые методы, способы их распространения и новых игроков на рынке. Развитие информационно-коммуникационных технологий на финансовом рынке, а также активное оказание электронных финансовых услуг повышают риски нарушения конфиденциальности, сохранения доступности и целостности, что требует разработки и совершенствования требований к оказанию дистанционных и цифровых финансовых услуг.

Как указывается в Концепции повышения финансовой грамотности на 2020 – 2024 годы [1], по данным Всемирного Банка около 54% потребителей пользуются онлайн/дистанционными каналами для покупки финансовых продуктов и получения услуг.

Концепцией приводятся следующие тенденции в сфере электронных финансовых услуг:

1) мобильным банкингом пользуются 30-50% клиентов банков;

2) увеличение сотрудничества с финтех-компаниями ожидают 82% финансовых организаций;

3) при разработке стратегий 56% финансовых организаций предусмотрели цифровизацию технологий;

4) тенденция роста инвестиций в финтех-индустрию;

5) активное распространение данных с помощью технологий больших данных, а также электронных, мобильных приложений [1].

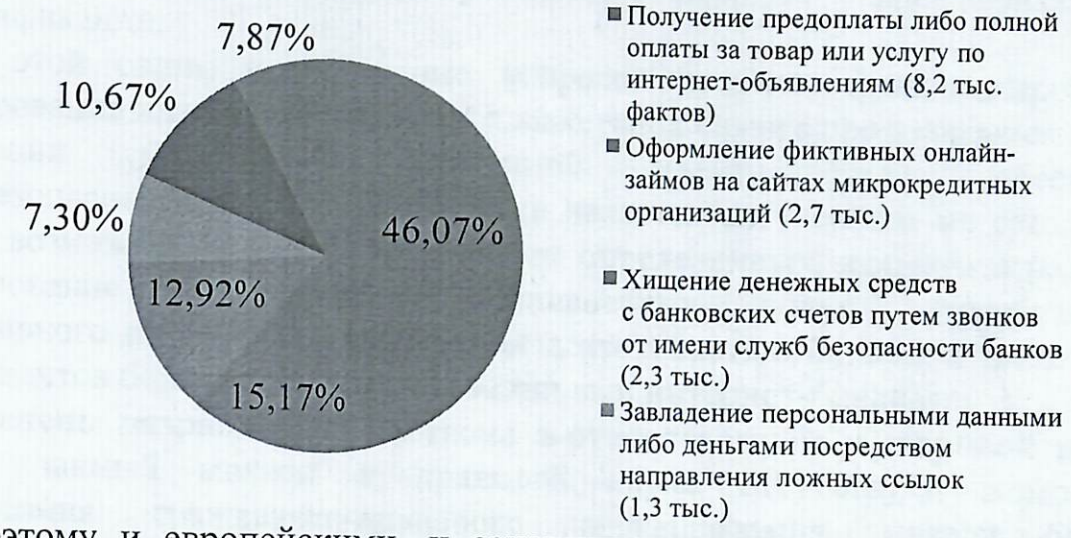
С развитием цифровизации повышается доступность финансовых услуг, качество и скорость обслуживания потребителей финансовых услуг, но вместе с тем возрастают и риски. Недостаточная финансовая и цифровая грамотность потребителей финансовых услуг, небрежное отношение к защите своих персональных данных приводят не только к нарушению их конфиденциальности, но и к серьезным финансовым потерям.

Так, согласно информации, указанной в Стратегии кибербезопасности финансового сектора РК на 2020-2022 годы, преступники ежемесячно проводят более 5000 попыток транзакций, и в качестве основных каналов хищения денег с банковских счетов названы банкоматы, мобильный и интернет-банкинг[2].

Кражи данных потребителей финансовых услуг или получение несанкционированного доступа к их личным кабинетам в интернет-банкингедля похищения средств, кража конфиденциальных сведений, умышленное повреждение информационных систем или коммуникационных средств не являются исчерпывающим перечнем угроз, связанных с развитием преступности в цифровом пространстве [2].

Согласно статистическим сведениям за 10месяцев 2021 года в Казахстане зарегистрировано 17,8 тыс. фактов интернет-мошенничества, из них способы мошенничества в процентном соотношении распределены следующим образом [3]:

Распространенные способы кибермошенничества



Поэтому и европейскими, и азиатскими исследователями поднимаются вопросы о необходимости жесткого законодательного регулирования интернет - банкинга в связи с потенциальными опасностями использования финтех-технологий.

К сожалению, несмотря на то, что Агентство РК по регулированию и развитию финансового рынка в соответствии с законодательством получает информацию об инцидентах информационной безопасности от банков и организаций, осуществляющих отдельные виды банковских операций, оно не публикует статистическую и аналитическую информацию о количестве фактов несанкционированного доступа в информационные системы, в том числе в системы интернет-банкинга.

Для сравнения: Банк России, регулирующий российский финансовый рынок размещает на своем интернет-ресурсе различные обзоры, связанные с несанкционированными платежами, кибертаками, инцидентами информационной безопасности. Так, согласно последнему опубликованному обзору объем операций без согласия клиентов в III квартале 2021 года по сравнению с III кварталом 2020 года возрос с 182 954 операций до 256 198 операций, а доля социальной инженерии (психологических методов воздействия на человека, направленных на получение конфиденциальной информация для доступа,к примеру, к системам банковского обслуживания)в дистанционном банковском обслуживании физических лиц с 31298 фактов до 52 081 фактов [4].

В качестве прогнозов на 2022 год исследователи предупреждают, что преступники продолжат развивать вредоносные программы, заражающие устройства пользователей онлайн-банкинга с обходом средств многофакторной аутентификации, а также методы социальной инженерии [5].

В целом государство осознает важность решения данных проблем и планирует усиливать требования к порядку оказания дистанционных и цифровых финансовых услуг, расширять перечень финансовых операций, доступных в цифровом формате, а также принимать меры по повышению

информационной безопасности. Для этого принимаются меры по разработке инновационных решений при получении финансовых услуг с применением удаленного доступа, биометрических методов идентификации и аутентификации.

В этой связи, исследование вопросов проблем функционирования и регулирования интернет-банкинга в Казахстане в связи с продолжением работ по реализации механизмов удаленной идентификации, обеспечению кибербезопасности финансового рынка является актуальным на сегодняшний день и возможно, данная работа станет определенным вкладом в развитие и регулирование дистанционных финансовых услуг, способствующим эффективного надзору за электронной деятельностью банков, а также защите прав клиентов банков при использовании ими интернет-банкинга.

Степень разработанности темы в отечественной и мировой науке

На данный момент в правовой науке отсутствуют комплексные исследования гражданско-правового регулирования интернет-банкинга. Отдельные вопросы интернет-банкинга как разновидности дистанционного банковского обслуживания исследованы российским автором Шахбазян М.Г. в диссертационной работе «Гражданско-правовое регулирование интернет-платежей в Российской Федерации».

В российской юриспруденции отдельные вопросы регулирования интернет-банкинга можно найти в работах по интернет-платежам и изучении зарубежного опыта правового регулирования платежных услуг, к примеру, в книге «Зарубежное банковское право (банковское право Европейского союза, Франции, Швейцарии, Германии, США, КНР, Великобритании)».

Вопросы информационной и договорной диспропорции потребителей финансовых услуг освещены в работе коллектива авторов «Защита прав потребителей финансовых услуг».

Совершенно отсутствуют исследования природы договора на оказание электронных банковских услуг, его доктринальных особенностей.

Также отсутствуют точечные юридические исследования по вопросам защиты прав клиентов интернет-банкинга в связи с повышенными рисками в части информационной безопасности и защиты персональных данных.

Таким образом, в результате анализа источников можно констатировать отсутствие в настоящее время отечественных и зарубежных исследований, посвященные интернет-банкингу, в том числе с точки зрения защиты прав клиентов интернет-банкинга.

Соответственно, в работе рассматриваются гражданско-правовые вопросы, направленные на совершенствование правового регулирования интернет-банкинга с акцентом на требования информационной безопасности и защиты персональных данных с учетом судебной практики и зарубежного опыта.

Объектом исследования являются общественные отношения, складывающихся в процессе нормативного регулирования интернет-банкинга в Казахстане и составляющие в совокупности комплекс банковских

правоотношений, реализующихся в процессе функционирования интернет-банкинга.

Предметом исследования являются нормы казахстанского законодательства, нормы зарубежного законодательства, регулирующие интернет-банкинг, а также судебная практика по гражданским делам, связанным с интернет - банкингом.

Целью работы является разработка научных положений и практических предложений по совершенствованию правового регулирования интернет-банкинга, с учетом зарубежного опыта.

Для осуществления цели поставлены следующие задачи:

- проанализировать национальные источники и международный опыт правового регулирования интернет-банкинга;
- исследовать научные и нормативные подходы к определению договорного регулирования оказания электронных банковских услуг;
- раскрыть содержание и особенности оказания услуг интернет-банкинга;
- рассмотреть проблемы защиты прав клиентов интернет-банкинга и судебной практики по решению споров, связанных с получением услуг интернет-банкинга;
- сформулировать рекомендации по решению правовых проблем функционирования интернет-банкинга в Республике Казахстан.

Положения, выносимые на защиту

1. В связи с отсутствием законодательного определения интернет-банкинга предложено интернет-банкинг понимать как технологии дистанционного обслуживания или способа осуществления банковской деятельности с помощью систем удаленного доступа для осуществления клиентами банковских операций в режиме реального времени и получения информации через интернет-ресурс банка или его мобильное приложение. Сформулирован вывод об отсутствии необходимости специального введения в законодательство понятия интернет-банкинга, так как оно входит в понятие электронных банковских услуг, осуществляемых посредством интернет-ресурса или мобильного приложения банка.

2. В связи с необходимостью определения сущности электронных банковских услуг, сформирована авторская позиция о необходимости определения электронных банковских услуг как осуществление банками информационных и электронных платежных банковских услуг посредством систем удаленного доступа клиента к своему банковскому счету.

3. В связи с имеющейся проблемой информационной диспропорции, связанной с договором на оказание электронных банковских услуг, сформировано авторское представление решения проблемы информационной и договорной диспропорции с учетом нынешних тенденций как в части трансформации банковских услуг (дальнейшей цифровизации банковских услуг), так и в части новых направлений в юриспруденции (внедрением юридического дизайна), в связи с чем предложено пункт 13 Правил оказания банками, филиалами банков-нерезидентов Республики Казахстан и

организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденных постановлением Правления Национального Банка РК от 31 августа 2016 года № 212, дополнить следующим абзацем:

«К внутреннему документу банка, регулирующему порядок оказания электронных банковских услуг, прилагается памятка, содержащая информацию о мерах безопасности при совершении банковских операций через интернет. Памятка должна излагаться доступным языком с описанием алгоритма действий клиента при подозрении на мошеннические действия третьих лиц и с использованием визуализации. Памятка должна на ежемесячной основе направляться клиенту по всем действующим каналам связи с клиентом.».

4. Для решения проблемы договорной диспропорции по договору на предоставление электронных банковских услуг, вследствие которой клиенты банка, являясь слабой стороной договора, не имеют возможность влиять на условия договора, а банки возлагают на клиента ответственность за несанкционированные платежи, совершенныемошенниками, что в свою очередь, ставит клиентов в заведомо невыгодное положение в последующих судебных разбирательствах, предложено пункт 10 Правил оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденных постановлением Правления Национального Банка РК от 31 августа 2016 года № 212, дополнить частью третьей следующего содержания:

«Является ничтожным и не допускается включение в договор условия, возлагающего на клиента ответственность за несанкционированный платеж, совершенный в случае утери или передачи информации третьим лицам в результате мошеннических действий, при наличии уведомления о несанкционированном платеже.».

5. Для усиления защиты клиентов интернет-банкинга от мошенничеств, связанных с удаленной идентификацией и передачей персональных данных, паролей, кодов, в том числе в результате атак социальной инженерии, влекущих денежные потери, обоснована необходимость дополнить полномочия регулятора (Национального Банка РК) полномочием утверждения признаков сомнительных банковских операций, при выявлении которых банк обязан отменить, заблокировать или приостановить их совершение. В связи с этим предлагается внести в статью 15 Закона РК «О Национальном Банке Республики Казахстан» перечень полномочий Правления Национального Банка и в статью 4 Закона РК «О платежах и платежных системах» перечень полномочий Национального Банка в области платежей и платежных систем.

Предлагается к сомнительных банковским операциям, совершаемым через интернет, отнести совершение операций с изменением устройства, с которого осуществляется вход в интернет-банкинг, и/или номера телефона и/или в случае получения уведомления клиента о несанкционированном платеже в течение определенного количества рабочих дней. Перечень таких сомнительных

банковских операций предложено утвердить подзаконным нормативным правовым актом Национального Банка.

6. Аргументирована необходимость, дополнительно к имеющейся законодательной обязанности банка обеспечивать выполнение процедур безопасности от несанкционированного платежа, законодательного установления обязанности банков по внедрению антифрод систем, анализирующих поведение клиента, с внедрением алгоритмов искусственного интеллекта и машинного обучения. В связи с чем, данную обязанность банков предлагается закрепить в пункт 4 статьи 56 Закона РК «О платежах и платежных системах и изложить его в следующей редакции:

«4. Банк, организация, осуществляющая отдельные виды банковских операций, или отправитель денег при осуществлении платежей с помощью средств электронных платежей обеспечивают выполнение процедур безопасности от несанкционированных платежей, в том числе предусматривающих внедрение системы противодействия мошенничеству (антифрод системы), анализирующей поведение клиента (характер, объемы и параметры совершаемых клиентом операций)».

Научная новизна

Научная новизна диссертационного исследования заключается в том, что в нем проведен комплексный анализ правового регулирования интернет-банкинга как в части нормативной основы его функционирования и анализа договора на оказание электронных банковских услуг, так и в части защиты прав клиентов интернет-банкинга посредством информационной безопасности банков и защиты персональных данных банковских клиентов и сформулированы авторские выводы и предложения по совершенствованию правового регулирования интернет-банкинга.

Практическая значимость

Практическая значимость темы заключается в возможности использования результатов исследования для совершенствования банковского законодательства в сфере оказания услуги интернет- банкинга.

Материалы исследования могут использоваться Национальным Банком РК, Агентством РК по регулированию и развитию финансового рынка для осуществления эффективного надзора за оказанием электронных услуг банками.

Материалы и разработки по данной теме также могут представлять интерес в правоприменительной практике для юристов, работников банков, банковских аналитиков, судов общей юрисдикции и арбитражей.

Результаты настоящей работы могут быть использованы в дальнейших научных исследованиях указанной проблемы и при преподавании предметов «Гражданское право», «Обязательственное право», «Информационное право», «Киберправо», «Финансовое и банковское право», «Банковское право зарубежных стран», «Банковское дело» и т.д.

Методологическая основа

Методологическая основа исследования состоит из общенаучного диалектического метода познания и частно-научных методов исследования:

системного, формально-юридического и сравнительно-правового анализа, синтеза, индукции, дедукции и др. (анализ нормативно-правовых источников; сравнение; обобщение; анализ документов).

Также применены положения отраслевых юридических наук и теории права.

Теоретическая основа диссертационного исследования. Теоретической основой работы стали научные труды зарубежных авторов: Ермаковой Е.П., Фроловой Е.Е., Кузнецовой Т.И., Малиновского Р.А., Несмеловой А.С., Алексеевой Д., Козлова С.В. Коломойцевой А.Н., Газизова А.Р. SyarifahLisaAndriati, FaradilaYulistariSitepu, Федюниной А.В., Гончарова А.М.

Нормативной основой исследования является действующее законодательство Республики Казахстан, регулирующее отношения, возникающие в сфере оказания банками услуги интернет-банкинга, в том числе Гражданский кодекс РК, Законы «О банках и банковской деятельности в Республике Казахстан», «О платежах и платежных системах», «Об электронном документе и электронной цифровой подписи» «О персональных данных и их защите», «Об информатизации» и другие нормативные правовые акты.

Структура работы. Структура работы состоит из введения, основной части, состоящей из трех разделов, включающих семь подразделов,заключения и списка использованной литературы.

Первый раздел посвящен исследованию понятий электронных банковских услуг, интернет-банкинга, их соотношения между собой, анализу необходимости закрепления понятия интернет-банкинга в законодательстве, а также нормативной основе функционирования интернет-банкинга.

Второй раздел раскрывает вопросы, связанные с договором на оказание электронных банковских услуг, а именно: нормативная база, признаки, особенности договора, а также проблемы, связанные с заключением договора.

В третьем разделе исследованы вопросы, имеющим важное значение для безопасного использования интернет-банкинга, таким как правовое регулирование удаленной идентификации и защита персональных данных при использовании интернет-банкинга.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ФУНКЦИОНИРОВАНИЯ ИНТЕРНЕТ-БАНКИНГА

1.1 Понятие интернет-банкинга и электронных банковских услуг

Начало развития интернет-банкинга началось в США в 80-х годах прошлого века на основе системы «банк-клиент» для корпоративных клиентов, а годом возникновения интернет-банкинга считается 1995 год, когда американский банк Presidential Savings Bank сообщил о возможности онлайн доступа к банковским услугам в дополнение к традиционной форме обслуживания. В том же году открылся первый виртуальный банк Security First Network Bank, который не имел офисов и обслуживал клиентов полностью через интернет. В Германии Commerzbank в 1995 г. создал дочерний виртуальный банк Comdirect, который предоставлял банковские услуги в онлайн-режиме. К 1997 г. уже множество банков по всему миру предоставляли банковскую информацию через интернет-сайты и предлагали совершение банковских операций онлайн [6].

Изначально онлайн обслуживание заключалось в получении информационных услуг и предлагалось корпоративным клиентам, то есть, юридическим лицам, а позже стали развиваться и розничные услуги интернет-банкинга, включающие проведение платежей и переводов.

В Казахстане интернет-банкинг в Казахстане функционирует более 20 лет. В марте 2000 г. в тестовом режиме запущен интернет-банкинг Казкоммерцбанка. В мае 2000 года ТЕХАКА BANK сообщил о запуске своей системы онлайн-обслуживания Netbank.kz. В июне 2000 года стартоваласистема «Интернет-Банкинг» Народного Банка Казахстана [7].

Следует отметить, что казахстанское законодательство не предусматривает понятие «интернет-банкинга».Основной закон для банковского рынка – Закон «О банках и банковской деятельности в Республике Казахстан» (далее – Закон о банках)не содержит норм об интернет-банкинге.

Интернет-банкинг наряду с мобильным банкингом упоминается в подзаконных актах, обязывающих банки второго уровня, филиалы банков-нерезидентов, организации, осуществляющие отдельные виды банковских операций, а также платежные организации ежеквартально представлять информацию о количестве зарегистрированных пользователей интернет и мобильного банкинга и о пользователях, совершивших операции в интернет и мобильном банкинге в отчетном квартале[8].

Однако это не означает отсутствия регулирования в Казахстане интернет-банкинга, поскольку казахстанское законодательство оперирует термином «электронные банковские услуги».

В этой связи, возникают следующие вопросы:

1) формулирования понятия интернет-банкинга ввиду его законодательного отсутствия;

2) соответствия определения электронной банковской услуги ее содержанию;

3) соотношения понятий интернет-банкинга и электронной банковской услуги;

4) необходимости введения законодательного понятия интернет-банкинга.

Интернет-банкинг в широком смысле можно определить как банковские услуги, оказываемые клиентам посредством сети Интернет.

В научных статьях интернет-банкинг определяется как:

- электронные финансовые (банковские) услуги, осуществляемые на основании выданной в установленном законом порядке лицензии с целью оказания клиенту (физическому или юридическому лицу) удаленного управления счетами и осуществления банковских операций [9];

- система «применения того или иного программного обеспечения различных услуг банка (кредитной организации либо оператора интернет-банкинга) по предоставлению доступа к счету клиента через интернет (с использованием сети интернет) и осуществлению расчетов в режиме реального времени» [10];

- сервис, предоставляющий доступ к банковскому счету через интернет для осуществления платежей, переводов, покупки иностранной валюты, открытия счетов, а также получения информации о состоянии счета, о совершенных операциях и т.д.[11];

- с появлением мобильных приложений банков и, соответственно мобильного банкинга, предлагаются уточнения, что интернет-банкинг позволяет осуществлять платежи через сайт банка с использованием сети Интернет [12].То есть, устройство, с которого производится доступ к банковским счетам, становится разграничительным признаком между этими двумя технологиями, в связи с чем мобильный банкинг выделяется как отдельный вид электронной банковской услуги наряду с интернет-банкингом.

Вместе с тем, более правильным представляется считать мобильный банкинг разновидностью интернет-банкинга, так как обе технологии могут использоваться только при наличии интернета, а во всем остальном порядок их функционирования идентичен.

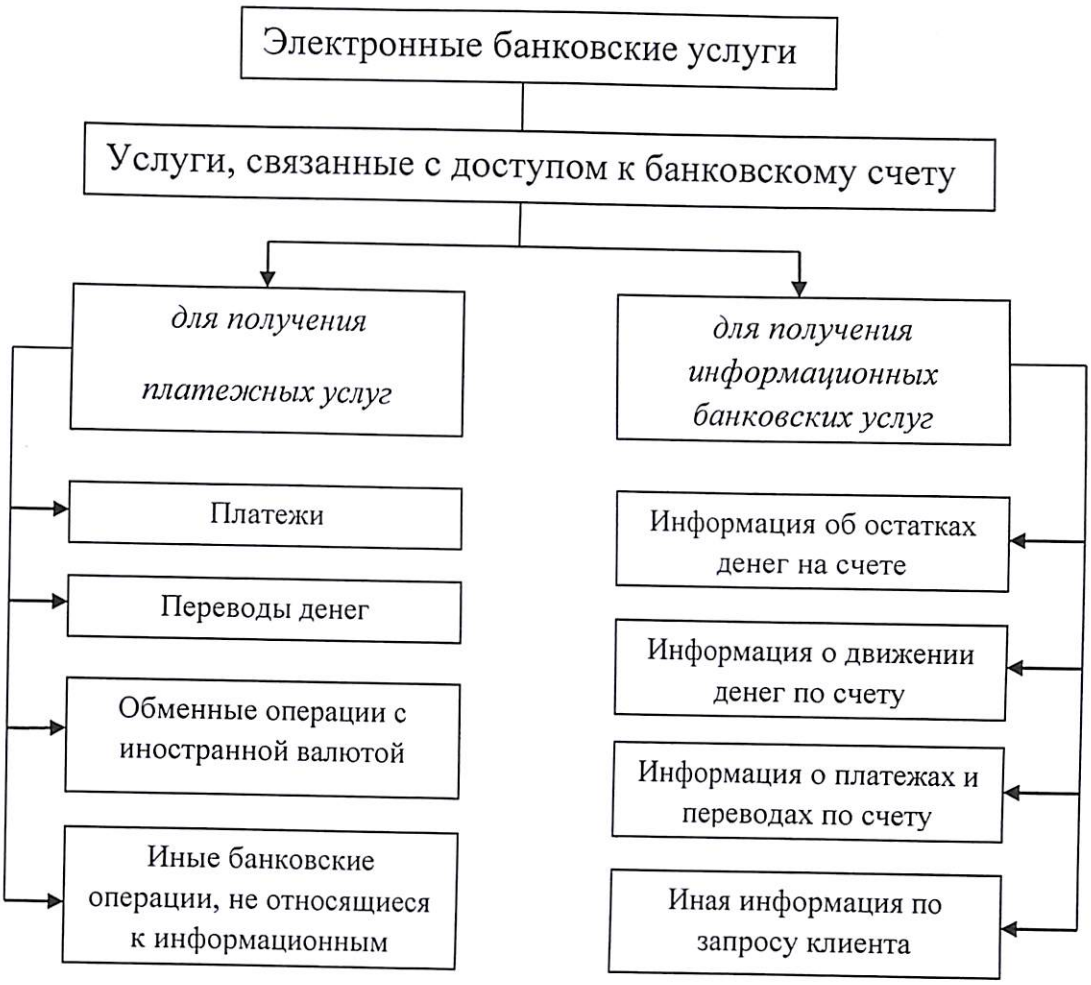
Таким образом, обобщая различные определения, можно сформулировать понятие интернет-банкинга как технологию дистанционного обслуживания или способ осуществления банковской деятельности с помощью системудаленного доступа для осуществления клиентами банковских операций в режиме реального времени и получения информации через интернет-ресурс банка или его мобильное приложение.

Понятие электронных банковских услуг было введено в 2008 году, с принятием Правил предоставления банками второго уровня и организациями, осуществляющими отдельные виды банковских операций,электронных банковских услуг, утвержденных постановлением Правления Национального Банка от 28 марта 2008 года №18 (далее – Правила № 18, утратили силу в настоящее время).

В настоящее время определение электронных банковских услуг закреплено на уровне законодательного акта и включает в себя «услуги, связанные с

доступом клиента к … банковскому счету … для получения платежных услуг и информационных банковских услуг» (подпункт 75) статьи 1 Закона «О платежах и платежных системах» (далее – Закон о платежах) [13]).

Наглядно понятие электронных банковских услуг можно представить так:



Из данного определения вытекает, что электронная банковская услуга не относится к банковской операции, а является лишь услугой доступа для дальнейшего осуществления банковских операций (платежных услуг банков, имеющих лицензию на такие виды банковских операций, как открытие и ведение банковских счетов клиентов и переводные операции) и получения информации.

Такое понимание электронной банковской услуги как «услуги, связанной с доступом клиента» к своему банковскому счету, не может считаться верным исходя из сути данной услуги, а также противоречит Закону о банках, статья 30 которого содержит исчерпывающий перечень разрешенных банку операций, в числе которых нет «услуг, связанных с доступом».

Более правильным представляется определение электронных банковских услуг, которое ранее предусматривалось в утративших силу Правилах № 18 и содержало в себе два вида услуг:

- уже упомянутые услуги, «связанные с получением доступа»для получения информации (по сути, информационные банковские услуги);

- услуги, связанные с «осуществлением платежей и переводов денег, открытием или закрытием банковского (-их) счета (-ов) и/или осуществлением иных видов банковских операций, предоставляемых банком…» [14], то есть, банковские операции.

Таким образом, законодательное определение электронных банковских услуг требует уточнения для более правильного отражения сути данных услуг.

Для такого уточнения сначала обратимся к понятию традиционной, не электронной, банковской услуги. Так, Правилами «традиционные» банковские услуги отождествлены с банковскими операциями, предусмотренным Законом о банках [15].

Автор статьи, рассмотревший шесть подходов к определению банковской услуги (функциональный, маркетинговый, производственный, институциональный, семантический, правовой), отмечает, что сторонниками правового подхода (Викулин А.Ю., Макаров О.М., Даниленко С.А., Сахаров Л.С., Тосунян Г.А., Сидоров В.Н., ЭшалянА.М.) банковская услуга рассматривается как сделка, совершать которую вправе только кредитные организации [16]. То есть, в данном случае акцент сделан больше на субъектный элемент данного термина, без учета содержания услуги.

Как отмечают авторы статьи Гайзатуллин Р.Р., Гараев З.Ф., один из первых исследователей электронных банковских услуг Грачев М.В. определял данные услуги как способ осуществления банковских бизнес-процессов посредством электронных сетей [10].

Если обратиться к правоприменительной практике, а именно, к договорам на предоставление электронных банковских услуг, то следует отметить, что не все банки дают пояснение данного термина в своих формах или внутренних документах. На момент изучения определение электронных банковских услуг имеется в Общих условиях соглашения о предоставлении электронных банковских услуг АО «Форте банк» как услуги, предоставляемой банком пользователю посредством системы дистанционного банковского обслуживания способами, не противоречащими законодательству Республики Казахстан [17]. То есть, данное определение отражает как субъектный состав, так и само содержание услуги – это услуги банка, оказываемые дистанционным способом.

Также необходимо отметить следующее. Предусмотренное Законом о платежах понятие электронной банковской услуги содержит платежные услуги, перечень которых установлен пунктом 1 статьи 12 данного Закона. Однако, к непосредственно электронным банковским услугам можно отнести лишь одну платежную услугу из перечисленных в указанном пункте девяти - услугу по приему и осуществлению платежей и (или) переводов денег с использованием банковского счета, и которую имеют право осуществлять только банки, имеющие лицензию на открытие и ведение банковских счетов клиентов и переводные операции.

В этой связи, возникает вопрос, вправе ли осуществлять электронные банковские услуги организации, осуществляющие отдельные виды банковских операций. Подзаконный акт – Правила оказания банками, филиалами банков-

нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденных постановлением Правления Национального Банка РК от 31 августа 2016 года № 212 (далее – Правила № 212) распространяются и на организации, осуществляющие отдельные виды банковских операций, то есть, предполагается, что не только банки, но и организации, осуществляющие отдельные виды банковских операций, могут оказывать электронные банковские услуги, включающие электронные платежные услуги.

Таким образом, регулятору необходимо устранить имеющееся противоречие Правил № 212 нормам Закона о платежах.

Также отдельно следует отметить, что перечень платежных услуг, предусмотренных Законом о платежах, гораздо шире понятия электронных платежных услуг, предусмотренных Правилами № 212 (к которым отнесены платежи, переводы, обменные операции и иные банковские операции),и в целях выработки понятия электронных банковских услуг необходимо руководствоваться именно термином «электронные платежные услуги».

С учетом вышеизложенных доводов предлагается рассмотреть следующую формулировку для уточнения законодательного понятия: электронные банковские услуги – это осуществление банками информационных и электронных платежных банковских услуг посредством систем удаленного доступа клиента к своему банковскому счету.

В части соотношения электронных банковских услуг и интернет-банкинга необходимо отметить следующее.

Электронные банковские услуги предоставляются через интернет-ресурс банка и через электронные терминалы [18], т.е. банкоматы. В этой связи, услуги интернет-банкинга являются одним из видов электронных банковских услуг, а значит, электронная банковская услуга (ЭБУ) – более широкое понятие, которое включает в себя услуги посредством интернет-банкинга, и их соотношение можно определить следующим образом:

Правила № 212 устанавливают порядок оказания электронных банковских услуг, требования к содержанию договора, способы идентификации клиента и другие процедуры в целях безопасности, а также защитные механизмы от

несанкционированного доступа, которые в основном применимы именно к услугам интернет-банкинга.

То есть, можно в целом сделать вывод, что регулирование электронных банковских услуг и есть регулирование интернет-банкинга, и особой необходимости в отдельном выделении/закрепление/введении в законодательство термина «интернет-банкинг» нет.

1.2 Нормативно-правовые основы функционирования/использования интернет-банкинга

Исследователи отмечают, что интернет-банкинг предоставляется двумя основными способами: в виде традиционного банка, который создает интернет-ресурс и предлагает своим клиентам интернет-банкинг. Второй альтернативой является создание «виртуального», «внеофисного» или «только интернет» банка [19].

В Казахстане представлен первый способ – банки с офисами дополнительно развивают систему интернет-банкинга.

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.

Функционирование интернет-банкинга предполагает два направления его регулирования:

1) регулирование отношений между банком и клиентом, которое осуществляется посредством общих норм о заключении договора, в частности о договоре банковского обслуживания (глава 38 ГКРК), а также требования к содержанию договора об оказании платежных услуг предусмотрены Законом о платежах.

Кроме того, в этом направлении действуют также общие нормы, регулирующие вопросы сохранения персональных данных (Закон РК «О персональных данных и их защите») и вопросы подписания электронных договоров («Об электронном документе и электронной цифровой подписи»);

2) регулирование деятельности банка, предоставляющего услуги в дистанционном формате, в том числе в части информационной безопасности, путем издания нормативных правовых актов и контроля за их исполнением в реализацию Закона РК «О Национальном Банке Республике Казахстан» и Закона о банках, а также Закон РК «Об информатизации»

В этом направлении действуют следующие законодательные акты:

- урегулированным в настоящее время аспектом дистанционного банковского обслуживания является его использование в целях совершения платежных операций, в связи с чем, основным актом можно назвать Закон о платежах;

- в части противодействия легализации (отмыванию) доходов, полученных преступных путем, сфера интернет-банкинга подпадает в сферу применения

Закона РК «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Основным подзаконным актом, регулирующим функционирование интернет-банкинга, являются уже упомянутые Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденных постановлением Правления Национального Банка РК от 31 августа 2016 года № 212.

Данными Правилами урегулированы вопросы предоставления электронных банковских с использованием систем удаленного доступа, обязанности банков по отношению к клиентам, требования к процедурам безопасности, определены понятия аутентификации, динамической и биометрической идентификации, а также случаи приостановления и прекращения оказания электронных банковских услуг.

К другим нормативным правовым актам, регулирующим сферу интернет – банкинга, а именно в части обеспечения информационной безопасности, относятся:

- постановление Правления Национального Банка № 48 от 27 марта 2018 года «Об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций (Требования) и Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах»;

- постановление Правления Агентства по регулированию и развитию финансового рынка от 21 сентября 2020 года № 90«Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности»

- постановление Правления Агентства по регулированию и развитию финансового рынка № 111 от 23 ноября 2020 года «Об утверждении методики оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности»;

- постановление Правления Национального Банка № 47 от 27 марта 2018 года «Об утверждении Правил и сроков представления банками, филиалами банков-нерезидентов Республики Казахстан сведений о наличии систем управления информационной безопасностью, а также о соблюдении требований к обеспечению информационной безопасности в Национальный координационный центр информационной безопасности»;

- постановление Правления Агентства по регулированию и развитию финансового рынка № 89 от 21 сентября 2020 года «Об утверждении требований к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности»;

- постановление Правления Агентства по регулированию и развитию финансового рынка № 110 от 23 ноября 2020 года «Об утверждении Правил оценки уровня защищенности от угроз информационной безопасности»;

- Постановление Правительства Республики Казахстан № 83 от 20 декабря 2016 года «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

Как видно из данного перечня, вопросы информационной безопасности урегулированы достаточно обширным перечнем подзаконных актов. Здесь следует отметить, что банки как субъекты финансового рынка находятся в ситуации регулирования со стороны трех государственных органов, устанавливающих требования по информационной безопасности, а именно: Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности, Агентства по регулированию и развитию финансового рынка и Национального Банка».

В этой части планируется создание четкой иерархической структуры полномочий уполномоченного органа, Агентства по регулированию и развитию финансового рынка и Национального банка[2].

Так, в Стратегии сообщается, что «под разработанные уполномоченным органом в сфере обеспечения информационной безопасности концептуальные требования в виде концепций, стратегий, законов Агентство и Национальный Банк в пределах своих полномочий на своем уровне будут вырабатывать детализированные и уточненные требования к организации систем управления информационной безопасностью субъектов финансового рынка, а также к обработке инцидентов, на основании которых будут осуществляться проверки субъектов» [2].

В статьях, посвященных иностранному регулированию интернет-банкинга, рассматривают интернет-банкинг как особой вид банковской услуги, и выделяют разновидности таких банковских услуг, как онлайн-платежи, оплата счетов, получение кредитов и онлайн-инвестирование[20].

Последняя разновидность, связанная с инвестированием через интернет-банкинг, пока отсутствует в Казахстане, но в ближайшее время будет развиваться в связи с расширением услуг банка по брокерскому обслуживанию своих клиентов на основе не банковской лицензии, а лицензии на осуществление брокерской и дилерской деятельности на рынке ценных бумаг и договора о брокерском обслуживании.

Первых же три разновидности уже широко применяются в Казахстане, и отношения между банком и клиентом для оказания данных услуг регулируются договором, который будет рассмотрен в следующей главе.

В дополнение к вопросу нормативной базы, регулирующей функционирование интернет-банкинга, также стоит отметить вопросы защиты прав потребителей.

Данные права в части цифровых финансовых услуг на законодательном уровне отдельно не урегулированы. Права потребителей финансовых услуг, в том числе в цифровом формате, защищены путем применения регулятором

комплексных мер по установлению требований к деятельности банков и контроля за их исполнением, на основании норм Закона о банках.

Так, глава 7-1 Закона о банках, которая называется «Меры по защите потребителей банковских услуг», регулирует вопросы гарантирования депозитов и обеспечения беспрерывности предоставления банковских услуг.

Поэтому для защиты клиентов интернет-банкинга применимы общие положения, распространяющиеся на потребителей традиционных банковских услуг, сосредоточенные в нормативных правовых актах о банковском обслуживании.

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

Необходимость введения в законодательство понятия интернет-банкинга отсутствует, так как он является способом осуществления одного из видов электронных банковских услуг, оказываемых посредством интернет-ресурса банка. Само же понятие электронных банковских услуг требует пересмотра для более правильного отражения сути данных видов услуг. Предлагается изложить понятие «электронные банковские услуги» как осуществление банками информационных и электронных платежных банковских услуг посредством систем удаленного доступа клиента к своему банковскому счету.

2 ДОГОВОРНОЕ РЕГУЛИРОВАНИЕ ОКАЗАНИЯ ЭЛЕКТРОННЫХ БАНКОВСКИХ УСЛУГ

2.1 Нормативные основы договора об оказании электронных банковских услуг

В данной части исследования на изучение были поставлены следующие вопросы:

1) на каком законодательном уровне предусмотрено заключение договора об оказании электронных банковских услуг;

2) полномочия государственных органов в отношении договора об оказании электронных банковских услуг;

3) порядок заключения договора об оказании электронных банковских услуг;

4) каково соотношение договора об оказании электронных банковских услуг и договора об оказании платежных услуг.

Договор о предоставлении электронных банковских услуг следует отнести к договорам банковского обслуживания. Пункт 2 статьи 739 Гражданского кодекса РК перечисляет виды данных договоров, в числе которых предусматривает «иные виды договоров, предусмотренные законодательством или соглашением сторон» [21].

Таким образом, данная норма позволяет предусмотреть необходимость заключения договора об оказании электронных банковских услуг на уровне подзаконных актов, что и действует в настоящее время. Так, заключение договора о предоставлении электронных банковских услуг и требования к его содержанию предусмотрены Правилами № 212.

Данные Правила утверждены Национальным Банком РК в рамках его полномочий в области платежей и платежных систем по утверждениюправил оказания электронных банковских услуг, установленных Законом о платежах. В таком контексте указанного полномочия представляется правомерным утверждение Национальным Банком требований к содержанию договора об оказании электронных банковских услуг, в числе которых способы предоставления электронных банковских услуг и получения доступа к ним, процедуры безопасности, а также порядок аутентификации и подтверждения прав клиента на получение электронных банковских услуг и ответственность сторон за неисполнение или ненадлежащее исполнение своих обязательств по договору.

Пунктом 23 Правил № 212 [18] установлено, что договор должен содержать процедуры безопасности, установленные внутренними документами банка и договором. При этом требования к информационной безопасности устанавливаются, как уже указывалось выше, различными нормативными правовыми актами трех регулирующих государственных органов - Комитета по информационной безопасности Министерства цифрового развития,

инноваций и аэрокосмической промышленности, Агентства по регулированию и развитию финансового рынка и Национального Банка.

В этой связи, предлагается в пункт 23 Правил № 212 внести дополнение, что процедуры безопасности устанавливаются не только внутренними документами и договором, но и законодательством, изложив его в следующей редакции:

«23. Предоставление банком электронных банковских услуг производится в соответствии с процедурами безопасности, установленными законодательством Республики Казахстан, внутренними документами банка и договором».

Также в целом возникает вопрос полномочий указанных государственных органов в части оказания электронных банковских услуг. Возможно нормативный правовой акт, регулирующий оказание электронных банковских услуг, необходимо принимать как совместный акт указанных регулирующих государственных органов.

Предметом договора по оказанию услуг в интернет-банкинге является предоставление банком банковских услуг посредством систем удаленного доступа.

Как правило, это стандартная форма договора, утверждаемая уполномоченным органом банка, и заключение договора происходит путем присоединения на основе статьи 389 ГКРК, согласно которой договором присоединения признается договор, условия которого определены одной из сторон в формулярах или иных стандартных формах и могут быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом. Заявления на подключение к системам удаленного доступа и договор рассматриваются в качестве единого документа.

Система удаленного доступа в соответствии с Законом о платежах [13] определяется как «совокупность средств телекоммуникаций, цифровых и информационных технологий, программного обеспечения и оборудования, обеспечивающих связь между клиентом и поставщиком платежных услуг для получения электронных банковских услуг».

Кроме того, требования пункта 4 статьи 13 Закона о платежах [13] также применимы к договору об оказании электронных банковских услуг, так как устанавливают, что договор оказания платежных услуг должен содержать, помимо других условий, порядок «защитных действий от несанкционированных платежей» и порядок «регулирования вопросов по несанкционированным платежным услугам».

Вместе с тем, возникает ситуация, когда требования к содержанию договора устанавливаются как законодательным актом в части электронных платежных услуг (Закон о платежах), так и подзаконным актом (Правила № 212). При этом законодательным актом не оговаривается, что дополнительные требования могут быть установлены нормативным правовым актом Национального Банка. Скорее всего, данное обстоятельство связано с тем, что платежные услуги и электронные банковские услуги не тождественны, а совпадают лишь в определенной части, а именно в части предоставления услуг по приему и

осуществлению платежей и (или) переводов денег с использованием банковского счета посредством систем удаленного доступа:

Необходимо отметить, что потребители, как правило, присоединяются к условиям данных договоров путем физического подписания соответствующего заявления в банке при получении другой услуги, за которой обращаются в банк либо фактом регистрации учетной записи в интернет-банкинге [22]. То есть, как правило, условием подключения клиента к интернет-банкингу является наличие открытого банковского счета (выпуска платежной карточки). Кроме того, в некоторых банках присоединение осуществляется не только к условиям договора, но и к внутренним правилам банков.

2.2 Понятие, содержание, особенности исполнения договора об оказании электронных банковских услуг

Как было уже выше отмечено, в научной литературе отсутствуют исследования доктринальных особенностей договора на оказание электронных банковских услуг. В этом подразделе рассмотрены признаки договора электронных банковских услуг, его особенности, а также природа обязательств, возникающих из данного договора.

Договор на оказание электронных банковских услуг является поименованным договором, так как предусмотрен законодательством, и исходя из количества сторон относится к двусторонним сделкам: сторонами являются банк и клиент, которым может быть как физическое, так и юридическое лицо.

Так как договор о предоставлении электронных банковских услуг относится к договорам банковского обслуживания, то исходя их определения договора банковского обслуживания, предусмотренного пунктом 1 статьи 739 Гражданского кодекса РК, предусматривающего оплату клиентом банковских услуг, то договор электронных банковских услуг можно отнести к возмездным договорам. Как подтверждение возмездности, на практике договорами на оказание электронных банковских услуг предусматривается обязанность клиента оплачивать комиссии/вознаграждения банку за совершение операций в соответствии с тарифами банка (пункт 3.2. Договора АО «Народный Банк Казахстана») [22].

Договор на оказание электронных банковских услуг не требует внесения денег клиентом, а обязывает его при необходимости совершения платежа обеспечить на банковском счете нужную сумму. Учитывая, что по договору предоставляются как платежные, так и информационные услуги, он может действовать и при отсутствии денежных средств на счете. В этой связи, договор на оказание электронных банковских услуг можно отнести к консенсуальным договорам.

Также данный договор относится к двусторонним, взаимно обязывающим договорам, то есть, предусматривающим как права, так и обязанности для каждой из сторон.

Так, банк обязан исполнять поручения клиента, предоставлять информацию по запросу клиента, хранить тайну операций, а также обеспечивать функционирование интернет-банкинга, принимать меры безопасности и т.д.

Клиент, в свою очередь, обязан обеспечивать наличие достаточных средств в случае совершения платежей и переводов, оплачивать услуги банка, соблюдать меры безопасности, информировать о подозрениях или случаях несанкционированных платежей.

Что касается срока договора на оказание электронных банковских услуг, то он как правило, он является бессрочным. Вместе с тем, он может быть привязан к сроку договора текущего счета, который в соответствии с пунктом 3 статьи 747 Гражданского кодекса РК может быть бессрочным, если законом или договором не установлены конкретные сроки действия.

Банковским законодательством не определена форма договора на оказание электронных банковских услуг, в связи с чем, следует руководствоваться нормами гражданского законодательства, предписывающими необходимость соблюдения письменной формы для заключения сделок в предпринимательской деятельности, а банковская деятельность – одна из видов предпринимательской деятельности.

Правила № 212 не содержат норм о способах подписания договора на оказание электронных банковских услуг. Данные способы установлены другим нормативным правовым актом Национального Банка РК [23], который для подписания договора банковского обслуживания (к которому относится и договор на предоставление электронных банковских услуг) допускает возможность использования динамической идентификации.

Договор о предоставлении электронных банковских услуг, как уже указывалось выше, является договором присоединения. Банк разрабатывает стандартную форму договора, а клиент присоединяется полностью к его условиям, что соответствует признакам договора присоединения, установленным пунктом 1 статьи 389 Гражданского кодекса РК.

В правовой доктрине много споров касательно публичности договора банковского счета, но в отношении договора на предоставление электронных банковских услуг (интернет-банкинга или дистанционного банковского обслуживания), как уже отмечалось, отсутствуют какие-либо мнения. Законодательство в целом не содержит указаний на публичность договоров

банковского обслуживания, в связи с чем, предлагается восполнить данный пробел в отношении исследуемого договора.

Исходя из определения публичного договора, предусмотренного Гражданским кодексом, первый признак публичного договор – субъектный состав («лицо, осуществляющее предпринимательскую деятельность») – присущ договору на оказание электронных банковских услуг, так как стороной, оказывающей услуги, является банк, деятельность которого относится к предпринимательской деятельности.

То есть, вторым квалифицирующим признаком публичного договора является характер осуществляемой предпринимателем деятельности.

Данный признак может быть свойственен договору на оказание электронных банковских услуг, вместе с тем данные услуги согласно Правил № 212 осуществляются только по тем банковским операциям, которые предусмотрены выданной банку лицензией, и что немаловажно – только при наличии в банке систем удаленного доступа. Законодательство не обязывает банк внедрять системы удаленного доступа, это добровольное решение банка в случае его желания предоставлять электронные банковские услуги.

Учитывая, что в настоящее время в условиях конкуренции с другими банками, а также финтех-компаниями любой банк осознает необходимость дистанционного предоставления услуг и внедряет системы удаленного доступа, то можно считать, что по характеру деятельности договор на оказание электронных банковских услуг соответствует признаку публичности.

Следующим квалифицирующим признаком публичного договора является осуществление этой деятельности в отношении каждого, кто обращается за услугой.

Как уже отмечалось выше, доступ в интернет-банкинг предоставляется, как правило, при наличии открытого банковского счета, выпуска платежной карточки. Также такой доступ может предоставляться при выдаче клиенту кредита, и интернет-банкинг позволяет оказывать клиенту электронные банковские услуги по погашению им очередных платежей по кредиту или предоставлению информации о задолженности.

Таким образом, сложившаяся практика заключения договора на оказание электронных банковских услуг позволяет сделать вывод, что данный договор заключается только с действующим клиентом банка, у которого уже заключен с банком «первичный» договор банковского обслуживания (договор банковского счета, банковского вклада, кредитный договор).

То есть, исследуемый договор не может быть заключен в отношении каждого, кто обратится в банк, и по данному признаку не может считаться публичным договором.

На основании изложенного, договор на оказание электронных банковских услуг следует относить к поименованным, двусторонним, консенсуальным, бессрочным и не публичным договорам, и в случае заключения договора путем присоединения потребителя в целом к условиям, которые разработаны банком в виде стандартных форм – к договорам присоединения.

2.3 Проблемы договора об оказании электронных банковских услуг и предложения по их устранению

Учитывая, что потребители не имеют привычки читать подписываемые договоры, а тем более договоры, которые размещены на интернет-ресурсе банка, условия функционирования интернет-банкинга, как правило, на этапе заключения договора остаются для клиента нераскрытыми.

То есть, в данном случае можно указать первую проблему интернет-банкинга: наличие «информационной диспропорции», когда клиенту могут быть непонятны и даже неизвестны условия договора при использовании им интернет-банкинга.

Как справедливо указывает авторы книги «Защита прав потребителей финансовых услуг» банк «не вправе пользоваться этой диспропорцией, а если пользуется, то его клиент может рассчитывать на защиту со стороны правопорядка» [24].

Как уже сказано выше, договор о предоставлении электронных банковских услуг, как правило, заключается с клиентом после заключения «основного» договора (к примеру, на открытие текущего счета при получении платежной карточки или при выдаче банковского займа), то есть договор об оказании электронных банковских услуг, по сути, является «вторичным».

Об этом упоминается в Отчете о результатах мониторинга (общественной инспекции) в области защиты прав потребителей финансовых услуг, проведенного в России в 2016 и 2019 годах[25, с.111], который указывает, «что заявления к договору о предоставлении банковских услуг, если речь идет об услуге, которую потребитель не рассматривает в качестве целевой, ради которой он обратился в банк, часто заключаются непосредственно при заключении основного договора, а заполнение соответствующих заявлений производится сотрудником банка. В результате ознакомление с правилами ДБО при подписании договора происходит «в общих чертах», а условия договора о ДБО подписываются потребителем автоматически, если условия предоставления основной услуги его устраивают».

По результатам данного мониторинга консультантами были сделаны следующие выводы [25, с.110-112]:

1) банки не предоставляют клиенту необходимую и достоверную информацию об интернет-банкинге;

2) банки навязывают интернет-банкинг клиентам без учета их потребностей;

3) договоры содержат положения, нарушающие права потребителей;

4) специфика договоров затрудняет возмещение и компенсацию;

5) банки прикладывают недостаточно усилий для обеспечения безопасности интернет-обслуживания клиентов».

Было бы нелишним проведение в Казахстане подобного исследования с целью анализа состояния защиты прав клиентов интернет-банкинга, которое скорее всего, выявило бы аналогичные проблемы.

Остановимся более подробно на проблеме договорных положений, нарушающих права потребителей. В этой части хотелось бы отметить, что вопрос безопасности интернет-банкинга является ключевым и должен стоять на первом месте у банка, предлагающего дистанционные банковские услуги.

При этом банки включают в договоры положения, перекладывающие на клиента ответственность за безопасность, в частности, за проведение платежей в случае несанкционированного доступа третьих лиц к интернет-банкингу.

К примеру, соглашение одного из банков включает такие условия [26]:

1) «банк не несет ответственности за ущерб, возникший вследствие несанкционированного использования третьими лицами средств подтверждения Пользователя, если такое использование стало возможным не по вине банка» (пункт 7.5.);

2) «банк не несет ответственность за несанкционированные платежи, совершенные с банковского счета Пользователя», прошедшего идентификацию и аутентификацию (пункт 7.9., подпункт 1) пункта 2.1);

3) «ответственность за ущерб, возникший вследствие несанкционированного доступа третьих лиц к СДБО, возлагается на виновную сторону» (пункт 7.4.).

Подобные условия можно найти во многих договорах о предоставлении электронных банковских услуг, и в дальнейшем активно используются банками, выступающими ответчиками в судах по искам клиентов.

К примеру, в гражданском деле по иску клиента А.А. к банку о возврате похищенной с депозита суммы банк сослался на предусмотренную договором ответственность клиента за ущерб, причиненный в связи с передачей третьим лицам идентификационных данных клиента.

На основании данного положения договора требования А.А. признаны судом необоснованными, и в иске о взыскании об обязывании банка возвратить сумму отказано.

Суд посчитал, что «мошеннические действия со стороны третьих лиц и несанкционированный перевод денежных средств с депозитного счета истца осуществлены по причине действий самого истца по передаче личных идентификационных данных карты истца и подключению чужого номера телефона к сервису «Доставка СМС-паролей» [27].

О переносе банками рисков на клиентов сообщает и Центральный банк России [28], о проблеме возложения ответственности на клиента указывается и в результатах вышеупомянутого мониторинга, анализе судебной практики за 2016 год по спорам в результате хищений через каналы ДБО [29], а также авторами статьи по проблеме защиты прав клиентов банков [30].

Безусловно, клиент должен осознавать необходимость сохранения конфиденциальности своих идентификационных данных, но банки не должны полностью снимать с себя ответственность, о чем говорят и зарубежные авторы, отмечая, что «банки также должны разделить ответственность за то, чтобы их клиенты не становились жертвами атак мошенников[31].

Статьей 56 Закона о платежах механизм возврата потерянных денег заложен через понятие санкционированного платежа, который должен совершаться «лицом, которое имело полномочие совершить данный платеж» «с соблюдением установленного порядка защитных действий от несанкционированных платежей».

Но в случае мошеннических схем с использованием методов социальной инженерии доказать несанкционированность платежа становится невыполнимой задачей для клиента.

Вместе с тем, нельзя категорически утверждать, что клиент всегда проигрывает. Так, в течение 2018-2019 гг. рассматривалось дело по иску ДБ АО «Сбербанк» о признании незаконными действий РГУ «Национальный Банк Республики Казахстан» в лице Алматинского областного филиала по вынесению письменного предписания с требованием:

- произвести клиенту возврат денег по мошенническим транзакциям, связанным с изъятием вклада;
- обеспечить возврат вкладов на банковские счета вкладчиков, указанные в договоре сберегательного счета.

В данном деле клиент Т.Л. самостоятельно выслала свои конфиденциальные данные мошенникам, тем самым предоставила им возможность удаленного доступа в систему интернет-банкинга.

Банк посчитал, что Национальный Банк необоснованно потребовал от банка возместить сумму несанкционированной операции, просил признать данные действия незаконными, но суды первой и апелляционной инстанции не согласились и отказали в иске.

Итогом этого кейса является то, что клиент Т.Л. смогла возместить похищенные деньги, обратившись в Национальный Банк, который до 2020 года был регулятором финансового рынка, а суд в дальнейшем поддержал действия Национального Банка, признав их законными [32].

Конечно, подобные судебные решения оказываются в меньшинстве в общем количестве дел данной категории, что дополнительно указывает на отсутствие единообразной судебной практики рассмотрения дел, связанных с использованием интернет-банкинга.

В целом же, в связи с возложением на клиента ответственности за риски использования интернет-банкинга, отказов судов в исках клиентов к банкам, сложностью привлечения мошенников к уголовной ответственности, шансы возместить потерянные деньги минимальны.

Поэтому второй проблемой интернет-банкинга является «договорная диспропорция», когда клиент банка не имеет возможности влиять на содержание договора и вынужден полностью присоединяться к договору, положения которого заведомо ставят его в проигрышное положение в случае мошеннических действий третьих лиц.

Конечно, заключение договоров путем присоединения к стандартным формам банков обусловлено большим количеством участников данных отношений, для которых предоставляются одинаковые условия обслуживания,

что в свою очередь, требует стандартизации форм с целью снижения расходов банка и оперативного заключения договора.

Невозможность клиента влиять на условия договора, заключаемого путем присоединения, регулярно обсуждается в юридической науке. Под сомнение ставится основополагающий принцип свободы договора, который предполагает:

1) свободу субъектов гражданско-правовых отношений заключать договоры с другими субъектами;

2) свободу выбора субъектов;

3) свободу выбора вида договора;

4) свободу в определении условий договора (пункт 2 статьи 2 Гражданского кодекса РК). В случае заключения договора путем присоединения ограничивается именно этот элемент свободы договора.

Как отмечают авторы статьи [33] с развитием банковских технологий, включая цифровое пространство, все больше возникает вопросов о свободе договора при получении банковских услуг.

Примечательно, что ограничение свободы договора посредством стандартных форм является мировой тенденцией в договорном праве уже с начала XX века [34].

Хотя заключение договоров путем присоединения, применяемое в банковской практике, лишает клиента возможности обсуждения и изменения условий договора, нельзя утверждать, что заключение иным способом повысит информированность и уровень осознания клиентом необходимости соблюдения мер информационной безопасности.

Даже если клиенты начнут читать подписываемые договоры, условия, написанные сложным, профессиональным языком, зачастую просто не понятны обычным потребителям, а те из них, кому условия понятны, рассчитывают на то, что события, влекущие ответственность, не наступят.

В части изложения условий договора понятным, ясным языком хотелось бы отметить следующее. В настоящее время в юриспруденции развиваются совершенные новые направления, и одним из них является Legaldesign – юридический дизайн. Сложный юридический язык законов, контрактов, зачастую непонятный даже самим юристам, способствует развитию данного направления, которое требует пересмотра подходов подготовки текстов как законодательных и подзаконных актов, так и договоров. Главная цель юридического дизайна – сделать документ понятным для клиента, при этом понятность может достигаться как с помощью структурирования текста (шрифты, необходимые отступы, выделение блоков), так и с помощью визуализации, например, с помощью инфографики.

Конечно, не стоит надеяться, что требования со стороны законодательства к содержанию договоров будут включать и требования к их оформлению с учетом развивающихся тенденций юридического дизайна. Для решения данной проблемы необходима прежде всего заинтересованность банков как в изменении условий договоров, так и в повышении их «читабельности», ясности, для большей сбалансированности интересов клиентов. В договорах нужны более

подробно расписанные процедуры безопасности, и учитывая, что клиенты не читают договоры, данная информация из договоров должна направляться клиентам в виде понятных памяток, буклетов, напоминаний.

В части дополнительных мер защиты клиентов от денежных потерь при столкновении с мошенниками в качестве примера можно привести условие пункта 2.10. в договоре АО «Народный Банк Казахстана», который позволяет снизить денежные потери клиентов в случаях изменения устройства следующим образом:

Договором предусмотрено понятие «Доверенного устройства», с которого клиент входит в мобильное приложение банка, и безопасность обеспечивается путем проверки устройства на основании результатов процедуры верификации. Верификация позволяет исключить вероятность ее прохождения иным лицом. Установлены 2 уровня сессии в мобильном приложении, и в случае, если действия по карте проходят не с Доверенного устройства (уровень Light) банком установлены лимиты на совершение операций, в отличие от сессии с Доверенного устройства (уровень Normal), в которой ограничения отсутствуют [22].

Подобные дополнительные меры позволили бы лучше защитить клиентов интернет-банкинга от мошеннических действий.

В данный момент такие меры могут применяться банками по собственной инициативе, поэтому можно предложить следующие законодательные способы решения проблемы информационной и договорной диспропорции:

1) при заключении «основного», первичного договора с банком, обязать банк выдать (направить) клиенту памятку по информационной безопасности. Такую обязанность предусмотреть в Правилах № 212, а именно пункт 13 дополнить следующим предложением:

«К внутреннему документу банка, регулирующему порядок оказания электронных банковских услуг, прилагается памятка, содержащая информацию о мерах безопасности при совершении банковских операций через интернет. Памятка должна излагаться доступным языком с описанием алгоритма действий клиента при подозрении на мошеннические действия третьих лиц и с использованием визуализации. Памятка должна на ежемесячной основе направляться клиенту по всем действующим каналам связи с клиентом.»;

2) предусмотреть в Правилах № 212 норму, в соответствии с которой банку в договоре запрещается возлагать ответственность за несанкционированные платежи, совершенные в случае утери или передачи информации третьим лицам в результате мошеннических действий, и в целом признать данное условие недобросовестным, а именно, дополнить пункт 10 данных Правил частью третьей следующего содержания:

«Является ничтожным и не допускается включение в договор условия, возлагающего на клиента ответственность за несанкционированный платеж, совершенный в случае утери или передачи информации третьим лицам в результате мошеннических действий, при наличии уведомления о несанкционированном платеже.»

Данное предложение согласуется с нормой пункта 9 статьи 40 Закона о платежах, которая предусматривает, что клиент несет все риски несанкционрованного платежа в случае неуведомления банка. Вместе с тем, внедрение дополнительных мер защиты от методов социальной инженерии должно быть не только на уровне договоров, но и на уровне законодательства, поэтому необходимы изменения в законодательство, которые будут предложены в следующей главе.

Таким образом, на сегодняшний день законодательством предусмотрены требования к содержанию договоров, содержащие, в числе прочих условий, процедуры безопасности использования интернет-банкинга и порядок защитных действий от несанкционированных платежей.

Но в силу информационной и договорной диспропорции и постоянно совершенствующих методов мошенничества, в частности, в области социальной инженерии, клиент интернет-банкинга не достаточно защищен от незаконных действий третьих лиц.

Для решения данной проблемы необходимы дополнительные меры защиты, как на уровне договора, так и на законодательном (нормативном) уровне, к примеру, утверждение перечня недобросовестных условий.

3 ПРОБЛЕМЫ ЗАЩИТЫ ПРАВ КЛИЕНТОВ ИНТЕРНЕТ-БАНКИНГА

3.1 Использование удаленной идентификации как способа защиты прав клиентов интернет-банкинга

Удаленная идентификация является неотъемлемой частью интернет-банкинга, благодаря которой клиенты банков могут дистанционно получать банковские услуги.

В настоящее время существуют 4 способа идентификации при оказании банком электронных банковских услуг (как платежных, так и информационных банковских услуг):

1) посредством электронной цифровой подписи (ЭЦП);

2) динамическая идентификация;

3) биометрическая идентификация;

4) уникальный идентификатор пользователя и пароль (для физических лиц) [18].

ЭЦП регулирует Закон РК «Об электронном документе и электронной цифровой подписи», определяя ее как «набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания» [35].

Согласно Правилам № 212 для получения электронных банковских услуг посредством ЭЦП клиенту требуется регистрационное свидетельство, выданное аккредитованным удостоверяющим центром РК или иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне РК.

Процедура аккредитации удостоверяющего центра (УЦ) – «официальное признание уполномоченным органом в сфере обеспечения информационной безопасности компетентности удостоверяющего центра в оказании услуг»по выдаче ЭЦП[35].

Уполномоченным органом в сфере обеспечения информационной безопасности в Казахстане является Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК, который осуществляет государственную услугу по аккредитации УЦ с февраля 2020 года.

На интернет-ресурсе www.gov.kz можно найти перечень аккредитованных УЦ [36].

Использование ЭЦП считается способом, обеспечивающим достаточно высокий уровень безопасности при использовании интернет-банкинга, так как она снижает риск ошибок со стороны банка в идентификации клиента, и соответственно, значительно снижает риск мошенничеств.

Стоит отметить, что ЭЦП больше практикуется среди клиентов-юридических лиц. Физическим лицам скорее всего использование ЭЦП не

совсем удобно: для того, чтобы зарегистрироваться в системе интернет-банкинга необходимо посетить офис банка для получения специального программного обеспечения на USB-флеш-накопителе, которое нужно установить на домашний компьютер.

Вместе с тем, ЭЦП нельзя назвать 100% безопасным способом идентификации способом идентификации, так как доступ к ЭЦП может быть в результате:

- действий или сговора работников юридического лица, имеющих доступ к ключам и аутентификационным данным вследствие недостаточных мер по парольной защите внутри компании;
- мошеннических действий третьих лиц путем взлома и заражения компьютера вредоносным программным обеспечением.

К примеру, в апреле 2016 года Специализированный межрайонный экономический суд Мангистауской области рассматривал дело по иску ТОО «П.» к АО «Нурбанк» [37].

Иск подан в связи с тем, что с расчетного счета ТОО «П.» в результате несанкционированного доступа в интернет-банкинг была списана сумма в размере 721 000 тенге и перечислена неизвестному физическому лицу.

В ходе заседания стало известно, что по заявлению директора ТОО «П-А» Национальным Банком была проведена проверка, в результате которой установлено, что платежи были проведены в соответствии с требованиями Закона РК «О платежах и переводах», поскольку электронный платежный документ был подписан ЭЦП клиента.

На судебном заседании директор ТОО «П.» пояснил, что при проведении проверки лицевого счета ТОО в системе «Интернет-банкинг» обнаружил платежное поручение на сумму 721 000 тенге с его ЭЦП. Поскольку не создавал и не подписывал данный документ, он немедленно позвонил в банк, однако банк сообщил, что платеж исполнен, и сумма перечислена в другой банк, в связи с чем, они не смогут произвести возврат денежных средств.

В судебном решении по данном делу сообщается, что возбуждено уголовное дело в отношении нескольких физических лиц, которые используя вредоносное программное обеспечение, покушались на хищение и совершили хищение денежных средств со счетов юридических и физических лиц, в том числе по факту хищения со счета ТОО «П.» суммы в размере 721 000 тенге в АО «Нурбанк».

Данное дело решено в пользу клиента, поскольку как указывает суд, ответчиком (банком) не представлены доказательства, подтверждающие, что истец разгласил, утратил носитель ключевой информации, использование ЭЦП истца лицами, не имеющими права давать распоряжение по счетам Клиента.

Авторы статьи [38] советуют при использовании ЭЦП «регулярно проверять компьютер на предмет заражения вирусами, применять антивирусные программы, не оставлять ключ электронной цифровой подписи подключенным к компьютеру, когда его не используют».

Второй, более распространенный способ идентификации в интернет-банкинге - динамическая идентификация - определяется правилами Национального Банка РК как «процедура установления личности клиента»путем использования одноразового (единовременного) кода с целью «однозначного подтверждения его прав на подписание заявления на открытие банковского счета и подписание договора банковского обслуживания» [39],«на получение электронных банковских услуг» [18].

Динамичной она названа в связи с тем, что требует постоянно меняющиеся одноразовые паролями для каждого сеанса работы в интернет-банкинге.

Согласно Правилам № 212 при динамической идентификации банк создает одноразовый (единовременный) код и направляет клиенту в соответствии с условиями договора, заключенного между ними.

К примеру, в Правилах банка одноразовый код (сеансовый ключ) формируется Системой Интернет-банкинг по запросу Клиента и направляется Банком в составе SMS-сообщения на номер телефона (используемого как логин) [40].

- банк обязан создавать новый одноразовый (единовременный) код для каждого доступа к электронным платежным услугам;
- банк обязан создавать новый одноразовый (единовременный) код при повторном доступе клиента к электронным платежным услугам.

Отличием биометрической идентификации является то, что она осуществляется не посредством использования одноразового пароля, а «на основе физиологических и биологических особенностей» [18] клиента.

Необходимо отметить, что биометрическая идентификация используется банками давно. Так, в статье [41]отмечают, что «HomeCredit Bank» собирает биометрические данные с 2015 года, с момента запуска терминалов cash-out (терминалы для снятия наличных денег), где имеется система отпечатков пальцев при снятии наличных. В них можно зарегистрировать до шести отпечатков пальцев и беспрепятственно снимать средства через эти аппараты. Банк сейчас удалённо предоставляет кредиты с получением денег на указанный счёт, открывает депозиты и счета, производит бесплатные переводы на карты любых банков РК и так далее.

Жилстройсбербанк идентифицирует клиента через видеозвонок. Во время видеоинтервью система Алтын банка распознаёт лицо из видеопотока и сравнивает его с фотографией на удостоверении личности, которое предоставил клиент».

В октябре 2020 года Национальный Банк РК запустил сервис удаленной биометрической идентификации для получения финансовых услуг через РГП «КЦМР НБРК», которая имеет доступ к фотоизображениям из государственной базы данных физических лиц.

С внедрением данного сервиса другие биометрические сервисы, предоставляемые коммерческими структурами и основанные на проведении сверки фотоизображений физических лиц, но не использующие эталонную

государственную базу данных, не соответствуют установленной Национальным Банком РК процедуре и утверждённым правилам.

Под утвержденными правилами понимаются Правила № 212, которые описывают процедуру биометрической идентификации. Она проводится в виде видеоконференции с клиентом либо путем использования технологий выявления движения клиента, после которой банк передает в центр обмена идентификационными данными (ЦОИД) индивидуальный либо бизнес-идентификационный номер клиента и видеоизображение клиента, полученное из сеанса видеоконференции либо с помощью технологии выявления движения интервьюируемого в процессе дистанционной идентификации.

ЦОИД посредством программного обеспечения определяет степень соответствия по биометрическим показателям фотоизображения, полученного из сеанса видеоконференции, и фотоизображения клиента из доступных источников. Видеозаписи обращений клиентов хранятся в банке[18].

Результаты степени соответствия по биометрическим показателям фотоизображений и идентификационные данные клиента, полученные ЦОИД из доступных источников, передаются в банк. Результаты степени соответствия хранятся в базе данных ЦОИД.

Согласно внутренним документам РГП «КЦМР НБРК»[42] результаты степени соответствия принимаются с совпадением 85% и выше. Банк в случае получения результате сличения менее 85% может сообщить о данном клиенте в правоохранительные органы, а также вправе включить клиента в базу «Мошенники» и проинформировать об этом РГП «КЦМР НБРК», которое, в свою очередь, добавляет видеоизображение к базе «Мошенники» и помещает информацию о попытке мошенничества в досье клиента.

Несмотря на то, что в Правилах № 212 предусматривается биометрическая идентификация только по фотоизображению, во внутренних документах РГП «КЦМР НБРК» указывается, что функционал данной системы будет расширяться.

В последующем планируется наряду с фотоизображением использование биометрических персональных данных: отпечатка пальца, голоса, радужной оболочки глаза, рисунка вен, которые будут сверяться с данными из накопленной базы данных.

Согласно пункта23-1 Правил РГП «КЦМР НБРК» в случае неуспешной биометрической идентификации клиента более двух раз банк проводит процедуру дополнительной проверки клиента в офлайн режиме либо отказывает клиенту в предоставлении услуг [43].

Среди преимуществ биометрической идентификации называют [44]:

«1) высокий уровень безопасности;

2) неотчуждаемость аутентификационных данных;

3) удобство использования».

Как указано выше, в настоящее время биометрическая идентификация в Казахстане проводится по фотоизображению. При этом не ясно, какие методы распознавания лица используются.

Так, биометрия лица может проводиться по геометрии лица (по чертам лица и форме черепа) и по термограмме (по расположению кровеносных сосудов и распределению температурных полей). Геометрия лица также делится на два направления: 2d – распознавание лица (более распространенное) и 3d распознавание лица (труднореализуемое направление) [44].

Несмотря на то, что биометрическая идентификация считается, что обладает самой высокой надежностью, но и этот способ нельзя считать панацеей от кибермошенников.

К примеру, мошенники в Китае с 2018 года обманывали государственную систему распознавания лиц. Они покупали фотографии в высоком разрешении и «оживляли» их в приложениях, создавая видео. В таких видео «лица кивают, моргают, двигаются и открывают рот» [45].

Как отмечается в статье [46] слабыми местами системы безопасности в части биометрических данных являются утечки данных, кражи цифровой личности, взлом базы данных, ложная идентификация. Автором приводятся примеры инцидентов. Так, в Индии в 2017 и 2019 годах произошли массовые утечки биометрических данных. В 2018 году хакеры продавали данные из системы биометрической идентификации Aadhaar. В 2017-м хакеры взломали сеть американской компании AvantiMarkets, в которой хранились биометрические данные клиентов организации. В качестве ложной идентификации есть факт применения штрафа к женщине, похожей на нарушительницу на 61% .

Для предотвращения рисков биометрической идентификации полностью согласна с автором статьи [46], что требуется «развитие соответствующей инфраструктуры, программного обеспечения, информационной безопасности и создание качественной правовой основы, чтобы можно было безопасно пользоваться этим механизмом».

Биометрическая идентификация не должна быть единственным способом идентификации в интернет-банкинге, так как ни один способ не дает 100% защиты, а должна использоваться в сочетании с другими способами идентификации.

Как отмечает регулятор в обзоре [47],в 2019 году вступила в действие директива Евросоюза PSD2, которая «содержит два ключевых элемента, имеющих особое значение – строгая идентификация клиентов (SCA) и появление двух типов новых регулируемых поставщиков платежей (поставщиков услуг по инициированию платежей и поставщики информации об учетной записи). В центре SCA – двухфакторная аутентификация т.е. клиент должен предоставить два разных вида подтверждающей информации. Это может быть то, чем он владеет (например, мобильный телефон), то, что он знает (пин-код или секретное слово), или то, что он есть (отпечаток пальца/идентификация лица)».

Это означает, что директива требует, чтобы банки обязательно использовали многофакторную аутентификацию при выполнении любых удаленных операций, и в процессе идентификации пользователя должны использоваться несколько способов подтверждения личности.

Вместе с тем, с учетом развития информационных технологий в настоящее время обсуждается возможность сочетания биометрических и блокчейн-технологий в процедурах идентификации клиентов.

Закон «Об информатизации» определяет блокчейн как информационно-коммуникационную технологию, обеспечивающую«неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования» [48].

Принцип работы блокчейна заключается в том, что хранение данных распределено по блокам, связанным определенными математическими алгоритмами, где каждый блок содержит ссылку на предыдущий блок и метку о времени и защищен криптографическим шифрованием. Главная особенность блокчейна – отсутствие централизации: информация хранится не на компьютерах одной организации (например, банка или государственного органа), а на тысячах компьютерах, не связанных единым владельцем или местом нахождения.

Эти особенности исключают возможность несанкционированного вмешательства в систему, вследствие чего использование технологии распределенного реестра характеризуется высоким уровнем безопасности и конфиденциальности данных, что способствует уменьшению мошенничества.

Таким образом, блокчейн-технология позволяет создать децентрализованную модель цифровой идентификации, в которой персональные данные, в том числе биметрические, надежно хранятся в распределенных базах данных.

Авторами статьи об идентификации личности с объединением блокчейн и биометрии для обеспечения безопасности персональных данных [49] предложена следующая схема такого внедрения:

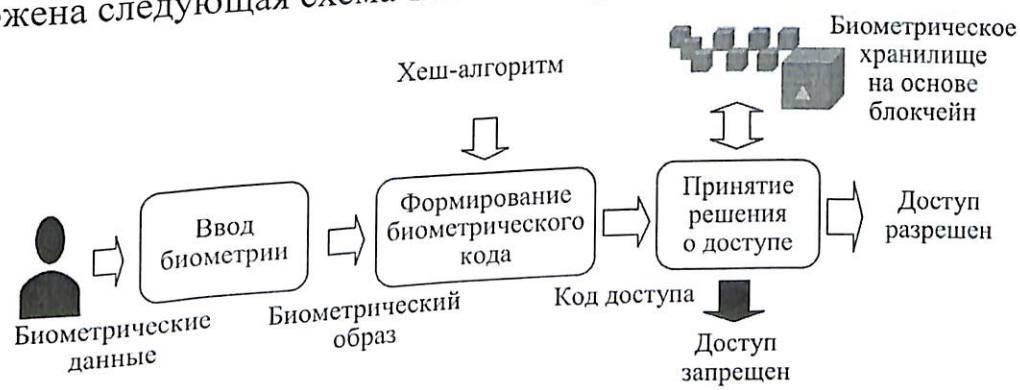


Рис. Схема биометрической аутентификации с использованием блокчейн-технологии

В зарубежной практике есть достаточно много примеров внедрения блокчейн-технологий в банковские процессы. Так, российский Альфа банк создал мобильное приложение совместно с разработчиками BlockNotary, которые ранее разработали блокчейн-решение для устранения проблемы соблюдения принципов «Знай своего клиента» и противодействия отмыванию преступных доходов. Суть технологии заключается в записи короткого онлайн-

интервью, последующей генерации хеш-видео и включения полученного хеша в блокчейн, после чего у сервиса есть идентификацинные данные клиента [50].

АКБ «РосЕвроБанк» в 2017 году сообщил о разработке системы удаленной идентификации клиентов на базе блокчейна, которая позволяет провести идентификацию с помощью данной технологии другим банкам в случае запроса клиентом РосЕвроБанка через его мобильное приложение услуг другого банка [51].

Стоит отметить, что такое внедрение возможно в случае нормативного закрепления в банковском законодательстве, а также законодательстве о защите персональных данных, что на данный момент отсутствует.

Национальным Банком разработан проект Программы создания Национальной платформы цифровой биометрической идентификации на 2021-2024 годы, в которой описаны уже работающие проекты за рубежом и отмечено, что объединение биометрии и блокчейн-технологии позволит создать решения для сохранения личности пользователя без потери контроля со стороны самого человека [52]. Однако согласно данной Программе внедрение блокчейна в казахстанскую систему цифровой идентификации пока не планируется, а выбрана федерализованная модель с несколькими организациями-провайдерами с использованием централизованной платформы.

Темпы развития цифровых технологий, а с ними и совершенствующие мошеннические методы в скором времени могут потребовать нормотворческой работы для возможности функционирования системы биометрической идентификации с использованием блокчейн-технологий.

Вместе с тем, данный вопрос требует тщательного изучения со стороны рисков, несмотря на то, что сторонники данной технологии настаивают на высоком уровне надежности, конфиденциальности, безопасности. Ни одна технология не может обеспечить абсолютную безопасность, и даже если данная технология препятствует несанкционированным вмешательствам в систему путем атак на базы данных, она не исключает риски, связанные с самим клиентом (недостаточные меры по хранению ключей, паролей, передача их социальным инженерам).

3.2 Защита персональных данных при использовании интернет-банкинга

Вопросы защиты персональных данных, в том числе при использовании интернет-банкинга, урегулированы нормами отраслевых законов (Законами РК «О персональных данных и их защите», «Об информатизации», Гражданским и Уголовным кодексами), а также нормами банковского законодательства, в частности, нормативными правовыми актами регулятора финансового рынка.

В реализацию Закона РК «О персональных данных и их защите» (далее – Закон о ПД) действуют нормативные акты Правительства (Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных от 03.09.2013 г. № 909 (далее – Правила № 909),

Правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач от 12.11.2013 г. № 1214), а также постановление Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 21.10.2020 г. № 395/ НҚ «Об утверждении Правил сбора, обработки персональных данных».

В соответствии с пункта 14 статьи 13 Закона о платежах «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» [13].

К числу нормативных правовых актов регулятора финансового рынка актов, регулирующих вопросы защиты персональных данных при использовании интернет-банкинга, относятся Правила № 212, устанавливающие порядок оказания электронных банковских услуг, постановление Правления Национального Банка от 27.03.2018 года за № 48 об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций (Требования) и Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

В частности, Правилами № 212 предусмотрено, что сеанс видеоконференции с клиентом проводится «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» [18].

Также устанавливаются 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» [18].

Утечка персональных данных, к которым относятся биометрические данные, логины, идентификаторы, пароли, которые используются для удаленной идентификации в интернет-банкинге, приводит не только к нарушению конфиденциальности личных данных клиентов, но и к хищениям с их банковских счетов. В этой связи, остро встает вопрос о необходимости обеспечения банком и его клиентами информационной безопасности.

Предлагаемые банком договоры, судебная практика, новости о мошеннических операциях с получением персональных данных побудили меня на проведение собственного простейшего «теста на проникновение» в мобильные приложения трех банков для понимания (не считается

профессиональным), насколько легко мошенникам получить доступ к интернет-банкингу, со следующими результатами:

1) в банке 1 для входа в мобильный банкинг «мошеннику», знающему Ф.И.О. и телефон клиента, потребовался только пароль из СМС, который он «выведал» с помощью методов социальной инженерии. Отмечаем, что ИИН, который также требовался для входа, «мошенник» может легко найти в интернете по Ф.И.О.;

2) в банке 2 «мошеннику» потребовалось «выведать» от жертвы 2 пароля из СМС, а также девичью фамилию матери. Дату рождения, которая содержится в ИИН, которую нужно было ввести для входа, «мошенник» также мог легко найти в интернете по Ф.И.О.;

3) в банке 3 «мошенник» должен был, помимо введения пароля из СМС, пройти видеоидентификацию, с выполнением команд банка «поверните голову направо», «поверните голову налево», «улыбнитесь».

Таким образом, с применением мошенниками продвинутых методов социальной инженерии клиенты банков 1 и 2 менее защищены от несанкционированного доступа в их личные кабинеты интернет-банкинга и соответственно, от потерь денег со счетов.

Клиентов банка 3 можно считать более защищенными, так как «мошенник» не смог пройти видеоидентификацию, и банк сообщил, что «не удалось распознать лицо».

Центр анализа и расследования кибератак (далее – ЦАРКА) в феврале 2020 года сообщил, что проблемы GDPR (акта Европейского союза по защите персональных данных) выявлены во всех банках – объектах исследования (26 банков) [53].

Согласно исследованию компании «Делойт» по оценке киберрисков банках Казахстана, проведенного в июне 2021 года, обзор веб-сайтов 24 казахстанских банков показал, что только 35% из них были приведены в соответствие с требованиями GDPR [54].

Экспертно-аналитический центр InfoWatch за период 2018 - 2020 годы зафиксировал 24 случая «компрометации конфиденциальной информации, повлекших более 11 млн.записей персональных и платежных данных», и.«более91% утечек в Казахстане связано с компрометацией персональных данных», из них на банки и финансы приходится 12,5% всех утечек [55].

В этой связи, возникают вопросы, насколько защищены персональные данные в Казахстане законодательно и как складывается правоприменительная практика по данной теме.

По мнению автора статьи риски интернет-банкинга в отношении персональных данных клиентов могут разделяться на внутренние и внешние, а также на пассивные и активные [56].

Внутренние риски связаны с действиями работников, имеющих доступ к персональным данным клиентов, а внешние риски связаны с действиями третьих лиц (мошенническими атаками).

Пассивные риски предполагают, что банк внедряет все меры по защите персональных данных, и несанкционированный доступ к счетам клиента происходит в отсутствие вины банка. 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.

Внешние, внутренние и активные риски могут быть снижены за счет нормативного регулирования (требованиями по информационной безопасности, ответственностью за неисполнение ном законодательства, а также внутренними документами самого банка).

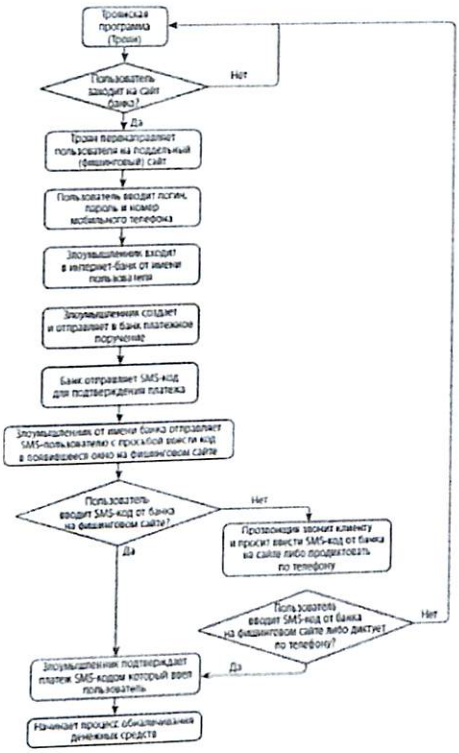
Необходимо отметить, что в соответствии с Правилами оценки уровня защищенности от угроз информационной безопасности, утвержденными Постановлением Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2020 г. № 110, банку для соответствия наивысшему уровню защиты от угроз информационной безопасности необходимо разработать более 20 внутренних документов (Политики информационной безопасности, перечня защищаемой информации, порядок работы с защищаемой информацией, создание бизнес-процессов и др.).

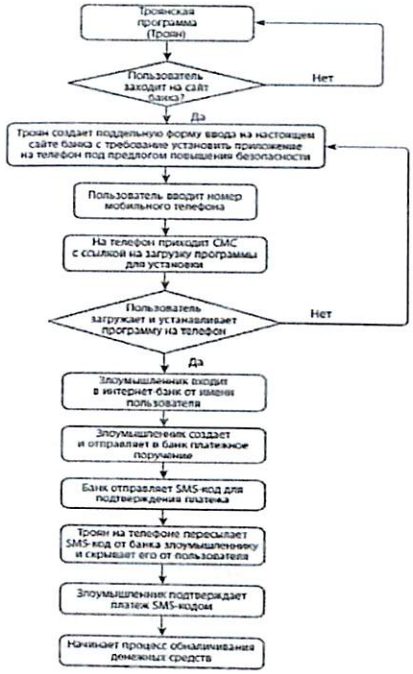
Правила № 909 устанавливают требования шифрования либо наличия защищенных каналов для передачи данных иным лицам; хранения данных с применением средств криптографической защиты информации; применения средств идентификации и (или) аутентификации пользователей при работе с этими данными [57].

Согласно Правил № 212 идентификация не проводится без аутентификации (установление подлинности) – процедуры подтверждения «подлинности и правильности составления электронного документа в соответствии с требованиями процедуры безопасности» [18].

Пассивные риски интернет-банка связаны с действиями самого клиента, а точнее, с действиями мошенников, которые атакуют не системы банка, а его клиента и/или устройства клиента.

Авторами книгио мошенничествах в платежной сфере [58] приведены несколько блок-схем хищений с банковских счетов клиентов с помощью троянской программы на компьютере и мобильном устройстве жертвы, в том числе с перенаправлением на фишинговые сайты и использованием методов социальной инженерии:





Пассивные риски в определенной мере могут устранить нормы, предусмотренные в договорах, заключаемых банками с клиентами, а также меры «самозащиты» клиента, требующие постоянной информационной работы банка с клиентами.

В качестве примера рассмотрим Стандартные условия предоставления банковских и иных услуг АО «Евразийский банк» (договор присоединения), размещенный на интернет-ресурсе банка [59].

Согласно данному документу для клиентов предусмотрено, что банк не несет ответственность:

- за несанкционированный доступ к Счетам/Дебетным и Кредитным Картам Клиента, в случае утери или передачи информации третьим лицам, содержащей банковскую тайну (пункт 10-2);
- за предоставление третьим лицам информации о проведении расходных операций по банковскому(-им) счету/счетам посредством SMS– оповещения, направленного на номер телефона, указанный в заявлении (пункт 92-7).

Отдельно предусмотрено, что клиент банка самостоятельно несет риск и ответственность в отношении раскрытия информации о Клиенте и его банковских счетах и Карте, остатках и движении денег на этих счетах и иных сведений, составляющих банковскую тайну лицам, получившим доступ к мобильному телефону (устройству/оборудованию) Клиента (пункт 183).

Таким образом, клиент банка при использовании интернет-банкинга не должен надеяться только на банк, а использовать защитные программы для усиления безопасности электронных платежей в Интернете и обеспечивать защиту своих персональных данных, логинов, паролей в интернет-банкинге.

В частности, в 2018 году имел место судебный процесс по иску АО «AltynBank» к гр-ну У.Е. Поводом для обращения в суд послужили следующие обстоятельства: ответчик У.Е. в рамках предоставления банком электронных услуг, в 2017 году становится клиентом банка, путём регистрации и соблюдения всех процедур банка, в том числе проведения интервьюирования и открытия личного банковского счёта [60].

Затем между истцом и ответчиком заключаются два договора банковского займа электронным способом, в рамках предоставления электронных банковских услуг.

Вместе с тем, выясняется, что У.Е. эти займы не получал, а получило их третье лицо Б.Ф., путём восстановления номера мобильного телефона, получения нового ЭЦП и подачи заявки через банковское приложение AltynaI, от имени У.Е.

По результатам рассмотрения суд удовлетворяет требования Банка о взыскании задолженности с У.Е., так как ответчиком не установлен факт незаконного использования данных ответчика и незаконном получении оспариваемого суммы кредита [60].

В 2019 году У.Е. подает иск о признании недействительными заключенных договоров банковского займа. Суд отказал в удовлетворении данного иска. Довод У.Е. об отсутствии выражения воли суд отнес к упущению самого истца, который не обеспечил сохранность своих персональных данных, логина и паролей, паролей и вход в личный кабинет, открытый в банке [61].

Данный судебное решение –далеко не единственное решение, в которых клиенты банков проигрывают. Положения договоров, заключенных между клиентом и банком, возлагающих полную ответственность на клиента за несанкционированный доступ к его счетам в интернет-банкинге, приводят к тому, что любые доводы и предположения о недостаточных мерах по обеспечению безопасности платежей со стороны банка суд не примет во внимание.

В этом и заключается проблема: в подобных судебных делах отсутствует анализ состояния информационной безопасности банка. Полностью согласна с исследованием судебной практики в России [29], что «распространенные в настоящий момент договоры банковского обслуживания перераспределяют риски таким образом, что реально банк не несет ответственности за совершение мошеннических платежей с использованием ДБО даже в тех случаях, когда банк допустил массу критичных нарушений.

Авторы настоящего исследования не могут назвать такую практику справедливой. Банк является квалифицированным участником рынка, разрабатывает и/или использует системы ДБО, применяет различные системы выявления фальсифицированных транзакций и пр. Таким образом, банк не в меньшей степени, чем клиент, имеет возможность предотвратить хищение. Однако сложившаяся практика не мотивирует банковское сообщество заниматься повышением уровня информационной безопасности своих систем и процессов» [29].

В целом в исследовании [29] отмечается, что«негативная практика для клиентов банка обусловлена сложностью доказывания причинно–следственной связи между действиями/бездействием банка и последствиями в виде хищения денежных средств. Если у клиента отсутствуют доказательства прямой вины банка, то решение выносится не в его пользу».

Вариантом решения данной проблемы могло бы стать запрашиваемое судом заключение регулятора либо проведение судебной экспертизы с целью выявления нарушений со стороны банка в части информационной безопасности. Как отмечено в моей статье, это «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» [62].

Данная проблема присутствует и за рубежом. Так, авторы статьи, посвященной проблемам защиты прав потребителей, использующих интернет-банкинг в Индонезии [63], пишут, что правовая защита банковских клиентов – проблема не только Индонезии.

Они провели сравнительное исследование в Малайзии жалоб банковских клиентов, связанных с кибербезопасностью, и отметили, что Ассоциация потребителей Пенанга (остров в Малайзии) сожалела о заявлении Ассоциации банков Малайзии, которая считала, что клиенты сами виноваты, что стали жертвами мошенников.

Данная Ассоциация также заявила, что ответственность за защиту своих активов и устройств лежит на клиентах. Ассоциация потребителей же ожидала, что банки будут нести ответственность за защиту активов клиентов.

Несмотря на безусловную необходимость мер самозащиты со стороны клиента, регулятору и банкам нельзя успокаиваться на этом, ограничиваясь регулярным напоминанием клиентам о рисках интернет-банкинга.

Регулятору и банкам необходимо разрабатывать меры по борьбе с социальной инженерией.

Данные вопросы поднимались в сессии 5 «Цифровая и информационная безопасность потребителей финансовых услуг» наVI Международной конференции«Территория финансовой безопасности 2021».

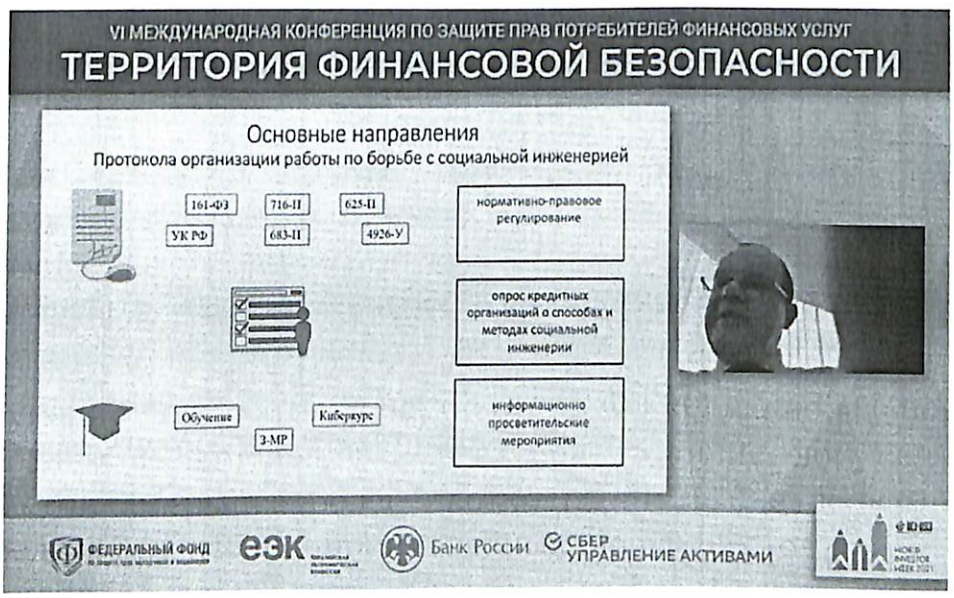
Представитель регулятора российского финансового рынка сообщил о направлениях работы Центрального банка РФ по борьбе с социальной инженерией:

1) повышение финансовой киберграмотности населения (меры оперативного предупреждения населения, образовательные программы);

2) совершенствование нормативно-правовой базы для решения проблемы социальной инженерии.

«Одной из важных задач сегодня стало создание условий, при которых банки будут заинтересованы в повышении качества антифрод-процедур. Регулятор в данный момент прорабатывает поправки в некоторые

регламентирующие документы, в частности, в ФЗ «О национальной платежной системе». Готовятся изменения в регламентирующие документы, которые позволят участникам рынка более плотно работать с цепочками по выводу денежных средств при несанкционированных операциях [64]:



Ассоциация банков «Россия» для борьбы с мошенническими переводами разработала проект поправок в Федеральный закон «О национальной платежной системе», которым предлагается следующее:

1) в случае уведомления клиента об оспаривании транзакции до зачисления на счет получателя, она приостанавливается;

2) в случае уведомления клиента об оспаривании транзакции после зачисления на счет получателя блокируются все расходные операции на карте получателя. Если получатель средств не предоставит подтверждающие транзакцию документы, то деньги будут возвращены отправителю средств [65].

Данные предложения не лишены недостатков, находятся на стадии обсуждения и доработки, вместе с тем, демонстрируют желание российских банков решить проблему социальной инженерии на законодательном уровне.

В Казахстане проблема социальной инженерии, необходимость ее решения на законодательном уровне пока, к сожалению, не поднимается.

Поэтому в первую очередь, данная проблема должны быть озвучена и необходимость ее проработки должна быть закреплена в государственных планах по борьбе с мошенничествами.

Далее необходима работа по разработке правовых способов противодействия методам социальной инженерии.

В этом направлении можно рассмотреть следующие предложения:

1) дополнить полномочия регулятора (Национального Банка РК) полномочием утверждения признаков сомнительных банковских операций, совершаемых через интернет, при выявлении которых банк обязан отменить, заблокировать или приостановить их совершение. Данные полномочия необходимо внести в статью 15 Закона РК «О Национальном Банке Республики

Казахстан» (перечень полномочий Правления Национального Банка) и статью 4 Закона о платежах (перечень полномочий Национального Банка в области платежей и платежных систем).

Признаки сомнительных банковских операций, совершаемых через интернет, в рамках указанного полномочия Национального Банка утвердить подзаконным нормативным правовым актом Национального Банка, и ккоторым, в частности, можно отнести совершение операций с изменением устройства, с которого осуществляется вход в интернет-банкинг/мобильный банкинг, и/или номера телефона и/или в случае получения уведомления клиента о несанкционированном платеже в течение определенного количества рабочих (операционных) дней;

2) к имеющейся законодательной обязанности банка обеспечивать выполнение процедур безопасности от несанкционированного платежа предусмотреть внедрение антифрод систем, анализирующих поведение клиента.

Система фрод-мониторинга может стать одним из эффективных банковских методов для обнаружения мошеннических операций. Автор статьи [66] пишет, что «идея такого мониторинга состоит в том, что для каждого клиента собирается и формируется его финансовый портрет, и если поведение держателя карты вдруг отличается от шаблонного, то можно говорить о вероятной мошеннической операции, после чего транзакция приостанавливается, и сотрудник банка связывается с держателем карты для подтверждения проведения платежа или перевода».

Здесь следует отметить, что сотрудник банка не должен связываться с клиентом, так как именно мошенники чаще всего представляются работниками банка. Более правильный подход у Сбербанка России, который внедрил антифрод систему, использующую искусственный интеллект: в случае нетипичных действий по карте операция автоматически блокируется, о ней оповещаются сотрудники центра безопасности, а клиента или мошенника «просят» клиента или мошенника связаться с call-центром банка для уточнения деталей [67].

Оказывается, искусственный интеллект, используемый в антифрод системе, анализирует более ста метрик, которые позволяют «определять мошеннические действия с точностью в 96-97%» [67].

По вопросу внедрения искусственного интеллекта, нельзя не упомянуть в целом складывающуюся мировую тенденцию развития уже «интеллектуального» дистанционного банковского обслуживания.

Искусственный интеллект находит широкое применение в различных банковских сервисах, а в борьбе с мошенничеством в интернет-банкинге может стать эффективным инструментом. Например, в Швеции разработана система, которая идентифицирует личность по особенностям набора букв и цифр на клавиатуре, что позволяет выявить мошенников, пытающихся выдать себя за банковских клиентов[68]. И как следствие применения искусственного интеллекта возникает вопрос необходимости его правового регулирования. И если в настоящее время пока механизмы регулирования искусственного

интеллекта в финансовой сфере не ясны, данный вопрос уже требует отдельного внимания и изучения и станет следующим этапом в научно-исследовательской и правоприменительной деятельности.

Для возможности функционирования антифрод систем в казахстанских банках, необходимо обязать их на законодательном уровне. Данную обязанность банков предлагается предусмотреть в пункте 4 статьи 56 Закона РК «О платежах и платежных системах, изложив его в следующей редакции:

«4. Банк, организация, осуществляющая отдельные виды банковских операций, или отправитель денег при осуществлении платежей с помощью средств электронных платежей обеспечивают выполнение процедур безопасности от несанкционированных платежей, в том числе предусматривающих внедрение системы противодействия мошенничеству (антифрод системы), анализирующей поведение клиента (характер, объемы и параметры совершаемых клиентом операций)».

Если перейти к способам самозащиты клиентов для предотвращения несанкционированного доступа к системам интернет-банкинга и краж со счетов, то таковыми являются:

«неразглашение конфиденциальной, аутентификационной информации;

использование только лицензионного ПО, а также обязательная установка обновлений ПО, ОС для минимизации эксплуатации уязвимостей;

использование расширенных функций системы ДБО, таких как SMS-OTP/Push-OTP уведомлений;

регулярная смена паролей к системе ДБО и устройствам с которой происходит работа в системе ДБО;

ограничение программной среды для использования системы ДБО, например, выделение отдельного ноутбука для использования только системы ДБО;

оперативная блокировка доступа к системе ДБО, либо к банковской карте, если появились подозрения на действия мошенников, поступают подозрительные звонки, приходят SMS-сообщения подозрительного содержания, был установлен факт утери устройства, с которого происходила работа с системой ДБО либо банковской карты, либо установлен факт компрометации аутентификационных данных к системе ДБО, банковской карты» [69].

Как отмечается в Стратегии [2] нормативное правовое обеспечение вопросов кибербезопасности казахстанского финансового рынка существенно отстает от текущих потребностей. Также в ней говорится, что «есть недостатки в области обязательного контроля и надзора за финансовыми организациями в части обеспечения кибербезопасности предоставляемых ими услуг.

Так, требования Закона Республики Казахстан от 4 июля 2003 года «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» не предусматривают меры по надзору и контролю кибербезопасности в финансовых организациях. Отсутствуют меры и

механизмы воздействия на финансовые организации в случае несоблюдения ими требований по кибербезопасности» [2].

Поэтому Агентство по регулированию и развитию финансового рынка и Национальный Банк планируют продолжать работу в части совершенствования регулирования кибербезопасности финансовых организаций в целях усиления контроля и обеспечения кибербезопасности как финансовых организаций с низким уровнем защищенности, так и в целом финансового рынка, что в свою очередь, повысит и защищенность клиентов при получении ими услуг посредством интернет-банкинга.

Таким образом, следует заключить, что вопросы удаленной идентификации и защиты персональных данных при использовании интернет-банкинга достаточно урегулированы законодательством Республики Казахстан.

Дальнейшее совершенствование законодательства, регулирующего вопросы интернет-банкинга, должно развиваться как в части принятия мер банками по повышению осведомленности клиентов о рисках дистанционных банковских услуг, так и в части повышения и усиления информационной безопасности банков, а также в части разработки правовых способов борьбы с социальной инженерией.

ЗАКЛЮЧЕНИЕ

В данном диссертационном исследовании проведен комплексный анализ правового регулирования интернет-банкинга в Казахстане правового регулирования интернет-банкинга как в части нормативного регулирования, анализа договора на оказание электронных банковских услуг, так и в части защиты прав клиентов интернет-банкинга в связи с повышенными рисками информационной безопасности и защиты персональных данных.

В результате данного анализа рассмотрены понятия интернет-банкинга, электронных банковских услуг, их соотношения между собой, изучены особенности договора на предоставление электронных банковских услуг, а также нормативная база интернет-банкинга и полномочия государственных органов в регулировании электронной банковской деятельности. Такжеособый акцент сделан на изучении вопросов защиты прав клиентов интернет-банкинга.

Сделаны следующие выводы в результате диссертационного исследования:

1) в целом вопросы правового регулирования интернет-банкинга подробно урегулированы нормативными правовыми актами различного уровня, которые представлены как общими нормами гражданского и банковского законодательства, так и специальными нормами, содержащимися в подзаконных нормативных правовых актах Правительства РК, Национального Банка РК и Агентства РК по регулированию и развитию финансового рынка;

2) договор на оказание электронных банковских услуг является договором присоединения, двусторонним, консенсуальным, бессрочным и не публичным, и в силу данных особенностей на практике имеются проблемы информационной и договорной диспропорции;

3) клиенты банка, являясь слабой стороной договора на оказание электронных банковских услуг, заключаемого путем присоединения к стандартным формам банков, недостаточно защищены в случаях денежных потерь из-за мошеннических действий третьих лиц;

4) в связи с развитием цифровых технологий необходима постоянная нормотворческая работа над усилением безопасности интернет-банкинга.

Данная работа должна проводиться в двух направлениях: техническом (совершенствование мер информационной безопасности банков) и социальном (информационная работа с потребителями финансовых услуг, устранение договорной диспропорции, повышение финансовой киберграмотности, борьба с социальной инженерией). Обязательным пунктом социального направления должно стать изучение методов социальной инженерии и разработка правовых способов борьбы с ней, в том числе с использованием зарубежного опыта;

5) необходимо постоянное всестороннее изучение новых технологий, таких как блокчейн, искусственный интеллект, машинное обучение, на предмет возможности внедрения в системы удаленного доступа банков для повышения их безопасности.

В результате исследования разработаны конкретные предложения в законодательные акты и подзаконные нормативные правовые акты, конечной целью которых является защита клиентов интернет-банкинга от денежных потерь из-за мошеннических действий третьих лиц.

Регуляторам рекомендовано осуществлять постоянную работу по сбору, обработке и анализе информации о несанкционированных платежах, изучать международный опыт регулирования функционирования интернет-банкинга и внедрять в свою регуляторную деятельность.

Выработаны также рекомендации для судов при рассмотрении дел, связанных с интернет-банкингом, рассматривать их с учетом того, что клиент является слабой стороной договора на оказание электронных банковских услуг и не обладает профессиональными знаниями по информационной безопасности. В этой связи, нельзя возлагать полную ответственность на клиента за несанкционированные платежи, и данные условие в договоре необходимо считать недобросовестным и ничтожным. Кроме того, судам рекомендуется запрашивать заключение регулятора либо проведение судебной экспертизы с целью выявления нарушений со стороны банка в части информационной безопасности.

Результаты проведенного исследования могут быть использованы при разработке изменений в законодательство, регулирующее вопросы электронных банковских услуг, а также акцентируют внимание на необходимости внедрения новых подходов к банковскому регулированию с учетом не только технических вопросов информационной безопасности, но и с учетом особенностей психологии человека.

Полученные выводы и рекомендации могут представлять интерес для юристов, работников банков, банковских аналитиков, судов общей юрисдикции и арбитражей.

Результаты диссертации могут быть использованы в дальнейших научных исследованиях указанной проблемы и при преподавании гражданского права, обязательственного права, финансового и банковского права, информационного права и киберправа.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Концепция повышения финансовой грамотности на 2020 – 2024 годы, утвержденная Постановлением Правительства РК от 30 мая 2020 года № 338 //САПП Республики Казахстан 2020 г., № 20-21 ст. 174

2. Сведения и материал с сайта: Стратегия кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы, утвержденная постановлениями Правления Агентства РК по регулированию и развитию финансового рынка № 69 от 20 июля 2020г. и Правления Национального Банка РК № 89 от 20 июля 2020г., https://finreg.kz/?docid=3550&switch=russian

3. Сведения и материал с сайта: А. Мамин провел заседание МВК по профилактике правонарушений https://primeminister.kz/ru/news/a-mamin-provel-zasedanie-mvk-po-profilaktike-pravonarusheniy-17105437

4. Сведения и материал с сайта: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств | Банк России http://www.cbr.ru/analytics/ib/review_3q_2021/#highlight=обзор

5. Сведения и материал с сайта: Кибербезопасность 2021-2022. Тренды и прогнозы https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2021-2022-trendy-i-prognozy/#id7

6. Дьякова, О. Н. История развития системы дистанционного банковского обслуживания / О. Н. Дьякова // Психология. Экономика. Право. – 2014. – № 4. – С. 68-76.

7. Сведения и материал с сайта: Горожанкин К. «Один в банке ночью… (Обзор казахстанского рынка банковских услуг)» https://lyakhov.kz/iguide/05/ibanking.shtml

8. Правила представления сведений о платежных услугах, утвержденные Постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 213 //Эталонный контрольный банк НПА РК в электронном виде, 08.11.2016

9. Серова, Л. А. Электронная банковская деятельность / Л. А. Серова // Цифровая экономика и финансы: Материалы III Международной научно-практической конференции, Санкт-Петербург, 19–20 марта 2020 года / Под научной редакцией Е.А. Синцовой [и др.]. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2020. – С. 425-429.

10. Гайзатуллин Р. Р., Гараев З. Ф. К вопросу о категории электронной банковской услуги как предмете исследования //Вестник Казанского технологического университета. – 2013. – Т. 16. – №. 11. – С. 272-277.

11. Нарыжная, Н. Ю. Что такое интернет - банкинг? / Н. Ю. Нарыжная, С. В. Белич // Информация как двигатель научного прогресса : сборник статей Международной научно-практической конференции, Волгоград, 25 января 2019 года. – Волгоград: Общество с ограниченной ответственностью "Аэтерна", 2019. – С. 79-80.

12. Барыло Е. В., Шакирова К. В., Зяблицкая Н. В. Развитие дистанционного банковского обслуживания. Сравнительная характеристика Интернет-банкинга

и мобильного банкинга //Региональные проблемы преобразования экономики. – 2020. – №. 6 (116). – С. 101-109.

13. Закон РК «О платежах и платежных системах» //Казахстанская правда от 10 августа 2016 г.

14. Правила предоставления банками второго уровня и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденные постановлением Правления Национального Банка РК от 28 марта 2008 года № 18 //Юридическая газета от 23 мая 2008 г.

15. Правила предоставления банковских услуг и рассмотрения банками, организациями, осуществляющими отдельные виды банковских операций, обращений клиентов, возникающих в процессе предоставления банковских услуг, утвержденные постановлением Правления Национального Банка РК от 28 июля 2017 года № 136 //Эталонный контрольный банк НПА РК в электронном виде, 07.09.2017

16. Кулаков Н. В., Адамов Н. А. 2.1. Понятийная основа банковских услуг //Курс развития России в новых экономических условиях. – 2017. – С. 2-2.

17. Сведения и материал с сайта: Общие условия соглашения о предоставлении электронных банковских услуг https://app.forte.kz/media/documents_translations/1/61b1bec23a86b.pdf

18. Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденных постановлением Правления Национального Банка РК от 31 августа 2016 года № 212 // Казахстанская правда от 04 апреля 2017 г.

19. Ермакова Е. П., Фролова Е. Е. Правовое регулирование цифрового банкинга в России и зарубежных странах (Европейский союз, США, КНР) //Вестник Пермского университета. Юридические науки. – 2019. – №. 46. – С. 606-625.

20. Фролова Е. Е. Правовое регулирование интернет-банкинга в Индии //Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2019. – Т. 23. – №. 3. – С. 351-374.

21. Гражданский кодекс Республики Казахстан (Особенная часть) //Казахстанская правда от 17 июля 1999 г.

22. Сведения и материал с сайта: ДОГОВОР ПРИСОЕДИНЕНИЯ использования услуг Финансового портала Homebank https://halykbank.kz/storage/app/media/Documents%202020/Other%20FL/RUS_Dogovor.pdf

23. Правила открытия, ведения и закрытия банковских счетов клиентов, утвержденные постановлением Правления Национального Банка РК от 31 августа 2016 года № 207//Эталонный контрольный банк НПА РК в электронном виде, 29.11.2016

24. Фогельсон Ю. Б. Защита прав потребителей финансовых услуг/МД Ефремова, ВС Петрищев, СА Румянцев и др.; отв. ред. ЮБ Фогельсон //М.: Норма, Инфра. – 2010 – 368 с.