**УДК 336.7(075.8)**

***Донецкова О.Ю.,***
*экономика илимдеринин кандидаты,*
*банк иши жана камсыздандыруу*
*кафедрасынын доценти,*
*"Оренбург мамлекеттик университети»,*
***Донецкова О.Ю.,***
*кандидат экономических наук,*
*доцент кафедры банковского дела*
*и страхования, ФГБОУ ВО*
*«Оренбургский государственный*
*университет»,*
***Donetskova O.Y.,***
*candidate of economic Sciences,*
*associate Professor of banking and insurance,*
*FSBEI "Orenburg state University»,*
*+ 7 (961) 9066825,*
*e-mail: olja-ja-77@mail.ru*
***Садыкова Л.М.,***
*экономика илимдеринин кандидаты,*
*банк иши жана камсыздандыруу*
*кафедрасынын доценти,*
*"Оренбург мамлекеттик университети»,*
***Садыкова Л.М.,***
*кандидат экономических наук, доцент*
*кафедры банковского дела и страхования,*
*ФГБОУ ВО «Оренбургский*
*государственный университет»,*
***Sadykova L.M.,***
*candidate of economic Sciences,*
*associate Professor of banking and insurance,*
*FSBEI "Orenburg state University»,*
*+7 (922) 8900077,*
*e-mail: sad.l.m@mail.ru*

# БААЛОО КООПСУЗДУГУН КАМСЫЗ КЫЛУУ, ЭЛЕКТРОНДУК ТӨЛӨМДӨРДҮ АЗЫРКЫ ЭТАПТА РОССИЯДА

# ОЦЕНКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ НА СОВРЕМЕННОМ ЭТАПЕ В РОССИИ.

# ASSESSMENT OF THE SECURITY OF ELECTRONIC PAYMENTS AT THE PRESENT STAGE IN RUSSIA

***Аннотация****: Макалада электрондук төлөмдөрдү өнүктүрүү жана алардын коопсуздугу маселелери каралат. Негизги төлөм системасы менен камсыз кылынган ишенимдүүлүк жана коопсуздук маселелери боюнча, алардын өзгөчөлүктөрү. Макалада электрондук бүтүмдөрдү уруксатсыз статистика келтирилген.*

***Аннотация****. В статье рассматриваются вопросы развития электронных платежей и их безопасности. Представлены основные платежные системы, их характеристики с точки зрения надежности и безопасности. Представлена статистика несанкционированных электронных сделок.*

***Annotation****.The article deals with the development of electronic payments and their security. The main payment systems are presented, their characteristics are given in terms of reliability and safety. The article presents statistics of unauthorized electronic transactions.*

***Негизги сөздөр****: электрондук төлөмдөр; төлөм системалары; коопсуздук; электрондук жүгүртүү; банктар.*

***Ключевые слова****: электронные платежи; платежные системы; безопасность; электронный оборот; банки.*

***Keywords****: electronic payments; payment systems; security; electronic turnover; banks.*

На сегодняшний день, современные электронные платежи выступают перспективными направлениями финансового посредничества. Однако, Россия не показывает себя явным лидером в сфере электронных технологий. [1] Финансовые посредники реализуют не все виды электронных платежей, как это происходит в других развитых странах. Тем не менее, они предлагают клиентам обширный спектр электронных услуг: начиная с оплаты мобильной связи до приобретения паев ПИФов.

По данным исследования в 2017-2019 г.г. наиболее эффективными банками среди стран СНГ в категории Mobile Banking Rank CIS сервисы представлены: Тинькофф Банка (банк РФ, оценивается в 73,8 %), Альфа-Банк (банк РФ, оценивается в 70,8 %), Почта Банк (банк РФ, оценивается в 69,3 %), ВТБ24 (банк РФ, оценивается в 64,0 %), Сбербанка (банк РФ, оценивается в 61,6 %). В ТОП - 10 также вошли Райффайзенбанк (РФ), два белорусских банка (Белгазпромбанк и Альфа-Банк), Банк Грузии и казахский ForteBank. [2]

Наиболее востребованными в России среди электронных финансовых и платежных сервисов являются интернет-банк, мобильный банк или SMS-банк. Услугами электронных платежей пользуются примерно 19,4 млн. человек (68,7% пользователей Интернета в России) используют эти сервисы. Молодежь от 20 до 24

лет активнее используют электронные платежи для оплаты интернет билетов или онлайн-контента. Население от 35 до 44 лет оплачивают мобильную связь и коммунальные услуги.

Платёжный электронный оборот активно развивается. По данным ЦБ, еще в 2013 году он составил 830 млрд рублей, а к концу 2019 г ожидается прирост до уровня 2395 млрд рублей. Обороты электронных платежных систем соответственно приумножаются, и это не может не прельщать внимания разных мошенников.

Все электронные платежные системы, функционирующие на рынке имеют определенную степень защиты. Охарактеризуем критерии безопасности электронных платежных систем [3].

Так, аутентификацию с использованием токенов имеется только у WebMoney, а у «Яндекс.Деньги», CyberPlat, E-port и «Рапида» такой безопасности не имеется.

По критерию многофакторной аутентификации отличаются WebMoney, которая имеет пароль + файл-ключ, у «Яндекс.Деньги применяет пароль + программа-кошелек. CyberPlat, E-port и «Рапида» многофакторной аутентификации также не имеют.

Шифрование используют практически все платежные системы:

- Алгоритм типа RSA, ключ 1024 бита применяется в WebMoney;

- Алгоритм RSA, ключ 1024 бита используется у «Яндекс.Деньги»;

- Алгоритм RSA, ключ 512 бит применяется в CyberPlat;

- Технология SSL 3.0, ключ от 40 до 128 бит реализуется E-port [4].

Так, в WebMoney, все операции обязательно подвержены шифрованию по криптоалгоритму. Однако, при использовании старых версии браузеров шифрование теряет свою защиту и возникает риск перехвата данных. Для приумножения доли электронных платежей провайдеры дополняют свои продукты множеством функций, не требующих расходов: персональный бюджет, визуализация расходов, автоматические платежи по заданному графику.

Наличие SMS-сервиса, анонимность частных клиентов и возможность перевода средств между частными клиентами присутствует во всех платежных системах, кроме CyberPlat.

Система blacklist успешно реализует WebMoney, другие анализируемые платежные системы данными характеристиками не обладают.

Дополнительные средства защиты от мошенников также имеются у WebMoney, в отличии от «Яндекс.Деньги», CyberPlat, E-port и «Рапида».

Общая схема осуществления электронных платежей выглядит следующим образом: банк, оформляет соглашение с ЭПС. Приобретая специальную лицензию, банк может выступать как эмитент платежных средств, и как банк-эквайрер. Механизм проведения электронного платежа не сложный. Первоначально, кассир проверяет подлинность карты. Во время оплаты предприятие через импринтер переносит реквизиты карты клиента на специальный чек и требует на нем подпись клиента в знак согласие на покупку услуги. Одна копия слипа остается на предприятии, вторая передается клиенту, третья - в банк-эквайрер и является основанием платежа предприятия со счета клиента.

В целях безопасного исполнения платежей предусматриваются нижние лимиты сумм для различных регионов и видов бизнеса, по которым осуществляются платежи без авторизации. При превышении лимита или подозрении на мошеннические действия автоматически включается процесс авторизации.

Универсальность механизма привлекательна для мошенничества. На сегодняшний день зафиксировано 5 основных видов преступлений с пластиковыми картами.

1. Операции с поддельными картами**.** Наиболее распространенный вид мошенничества. Для подделки применяют украденные заготовки карт, на которые наносятся реквизиты банка и клиента. Имея качественно технологии, преступники могут даже наносить информацию на магнитную полосу карты. Кроме того, имеют место быть организованные преступные группировки, сотрудничающие с работниками банков-эмитентов и имеющие доступ к информации о счетах клиентов, процедуре проведения транзакций.

2. Операции с похищенными/потерянными пластиковыми картами**.**

Причинить большой ущерб по похищенной карте возможно когда мошенник иметь сведения о PIN-код клиента. Тогда делается вероятным снятие немалой суммы со счета клиента через электронную сеть до того момен-

та пока банк-эмитент похищенной карты занесет ее в электронный стоп-лист (список недействительных карт).

3. Неоднократная уплата услуг и товаров на суммы, не превосходящие “floor limit” и не требующие авторизации. Для провести расчетов преступнику нужно лишь подделать подпись клиента.

4. Мошенничество с почтовыми/телефонными заказами**.**

Этот вид преступлений возник одновременно с развитием сервиса доставки товаров и услуг по почтовому или телефонному заказу клиента. Иметь сведения о е кредитной карты, мошенник может указать ее в бланке заказа и, приобретя заказ по адресу временной прописки, скрыться.

5. Многократное снятие со счета осуществляется при оформлении нескольких однотипных платежных чеков по одному факту оплаты по кредитной карте за приобретенные товары и услуги.

Отметим, что наибольшую долю 54% - имеют преступления, совершенные через интернет и мобильный телефон, 27% - подделка карт, подписей, пинкодов и т.п. [5].

Платежные операторы выделяют причины инцидентов несанкционированных операций. Наиболее распространенная причина - использование ЭСП без согласия клиента, применение вредоносного кода или злоупотребления доверием клиента [6]. Данные, предоставленные в Банк России от операторов услуг платежной инфраструктуры по форме отчетности 0403203 характеризуют отсутствие информированности клиентов о факте обращения в правоохранительные органы.

Учитывая, что средний объем нелегальной операции с использованием платежной карты не превышает 3,7 тыс. руб., клиенты не пишут заявления в полицию [7]. Таким образом, причинами такой тенденции выступает финансовая неграмотность населения в области информационной безопасности.

По факту несанкционированных операций со счетов юридических лиц имеется больше обращений в правоохранительные органы, чем с использованием платежных карт. Средний размер несанкционированных сделок со счета юридического лица составляет 2,76 млн руб [8]. Т.е. более чем в 700 раз, чем сумма нелегальной операции с использованием платежной карты. При этом, число несанкционированных операций с использованием платежных карт превышает больше чем в 400 раз нелегальные операции со счетов юридических лиц.

Наибольшие показатели в рамках своего федерального округа имеют Москва и Центральный ФО, Приволжский ФО и другие регионы.

Рассмотрим территориальное распределение несанкционированных операций с использованием платежных карт [9]:

1. Москва - 206 ед. несанкционированных операций со счетов юридических лиц на общую сумму 719 337,70 тыс. руб.;

2. Центральный федеральный округ - 116 ед. на 346287,40 тыс. руб. соответственно;

3. Приволжский ФО - 112ед. - 313 549,00 тыс. руб.;

4. Южный ФО - 65 ед. - 174 962,30 тыс. руб ;

5. Уральский ФО - 59 ед. - 111 174,9 тыс.руб.;

6. Санкт-Петербург - 49 ед. - 76 122,77 тыс. руб;

7. Сибирский ФО - 36 ед. - 42 005,20 тыс. руб;

8. Дальневосточный ФО - 26 ед. - 31 492,85 тыс. руб;

9. Северо-Западный ФО - 21 ед. - 22 858,33 тыс.руб;

10. Северо-Кавказский ФО - 13 ед .- 24 818,14 тыс.руб;

11 Севастополь - 4 ед. - 3 316,10 тыс. руб.

Отметим, что наибольшая доля преступлений осуществляется в г. Москва, по количеству и по объему совершенных несакционированных операций приравнивается к Центральному и Приволжскому регионах. Аналогичная тенденция наблюдается и по нелегальным операциям с использованием платежной карты.

Для обеспечения безопасности электронных платежей используют различные методы, которые условно делятся на две категории:

1. Методы, определяющие техническую защиту пластиковой карты.

2. Методы, направленные на предотвращение утечки платежной информации.

Для профилактических мер осуществляется работа с клиентами, обращенная на повышение культуры применения карт для электронных платежей.

Для обеспечения безопасности электронных платежей применяется PIN-код из четырех цифр, который дает один шанс на десять тысяч случайного угадывания кода. При осуществле-

нии трех неверных попыток ввода PIN-кода вероятность снять денег минимальная.

Некоторые банки используют случайно выбранный PIN-код с последующим криптопреобразованием его для запоминания, или держат зашифрованное значение PIN-кода в файле. По этой причине, в системе VISA рекомендуется, чтобы банки комбинировали номер счета клиента с его PIN-кодом перед зашифрованием. Однако не все банки это делают.

Также есть вероятность снижения обеспечения безопасности электронных платежей в случае, когда банкоматы располагаются в густонаселенных городах и посылают незашифрованные номера счетов и PIN-коды по телефонной линии в устройство управления филиала. Любое устройство прослушивания телефонной линии позволяет считывать данную информацию.

Разработчики криптографических систем испытывают недостаток информации о том, как в действительности осуществляются мошеннические действия на практике. Этот недочет отражается на неверном использовании модели угроз. Например, отрицательным моментом на практике явился поток мошенничеств с банкоматами. Этот факт стал следствием финансовых потерь, снижению доверия к банковскому сектору.

Программная криптографическая система защиты информации с использованием цифровой подписи EXCELLENCE определена для защиты информации, обрабатываемой, хранимой и передаваемой между IBM-совместимыми персональными компьютерами, посредством криптографических функций шифрования, цифровой подписи и контроля подлинности.

Данная система реализует следующие функции: зашифрование/расшифрование; цифровая подпись; контроль целостности; генерация (смены) личных ключей; установка парольной защиты; аутентификация открытых ключей.

Ключевая система со строгой аутентификацией и сертификацией ключей построена на широко применяемых в международной практике: наличие секретного и открытого ключей. Секретный ключ каждого клиента вписан на его индивидуальную электронную карточку (дискету) и обеспечивает защиту закодированной для него информации и нереальность подделки его цифровой подписи.

Оптимальным решением для банков в сфере обеспечения безопасности электронных платежей являются предложения аутсорсинговых компаний. Они в силу своей специализации и опыта работы способны обеспечить доступностью, функциональность и защищенность операций банков.

Относительно электронных платежей мошенники имеют следующие цели:

1. кража финансовых ресурсов.

2. насыщение финансовой системы фальшивыми средствами.

3. введение технической неисправности.

Банк России ежегодно фиксирует около 50 фактов хищения денежных средств посредством воздействия на банкоматы и на платежные терминалы. К ним относятся прямое подключение технических устройств и проведение внешнего управления ими; дистанционное управление, а также физическое повреждение. Совокупный ущерб составил более 5 млн рублей.

Следовательно, для минимизации убытков связанных с мошенническими атаками, необходимо придерживаться основных принципов формирования системы электронных платежей:

Во-первых, электронные платежи должны гарантировать защиту платежных данных от нелегального изменения.

Во-вторых, электронные платежи не должна подвергаться умышленным атакам со стороны мошенников.

В-третьих, электронные платежи не должны быть прочтены и модифицированы не санкционировано третьими лицами.

В-четвертых, электронные платежи должны быть независимы от воздействия из глобальной сети [10].

Таким образом, обеспечение безопасности электронных платежей гарантирует успешное сотрудничество и дальнейшее процветание электронной коммерции и банковского сектора в целом.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. Парусимова, Н. И. Банковский сектор катализатор роста [Текст]: / Н.И. Парусимова // Интеллект. Инновации. Инвестиции,2016. - № 11. - С. 67-69.

11. Mobile Banking Rank CIS 2017 [Электронный ресурс].- Режим доступа: http://markswebb.ru/e-finance/mobile-banking-rank-cis-2017 / 08.05.2019/. - Загл. с экрана.

2. CNews Analytics [Электронный ресурс]. - http://www.prostobankir.com.ua/it/stati/elektronnye_platezhi_riski_i_bezopasnost./08.05.2019/. - Загл. с экрана.

3. Мошенничества с пластиковыми картами [Электронный ресурс]: - http://www.aferizm.ru/moshen/pp_plast_kart.htm./ 08.05.2019 / - Загл. с экрана.

4. Обзор несанкционированных переводов денежных средств за 2016 год. Москва, ЦБ, 2017 [Электронный ресурс]: - http://www.cbr.ru/credit/Gubzi_docs/survey_transfers_16.pdf /08.05.2019/. - Загл. с экрана.

5. О развитии банковского сектора Российской Федерации. Декабрь. 2018 [Электронный ресурс]: - Режим доступа: http://www.cbr.ru/Collection/Collection/File/14236/razv_bs_18.pdf . / 15.04.2019/. - Загл. с экрана.

6. Прогноз развития банковского сектора в 2019 году: на позитивной ноте [Электронный ресурс]: - Режим доступа: https://raexpert.ru/researches/banks/bank_sector_forecast2019. / 25.04.20198/. - Загл. с экрана.

7. Банковский сектор в 2018 году: ставка на крупных [Электронный ресурс]: - Режим доступа: https://raexpert.ru/researches/banks/bank_sector_2018. /25.04.2019/. - Загл. с экрана.

8. Прогноз развития банковского сектора в 2018 году: кризис бизнес-модели [Электронный ресурс]. - Режим доступа: https://raexpert.ru/researches/banks/prognoz_2018./02.04.2019/. - Загл. с экрана.

9. Основные направления единой государственной денежно-кредитной политики на 2018 год и период 2019 и 2020 годов [Электронный ресурс]: - М.: Центральный Банк, 2018. - Режим доступа: http://www.cbr.ru/publ/ondkp/on_2018(2019-2020).pdf. /20.04.2019/. - Загл. с экрана.

**Рецензент:** Плужник А.Б., кандидат экономических наук, доцент кафедры банковского дела и страхования Оренбургского государственного университета.

**УДК 657. 6**

***Егорова Л.Г.,***
*ага окутуучу, бухгалтердик эсеп, талдоо жана аудит оșù бөлүмү*
***Егорова Л.Г.,***
*старший преподаватель кафедры бухгалтерского учета, анализа и аудита ОГУ*
***Egorova L.G.,***
*Senior Lecturer at the Department of Accounting, Analysis and Audit of OSU*
*моб. т.: +7(961) 92952 82*
*e - mail: egorowa70@mail.ru*

## СУТ ӨНӨР ЖАЙ ИШКАНАЛАРЫНДА МАТЕРИАЛДЫК НАРКЫН ЭСЕПКЕ АЛУУ БААНЫН

## УЧЕТ ОБЕСЦЕНЕНИЯ МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ НА ПРЕДПРИЯТИЯХ МОЛОЧНОЙ ПРОМЫШЛЕННОСТИ

## ACCOUNTING OF IMPAIRMENT OF MATERIAL VALUES AT THE ENTERPRISES OF THE DAIRY INDUSTRY

***Аннотация:*** *Көйгөйлөрү жана жолдору менен макалада унун азыркы Орусиянын экономикасы кайра иштетүүчү өнөр жай ишканалары үчүн материалдык мүлктөргө эскиришин камсыз кылууну оптималдаштыруу.*

***Аннотация:*** *В статье рассматриваются проблемы и пути оптимизации формирования резервов под снижение стоимости материальных ценностей для перерабатывающих производств в современной экономике России.*

***Annotation:*** *The article discusses the problems and ways to optimize the formation of reserves for reducing the value of material values for processing industries in the modern Russian economy.*

***Негизги сөздөр:*** *запастар; эсепке алуу; баа берүү; жешилиши; баалоо төлөөлөр; материалдарды Баанын Жобо; сүт өнөр жайы.*

***Ключевые слова:*** *материальные запасы; учет; оценка; обесценение; оценочные резервы; резерв под снижение стоимости материалов; молочная промышленность.*

***Keywords:*** *inventories; accounting; assessment; impairment; estimated reserves; reserve for material cost reduction; dairy industry.*