Список использованной литературы:

1. Хартия основных прав Европейского Союза; Европейский Союз; Хартия, Международный документ от 07.12.2000. URL: http://eulaw.ru/treaties/charter.
2. Договор о Европейском Союзе; Европейский Союз; Договор, Международный документ от 07.02.1992. URL: http://eulaw.ru/treaties/teu.
3. Договор о функционировании Европейского Союза; Европейский Союз; Договор, Международный документ от 25.03.1957. URL: http://eulaw.ru/treaties/tfeu.
4. Государство, религия, светское общество и права человека, Рекомендация ПАСЕ 1804 (2007). URL: http://www.coe.int/t/r/parliamentary_assembly/[russian_documents]/[2007]/%5BJuin 2007%5D/Rec1804_rus.asp.
5. О сектах и новых религиозных движениях, Рекомендация ПАСЄ 1178 (1992) // Общественная организация «Союз защиты семьи и личности». URL: https://www.sites.google.com/site/fppungoru/zakonodatelstvo/dokumenty-pase-i-es/rekomendaciaparlamentskoieradievropino11781992-1.
6. О незаконной деятельности сект, Рекомендация ПАСЄ 1412 (1999). URL: https://lib.sale/prava-cheloveka-pravo/rekomendatsiya-1412-1999-parlamentskoy-77948.html.
7. Религия и перемены в Центральной и Восточной Европе, Рекомендация ПАСЄ 1556 (2002). URL: https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2002]/[Avril2002]/Rek_1556.asp#TopOfPage.
8. Рекомендации на встрече ОБСЕ по свободе религии и вероисповедания в Вене 17-18 июля 2003 г. URL: http://www.religare.ru/2_6004.html.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Луценко Виктория Владимировна – аспирант кафедры социальной и гуманитарной политики Национальной академии государственного управления при Президенте Украины

INFORMATION ABOUT THE AUTHOR

Lutsenko Viktoriya Vladimirovna – Postgraduate Student at the Department of Social and Humanitarian Policy of National Academy of Public Administration under the President of Ukraine

L_vika17@ukr.net

УДК 347.73

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЛАТЕЖЕЙ КАК ГАРАНТИЯ БЕСПЕРЕБОЙНОГО ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНЫХ СИСТЕМ

Мария ПОЖИДАЕВА,
кандидат юридических наук, доцент,
доцент кафедры финансового права учебно-научного института
«Юридический институт
Государственного высшего учебного заведения
«Киевский национальный экономический университет
имени Вадима Гетьмана»

АННОТАЦИЯ

В статье рассматриваются особенности правового обеспечения безопасности платежей, в том числе и система защиты информации, которая циркулирует в платежных системах. На основе анализа законодательства Украины, международных стандартов, правил платежных систем предлагается целостное восприятие правового обеспечения безопасности платежей как гарантии надежности платежной системы.

Ключевые слова: безопасность платежей, платежная система, политика информационной безопасности, правила платежной системы.

LEGAL SECURITY OF PAYMENTS AS THE GUARANTEE OF CONTINUING FUNCTIONING OF PAYMENT SYSTEMS

Maria POZHYDAEVA,
Candidate of Juridical Sciences, Associate Professor, Associate Professor
of the Financial Law Department
in Kyiv National Economic University named after Vadym Getman

SUMMARY

The article deals with features of legal security of payments, including information protection system, that circulates in payment systems. Based on the analysis the legislation of Ukraine, international standards, rules of payment systems the holistic perception legal security of payments have been proposed for the guarantee of payment system reliability.

Key words: payment security, payment system, information security policy, payment system rules.

Постановка проблемы. В условиях всеобъемлющей цифровой трансформации, активной интеграции информационных технологий во все проявления социально-политической и экономической жизни общества вопросы безопасности по внедрению и использованию тех или иных инноваций требуют особенного внимания и соответствующей правовой регламентации.

К сожалению, в ходе диджитализации чем стремительнее развивается платежная сфера, жизненно необходимая для осуществления оплаты товаров, работ, услуг, тем изощреннее становятся схемы мошенничества, учащаются случаи несанкционированного доступа к данными платежных карт, а также осуществления незаконных платежных операций. Наряду с этим в финансовом секторе увеличивается количество рисков кибератак, мотивированных интересами отдельных государств, групп и лиц. Итак, на фоне усиления угроз и киберрисков появляются новые вызовы правовому обеспечению безопасности платежей.

Актуальность темы исследования состоит в том, что эффективное правовое обеспечение высокого уров-

ня безопасности денежных переводов, электронных и мобильных платежей как с помощью платежных карт, так и без них, а также сохранности клиентских денег способствует популяризации безналичных расчетов и уходу от использования наличных денег.

Как справедливо предусматривает украинский законодатель, обеспечение безопасности платежей достигается путем обязательного внедрения и использования соответствующей системы защиты, которая состоит из:

1) законодательных актов Украины и других нормативно-правовых актов, а также внутренних актов субъектов перевода, которые регулируют порядок доступа и работы с соответствующей информацией, а также ответственность за нарушение этих правил;

2) мероприятий охраны помещений, технического оборудования соответствующей платежной системы и персонала субъекта перевода;

3) технологических и программно-аппаратных средств криптографической защиты информации, обрабатываемой в платежной системе (см. п. 38.4 ст. 38 Закона Украины «О платежных системах и переводе денег в Украине» от 05.04. 2001 г.).

Состояние исследования. В отечественной научной литературе наработан определенный массив проблематики, посвященный тем или иным аспектам безопасности платежных систем, отдельным вопросам защиты информации в платежных системах, в том числе инновационным технологиям защиты электронных трансакций. Однако можно констатировать недостаток исследований по данной проблематике в юридической науке. В финансовом праве и информационном праве вопросы безопасности осуществления платежей не были комплексно исследованы, что затрудняет целостное восприятие правового обеспечения безопасности платежей как гарантии надежности платежной системы.

Отдельные вопросы безопасности платежных систем, организации мер по обеспечению безопасности в банковской системе анализировали в своих научных работах Е.А. Алисов, А.В. Иванкевич, Т.Т. Ковальчук, З.Р. Костак, В.И. Мазур, Н.М. Рущишин, И.О. Трубин, Т.А. Чернадчук и др.

Целью и задачей статьи является анализ законодательства Украины, международных стандартов, правил платежных систем в Украине, которые в целом предусматривают меры по обеспечению безопасности осуществления платежей как в торговой сети, так и сети Интернета, а также регулируют порядок доступа и работы с соответствующей платежной информацией. При этом раскрытие особенностей правового обеспечения безопасности электронных и мобильных платежей, проведения безналичных расчетов с помощью использования платежных карт, в том числе и системы защиты информации, которая циркулирует в платежных системах, является необходимым в достижении главной цели – защиты публичных финансовых интересов от внешних и внутренних угроз в платежном пространстве.

Изложение основного материала. Безопасность при осуществлении платежных операций является одной из главных составляющих надежной платежной системы и основой доверия со стороны пользователей платежных услуг. В то же время надлежащий уровень защиты платежной системы можно считать показателем стабильности данной системы в случае внешних воздействий разного характера.

Анализируя п. 38.5 ст. 38 Закона Украины «О платежных системах и переводе денег в Украине», следует сделать вывод, что для безопасности платежей важной является сама система защиты информации, которая должна обеспечивать:

1) целостность информации, которая передается в платежной системе, и компонентов платежной системы, что означает их существование в неискаженном виде (неизменном по отношению некоторого фиксированного их состояния);

2) конфиденциальность информации во время ее обработки, передачи и хранения в платежной системе, что указывает на необходимость применения ограничений круга субъектов, имеющих доступ к данной информации, и сохранения указанной информации втайне от субъектов, не имеющих полномочий на право доступа к ней;

3) невозможность отказа инициатором от факта передачи и получателем от факта принятия документа на перевод, документа по операциям с применением средств идентификации, документа на отозвание;

4) обеспечение постоянного, своевременного и беспрепятственного доступа к компонентам платежной системы лицам, имеющим на это право или полномочия, определенные законодательством Украины, а также установленные договором;

5) наблюдаемость с помощью автоматизации, контроля управления доступом, мониторинга и др. способами для фиксации деятельности идентифицированных пользователей и процессов платежной системы.

Как справедливо отмечает Е.А. Алисов, режим функционирования и технологические регламенты работы платежных систем должны предусматривать вопросы обеспечения их информационной безопасности [1, с. 125]. Итак, в соответствии с п. 38.3 ст. 38 Закона Украины «О платежных системах и переводе денег в Украине» необходимо сделать акцент на особенностях определения первоочередности нормативно-правовых и правоприменительных актов в сфере регулирования порядка защиты информации в платежных системах в зависимости от их территориального значения (пространственного измерения). Таким образом, порядок защиты и использования средств защиты информации участниками именно международных платежных систем, в первую очередь, регулируется правилами этих систем, а уже в случае отсутствия в таких правилах соответствующих положений – тогда законами Украины и нормативно-правовыми актами Национального банка Украины (далее – НБУ). При этом законодатель установил, что общий порядок защиты и использования средств защиты информации по переводу денежных средств определяется законами Украины, нормативно-правовыми актами НБУ и правилами платежных систем.

Также следует отметить, что вопрос безопасности платежей может возникать и при их возможном осуществлении как в особый период, так и чрезвычайных ситуациях в стране/странах. В частности, обобщая нормы ст. 1 Закона Украины «Об обороне Украины» от 06.12.1991 г., под особым периодом может рассматриваться период мобилизации или введения военного положения в Украине (в отдельных ее местностях). В связи с этим в свое время Правление НБУ приняло ряд нормативно-правовых актов, среди которых следует выделить такие

постановления, как «Об утверждении Положения о межбанковском переводе средств в Украине в национальной валюте в особый период» от 23.12.2003 г. № 576, «Об утверждении Положения о порядке осуществления безналичных расчетов в национальной денежной единице Украины в особый период» от 23.12.2003 г. № 577 и др. Данные акты определяют возможность осуществления безналичных расчетов в особый период в порядке, установленном центральным банком с учетом предусмотренных законодательством ограничений. И в то же время НБУ отождествляет установление особого периода с фактом наступления обстоятельств непреодолимой силы (см. п. 1.7 главы 1 постановления Правления НБУ от 23.12.2003 г. № 577), что не соответствует общепринятому правовому пониманию непреодолимой силы как природных явлений.

Продолжая анализ нормативно-правовых актов НБУ в сфере обеспечения безопасности платежей, следует заметить, что наряду с особым периодом отдельно выделяется и понятие чрезвычайной ситуации. В пп. 15 п. 1 раздела II постановления НБУ «Об утверждении Положения о надзоре (оверсайте) платежных систем и систем расчетов в Украине» от 28.11.2014 г. № 755 под чрезвычайной ситуацией рассматриваются причины и обстоятельства, составляющие угрозу для непрерывности деятельности платежной системы: экономический кризис, террористический акт, природные катастрофы (землетрясения, оползень, обвал, сель, цунами, лавина, наводнение, смерч, засуха, заморозки, гроза, природный пожар), техногенные катастрофы и аварии (взрыв, пожар), массовые беспорядки, сбои в поставках электроэнергии и т.д.

Итак, для обеспечения беспрерывной деятельности платежной системы в чрезвычайной ситуации платежная организация данной системы обязана разработать и утвердить план соответствующих мероприятий, направленных на поддержание технологий выполнения платежных операций в чрезвычайных условиях, в том числе и в случае отказа/сбоя работы телекоммуникационных сетей и/или отдельных составляющих программно-технического обеспечения, а также на восстановление беспрерывности проведения платежей. На основании изложенного выше можно сделать вывод, что бесперебойное, а следовательно, и безопасное функционирование платежной системы обеспечивает ее использование для расчетов с минимальным риском. Поскольку правила любой платежной системы также предусматривают положения о системе управления в ней рисками (правовым, финансовыми, расчетным, операционным, системным), механизме контроля, минимизации и устранения последствий воздействия рисков, возникающих в платежной системе (см. раздел VII постановления Правления НБУ от 28.11.2014 г. № 755).

В Украине органы руководства платежной организации значимой платежной системы обязаны назначить лицо (лиц) и / или подразделение (ия), ответственного (ых) за управление рисками и обеспечения информационной безопасности в платежной системе, и осуществлять надзор за его деятельностью (см. п. 5 раздела V постановления Правления НБУ от 28.11.2014 г. № 755). Следует указать, что при передаче электронной платежной информации для проведения трансакции средствами телекоммуникационной связи такие данные должны быть зашифрованы согласно требованиям соответствующей платежной системы, а при их отсутствии–всоответствииизаконамиУкраины и нормативно-правовыми актами НБУ (см. п. 38.2 ст. 38 Закона Украины «О платежных системах и переводе средств в Украине» от 05.04.2001 г.).

Для предотвращения и противодействия внутренним и внешним угрозам информационной безопасности при осуществлении электронных и мобильных платежей каждая платежная организация в правилах работы своей платежной системы должна предусмотреть политику информационной безопасности с помощью реализации комплекса организационных мероприятий и программно-технических средств, которые обеспечивают надежную защиту информации на каждом звене организационной и технологической инфраструктуры системы. При этом участники платежной системы обязаны выполнять установленные внутренними нормативными документами требования по обеспечению защиты информации, которая принимается и обрабатывается в системе, а также несут ответственность в случае нарушения данных требований в соответствии с указанными выше правилами платежной системы и условий договоров.

Следует отметить и тот факт, что описанию обязательных компонентов системы защиты информации в платежной системе посвящен пп. 15 п. 2 раздела II постановления Правления НБУ «Об утверждении Положения о порядке регистрации платежных систем, участников платежных систем и операторов услуг платежной инфраструктуры» от 04.02.2014 г. № 43. Также в свое время НБУ были разработаны рекомендации по составлению правил платежной системы, в т. ч. и п. 11 по обеспечению ее информационной безопасности, платежной организацией которой является резидент, и размещены на официальной странице центрального банка государства [2].

В то же время требует внимания не только соответствие системы защиты информации определенной платежной системы национальному законодательству, но и международным стандартам обеспечения безопасности платежей, среди которых следует выделить ряд общепринятых стандартов-требований в сфере безопасности обращения платежных карт. Данные международные стандарты разработаны и поддерживаются Советом по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC), который был учрежден международными платёжными системами Visa, MasterCard, American Express, JCB и Discover [3]. Например, каждая организация, которая принимает, обрабатывает, передает или хранит данные платежных карт на своем сайте, должна полностью соответствовать требованиям международного стандарта PCI DSS (Payment Card Industry Data Security Standard) безопасности данных индустрии платежных карт, о чем свидетельствует значок сертификата PCI DSS на ее интернет-странице. При этом организации, задействованные в процессе хранения, обработки и передачи данных, ежегодно проходят сертификацию безопасности согласно этому стандарту.

Не менее важными для безопасности онлайн-платежей являются современные криптографические протоколы защиты информации для передачи за-

шифрованных данных в сети. Сегодня это протокол TLS (Transport Layer Security), основанный на протоколе SSL (Secure Sockets Layer), дальнейшим развитием и обновлением которого занимается международное сообщество IETF (Internet Engineering Task Force), Инженерный совет Интернета [4]. Таким образом, сайты платежных провайдеров, использующие протокол TLS/SSL и потверждающие это определенным сертификатом, обеспечивают безопасное соединение и зашифровывают информацию о данных платежных карт, шифр которых взломать невозможно.

Также платежными системами в Украине для обеспечения безопасности платежей активно испльзуются такие технологии международных стандартов, как 3d Secure, токенизация и др. Технология 3d Secure позволяет максимально достоверно подтвердить, что именно этот пользователь совершает данный платеж с помощью пароля, который меняется при совершении каждой новой платежной операции путем его доставки СМС-сообщением. В международных платежных системах услуга такой проверки называется Verified by Visa и Mastercard SecureCode, что отображается соответствующим значком на сайте участника платежной системы.

Технология токенизации делает безопасными электронные платежи с помощью шифрования данных платежной карты в токен, который выглядит как случайная комбинация символов и, попадая в терминал торговца, транслируется по сети в банк для подтверждения платежа. Эта технология используется для интернет-трансакций и платежей в обычных магазинах с помощью смартфонов [5].

В последнее время у международных платежных систем распространенным и востребованным в виде платформы для защиты электронных платежей становится технология Point-to-Point Encryption (P2PE) [6]. Данный международный стандарт PCI P2PE (Payment Card Industry Point-to-Point Encryption) содержит требования к решениям, поддерживающим особый алгоритм шифрования данных платежных карт, который обеспечивает надежный обмен платежной информацией между торгово-сервисным предприятием, где находится POS-терминал, и банком-эквайером. В Украине для внедрения этого стандарта платежным системам необходимо усовершенствовать свои технологии решений вопросов, связанных с защитой информации во время осуществления платежей, и как результат – успешно пройти сертификацию на соответствие требованиям такого международного стандарта безопасности платежей.

Следует отметить, что в Украине согласно п. 39.3 ст. 39 Закона Украины «О платежных системах и переводе денег в Украине» с целью обеспечения безопасности денежных переводов платежными системами широко используются антифрод-фильтры для выявления мошеннических операций, а также многофакторная аутентификация пользователей (например, применение для аутентификации пароля вместе с аппаратным средством защиты информации (токеном) или биометрической аутентификации вместе с паролем) (см. пп.1 п. 3 раздела I постановления Правления НБУ «Об утверждении Положения об организации мероприятий по обеспечению информационной безопасности в банковской системе Украины» от 28.09.2017 г. № 95).

Выводы. Принимая во внимание изложенное выше, можно сделать обобщающий вывод, что для обеспечения надлежащего уровня безопасности платежей важным является эффективное правовое регулирование в этой сфере как на уровне национального законодательства, так и учитывание международных стандартов по внедрению и использованию инновационных технологий непрерывной защиты информации относительно перевода средств на всех этапах ее формирования, обработки, передачи и хранения в платежном пространстве. Все это в совокупности гарантирует целостную систему безопасности электронных и мобильных платежей.

Список использованной литературы:

1. Алісов Є.О. Деякі проблеми правового регулювання глобальної платіжної системи в Україні. Вісник Академії правових наук України. 2004. № 4. С. 116-126.

2. Рекомендації Національного банку України щодо складання правил платіжної системи, платіжною організацією якої є резидент. URL: https://bank.gov.ua/doccatalog/document?id=56198275.

3. Official PCI Securety Standards Council Site. PCI DSS (Payment Card Industry Data Security Standard). URL: https://www.pcisecuritystandards.org.

4. Transport Layer Security (TLS). IETF. URL: https://datatracker.ietf.org/wg/tls/documents/.

5. Филатова Е. Токенизация: как это работает? URL: https://psm7.com/без-рубрики/tokenization-how-does-it-work.html.

6. Керівник ФК «Леогеймінг Пей2 Альона Дегрік про впровадження технології P2PE для захисту електронних платежів. URL: https://window.unian.ua/10087805-kerivnik-fk-leogeyming-pey-alona-degrik-pro-vprovadzhennya-tehnologiji-p2pe-dlya-zahistu-elektronnih-platezhiv.html.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Пожидаева Мария Анатольевна – кандидат юридических наук, доцент, доцент кафедры финансового права учебно-научного института «Юридический институт Государственного высшего учебного заведения «Киевский национальный экономический университет имени Вадима Гетьмана»

INFORMATION ABOUT THE AUTHOR

Pozhydaeva Maria Anatolyevna – Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Financial Law Department in Kyiv National Economic University named after Vadym Getman

pozhydaeva_maria@ukr.net