МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ

УДК: [004+002.56]:336

АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАБОТЕ С НАЛИЧНЫМИ, БЕЗНАЛИЧНЫМИ И ЭЛЕКТРОННЫМИ ДЕНЬГАМИ

Статья поступила в редакцию 23.02.2016, в окончательном варианте 17.03.2016.

Дюдикова Екатерина Ивановна, аспирант, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: dudikova.e@gmail.com

Брумштейн Юрий Моисеевич, кандидат технических наук, доцент, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: brum2003@mail.ru

Танющева Наталия Юрьевна, кандидат экономических наук, доцент, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: n.tanyushcheva@rambler.ru

Демина Раиса Юрьевна, аспирант, Астраханский государственный технический университет, 414025, Российская Федерация, г. Астрахань, ул. Татищева, 16, e-mail: raisapereverzeva@gmail.com

Васьковский Евгений Юрьевич, аспирант, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: vaskovskiy_evgeniy@mail.ru

Кузьмина Алеся Борисовна, выпускница аспирантуры кафедры Информационных технологий, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: lesenok-1988@mail.ru

Дюдиков Иван Андреевич, выпускник аспирантуры кафедры Информационных технологий, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: shtorman@mail.ru

Рассмотрены особенности наличных, безналичных и электронных денег; преобладающие цели их использования; направления преобразования одних форм в другие. Приведены данные о частоте встречаемости в Интернете ключевых терминов по теме статьи. Проанализированы основные классы программно-аппаратных средств (ПАС), используемых для обеспечения технологических операций приема, выдачи, хранения денег; передачи информации, связанной с денежными средствами (ДС). Исследованы основные виды угроз для физических и юридических лиц, связанные с применением таких ПАС при работе с ДС. Проанализированы потенциально возможные и практически используемые меры риск-менеджмента при работе с ДС. Показаны направления влияния развития информационных технологий, уровней информационно-телекоммуникационной компетентности специалистов и населения на объемы использования и безопасность применения рассматриваемых в статье ПАС, технологий работы с ДС.

Ключевые слова: наличные деньги, безналичные деньги, электронные деньги, электронные платежные системы, номенклатура операций, программно-аппаратные средства, информационная безопасность, риск-менеджмент, персональные данные, информационно-телекоммуникационная компетентность

THE ANALYSIS AND RISK MANAGEMENT OF INFORMATION TECHNOLOGIES USAGE DURING THE WORK WITH CASH, NON-CASH AND ELECTRONIC MONEY

Dyudikova Ekaterina Ivanovna, post-graduate student, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: dudikova.e@gmail.com

Brumshteyn Yury Moiseevich, Ph.D. (Engineering), Associate Professor, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: brum2003@mail.ru

Tanyushcheva Natalia Yurevna, Ph.D. (Economics), Associate Professor, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: n.tanyushcheva@rambler.ru

Dyomina Raisa Yurevna, post-graduate student, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: raisapereverzeva@gmail.com

Vaskovsky Evgeny Yurievich, post-graduate student, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: vaskovskiy_evgeniy@mail.ru

Kuzmina Alesya Borisovna, post-graduate student (finished training) of Information Technologies Chair, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: lesenok-1988@mail.ru

Dyudikov Ivan Andreevich, post-graduate student (finished training) of Information Technologies Chair, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: shtorman@mail.ru

In article are considered features of cash, non-cash and electronic money; their prevailing usage purposes; the directions of transformation from one form to others. Authors are specified the occurrences frequency for key terms on article subject in the Internet. There are analyzed main classes of software and hardware (SaH), used for ensuring technological operations of reception, delivery, storage of money; the information transfer connected with the money. The main types of threats for legal entities and individuals, connected with application of such SaH during the work with money, are investigated. Authors are analyzed potentially possible and used measures of risk management for the work with money. Also in article are shown the directions of influence of information technologies development, levels of information and telecommunication competence of specialists and population, on volumes of usage and safety of application SaH, considered in article; technologies of work with money.

Keywords: cash, non-cash money, electronic money, operations nomenclature, software and hardware, information security, risk management, personal information, information and telecommunication competence

Введение. В настоящее время во всех странах, в т.ч. и в России, участники экономических и финансовых отношений используют разные формы денег, способы передачи информации о денежных средствах (ДС) и их движении по счетам. При этом широко применяются различные программно-аппаратные средства (ПАС), каналы телекоммуникаций. Это обуславливает актуальность всего комплекса вопросов, связанных с обеспечением физической, информационной, инженерно-технической и других видов безопасности денежного обращения – для всей страны, регионов, отдельных физических и юридических лиц (ФиЮЛ). Процессы расширения использования ПАС при работе с денежной информацией – важная компонента всесторонней информатизации общества – как за рубежом, так и в России [11, 18]. Указанные ПАС уже играют ключевую роль в снижении объема наличных денег (НД) в обращении, оказывают влияние на работу финансовых и иных организаций и пр. Вопросам информационной и других видов безопасности использования таких ПАС посвящен ряд статей. Однако недостаточно полно исследованы такие направления: оценка и управление безопасностью использования ПАС в условиях «параллельной» работы с разными формами денег, систематического использования операций конвертации одних форм денег в другие; влияние информационно-телекоммуникационной компетентности (ИТКК) ИТ-специалистов и населения [11] на безопасность применения ПАС; способы управления этой компетентностью [18]. Целью данной статьи является попытка устранения неполноты исследований по указанным направлениям.

Традиционные формы денег, электронные деньги и особенности их использования. Рассмотрим вопросы толкования терминов, используемых в статье.

Согласно Гражданскому кодексу (ГК) Российской Федерации (РФ) (ред. от 29.06.2015 г.) рубль является законным платежным средством, обязательным к приему по нарицательной стоимости на всей территории РФ. Платежи на территории РФ осуществляются путем наличных и безналичных расчетов (ст. 140 ГК РФ). Безналичные расчеты производятся через банки, иные кредитные организации, в которых открыты соответствующие счета, если иное не вытекает из закона и не обусловлено используемой формой расчетов (ст.861 ГК РФ).

В Республике Беларусь расчеты также могут проводиться в наличной и безналичной формах. Последней считаются расчеты между ФиЮЛ либо с их участием, проводимые через банк или небанковскую кредитно-финансовую организацию, его (ее) филиал в безналичном порядке [5].

В Директиве 2007/64/ЕС Европейского парламента и Совета ЕС от 13 ноября 2007 года акцентируется внимание на том, что НД представляют собой ДС, которые не хранятся на счете. К платежным операциям с использованием НД относятся операции, которые совершаются напрямую между плательщиком

и получателем без участия посредника. В этом документе ДС означают банкноты и монеты, безналичные и электронные деньги [14]. Таким образом, существование в вещественной форме и наличие неразрывной связи денежного носителя с денежной стоимостью – основные признаки НД (монеты и банкноты).

Под безналичными деньгами понимаются деньги (записи) на банковских счетах, используемые для оплаты и взаимных расчетов посредством перечисления с одного банковского счета на другой [26].

В настоящее время нет единого понимания сущности «электронных денег» (ЭД).

Европейский центральный банк считает, что ЭД – это «сумма ценности в денежном выражении, представленная в виде требования, выпущенного на заранее оплаченной основе, которая хранится на электронном носителе (например, карта памяти или компьютер), принимается в качестве средства оплаты лицами, отличными от эмитента, и предназначенная, преимущественно, для сделок на небольшие суммы» [32].

В директиве Европейского парламента и Совета ЕС 2009/110/ЕС от 16.09.2009г. ЭД определяют как «хранимую в электронном виде, в том числе и на магнитном носителе, представленную в виде требований к эмитенту стоимость в денежном выражении, эмитируемую при получении денежных средств для проведения платежных трансакций, определение которых приведено в статье 4 (5) Директивы 2007/64/ЕС, и принимаемую физическими или юридическими лицами, отличными от эмитента электронных денег» [15].

В Республике Беларусь под ЭД понимают «хранящиеся в электронном виде единицы стоимости, выпущенные в обращение в обмен на наличные или безналичные денежные средства и принимаемые в качестве средства платежа при осуществлении расчетов как с лицом, выпустившим в обращение данные единицы стоимости, так и с иными юридическими и физическими лицами, а также выражающие сумму обязательства этого лица по возврату денежных средств любому юридическому или физическому лицу при предъявлении данных единиц стоимости» [5].

С принятием закона «О национальной платежной системе» [24] в РФ также появилось официальное определение ЭД. Позже в Письме Банка России [23] было уточнено определение ЭД как безналичных ДС в рублях или иностранной валюте, учитываемых кредитными организациями без открытия банковского счета и переводимых с использованием электронных средств платежа. Однако в законе «О национальной платежной системе» [24] четко указывается, что оператор электронных денежных средств учитывает предварительно предоставленные законные деньги клиента путем формирования остатка электронных ДС в виде записи, отражающей размер денежных обязательств оператора электронных ДС перед клиентом в сумме депонированных законных денег.

Таким образом, ЭД не имеют однозначного определения в нормативных актах, поэтому они толкуются и как законные деньги (существующая или новая денежная форма) и как предоплаченный финансовый продукт. Однако тесная взаимосвязь ЭД и электронных расчетно-платежных систем (ЭРПС) признается всеми авторами [6, 17, 33].

В экономической литературе существует три трактовки ЭД [27].

В рамках расчетной трактовки ЭД связывают с банковскими картами (БК), системами дистанционного банковского обслуживания (далее – ДБО), электронным и телефонным банкингом, техническими инструментами хранения информации (например, [29]), либо отождествляют их с безналичными расчетами (например, [26]).

Сторонники второй трактовки (например, [19]) понимают под ЭД предоплаченный финансовый продукт и акцентируют внимание на том, что именно предварительно депонированные законные деньги обеспечивают ценность ЭД. Основное свойство ЭД как особого актива (в виде зафиксированного на техническом устройстве информации, предоставляющей право требования к оператору системы ЭД исполнения денежного обязательства) – возможность их многоцелевого использования. При этом в отличие от наличных и безналичных денег признание ЭД в качестве средства обмена зависит от волеизъявления участников расчетов. Таким образом, ЭД не представляют собой законное платежное средство, не имея внутренней ценности, государственной гарантии и всеобщего признания.

Сторонники денежной трактовки (например, [3]) считают целесообразным принятие нормативных актов, придающих ЭД статус «законная форма денег» и обеспечивающих беспрепятственное перемещение ЭД в рамках национальной платежной системы.

Достоинства и недостатки традиционных форм денег и ЭД сравнены в таблице 1.

Таблица 1

Достоинства и недостатки использования наличных, безналичных и ЭД

Достоинства	Недостатки
Наличные деньги	
Ценность гарантирована законом Всеобщее признание в качестве средства обмена и платежа Единый вид на всей территории страны Отсутствие посредников при совершении платежей Отсутствует стоимость проведения операции Отсутствует необходимость использования дополнительных устройств для доступа к деньгам Для владельцев денег: возможность сохранения неприкосновенности частной жизни в отношении расходования денег Автономность Легкость использования	Высокая стоимость эмиссии, обслуживания и обращения Высокий уровень износа и порчи Высокий уровень фальсификации Низкий уровень безопасности Низкий уровень государственного контроля и воздействия Зависимость проведения операции от времени и места (территориальные и временные ограничения) Требуется значительное время для совершения операции (для подготовки и выполнения условий совершения операции, в т.ч. проверка подлинности и пересчет) Необходимость размена, наличия купюр определенного номинала Отсутствие делимости Невозможность расчетов в сети Интернет
Безналичные деньги	
Ценность гарантирована законом Всеобщее признание в качестве средства обмена и платежа Единый вид на всей территории страны Средняя стоимость эмиссии, обслуживания и обращения Высокий уровень государственного контроля и воздействия Средняя / мгновенная скорость совершения транзакции Перемещение на любые расстояния Отсутствие зависимости проведения операции от времени и места использования ДБО Возможность длительного срока существования (не изнашиваются и не портятся со временем) Низкий уровень фальсификации Высокий уровень безопасности Портативны Делимость Простота использования (офис кредитной организации)	Высокая стоимость проведения операции Зависимость проведения операции от времени и места (офис кредитной организации) Проведение операций зависит от нормального функционирования банковской системы, в том числе бесперебойной работы банковских каналов связи, соответствующего программного обеспечения (ПО) и банковских офисов Для владельцев денег: отсутствие возможности сохранения неприкосновенности частной жизни Доступ третьих лиц к деньгам Необходимость дополнительных знаний и умений для использования ДБО
Электронные деньги	
Возможность использования в сети Интернет Перемещение на любые расстояния Отсутствие зависимости проведения операции от времени и места Средний уровень государственного контроля и регулирования Мгновенная скорость совершения транзакции Низкая стоимость эмиссии, обслуживания и обращения Низкая стоимость проведения операции Возможность длительного срока существования (не изнашиваются и не портятся со временем) Отсутствие необходимости посещения офисов для регистрации и работы с системой ЭД Портативны Делимость	Частное денежное обязательство оператора системы ЭД Средний уровень безопасности Необходимость использования специальных электронных устройств Зависимость от бесперебойной работы системы ЭД, в том числе абонентских устройств, каналов связи и соответствующего ПО Отсутствие единого утвержденного вида электронных денег в разных системах ЭД Признание в качестве средства обмена зависит от волеизъявления участника операции Средний уровень фальсификации Доступ третьих лиц к деньгам Необходимость дополнительных знаний и умений для использования систем ЭД и проведения расчетов ЭД

Наличные деньги являются основным платежным средством при совершении розничных операций в реальном мире, хотя в последние годы с ними активно конкурируют БК [25]. Юбилейные и памятные монеты и банкноты при использовании их в наличных платежах принимаются по номиналу. Однако они быстро выходят из обращения, оседают в коллекциях и становятся предметом сделок купли-продажи по стоимости, значительно отличающейся от номинальной. Это же касается не предназначенных для наличных расчетов специальных памятных монет, а также монет, выпускаемых по технологии «proof» (улучшенного качества) для коллекционеров. Коллекционные монеты из золота, платины, палладия, серебра реализуются по ценам, значительно отличающимся от их номинала. Для первых трех металлов они иногда могут служить и способом вложения средств – особенно при нестабильных курсах валют. Обслуживание операций с НД является дорогостоящим не только для государства, но и для ФиЮЛ. Так, хранение НД в организациях требует использования специальных мер: применения сейфов; инкассации; усиленных средств видеонаблюдения и сигнализации; использования защищенных банковских хранилищ, в т.ч. заглубленных в грунт [10] и др.

Особенности безналичных денег: способность обслуживания операций как в реальном мире, так и в сети Интернет; они используются в расчетах и платежах ФиЮЛ, причем последние все свои расчеты проводят через банковские счета; только на остаток безналичных ДС может осуществляться начисление процентов (что позволяет использовать банковские депозиты для получения дохода); в качестве кредита могут предоставляться исключительно безналичные деньги (однако микрофинансовые организации предоставляют займы НД).

Ниже мы будем использовать обобщенный термин «электронные терминалы» (ЭТ), который включает в себя две группы оборудования. 1) Устройства, которые могут выдавать выписки об остатках ДС и состоянии баланса счета, принимать и (или) выдавать ДС. Они, как правило, принадлежат не банковским организациям, а операторам терминальных сетей (ОТС). 2) Банкоматы (устройства самообслуживания, позволяющие выполнять ряд банковских операций). Они, как правило, принадлежат банковским организациям.

Способы пополнения банковских счетов: НД через ЭТ или кассу; безналичными ДС – путем перевода с банковского счета отправителя, либо без открытия банковского счета; путем уменьшением остатка ЭД на электронном счете (ЭС) и зачисления средств на банковский счет. Уменьшение остатка ДС на банковском счете возможно только путем списания ДС с банковских счетов. При этом передача распоряжения может осуществлять через офис, систему ДБО, карт-ридер. Переход денежной стоимости из безналичной в наличную форму выполняется через ЭТ или кассу.

В России практически каждый банк предоставляет для своих клиентов услугу ДБО. Примерами ДБО являются Телебанк (ВТБ 24 ПАО) и Сбербанк Онлайн (ПАО Сбербанк).

Расчеты с использованием ЭД наиболее распространены в сети Интернет и применяются для расчетов на небольшие суммы (в последнее время размеры этих сумм увеличиваются). Для физических лиц (ФЛ), использующих ЭС, ЭД могут быть персонифицированными и неперсонифицированными; для юридических лиц (ЮЛ) и индивидуальных предпринимателей ЭД персонифицированы. На остаток ЭД не начисляются проценты.

Пополнение ЭС возможно в трех вариантах. 1) С использованием банковского счета (путем оформления платежного поручения на бумажном носителе или в электронном виде; в офисе, в системе ДБО, через ЭТ с использованием БК. 2) С помощью НД через ЭТ или кассу. 3) Путем перевода ЭД с другого ЭС в системе ЭД. Вывод денег из системы ЭД возможен путем пополнения банковского счета; получения НД; либо переводом на счет ЭРПС, в т.ч. ЭС в иной системе ЭД.

В России наиболее распространены такие системы ЭД: WebMoney, Яндекс.Деньги, Деньги.Мэйл.Ру, МОБИ.Деньги, E-dinar, Pecunix, GoldMoney и другие.

Не являются ЭД карточки (с магнитной полосой или чипом) для проезда в метро и иных видах общественного транспорта, хотя бы, потому что они не допускают никаких других вариантов использования, кроме прямого назначения, и не предусмотрены для расчетов с организациями, не являющимися их эмитентом. Распечатка ранее предоплаченных через Интернет билетов в кино, на поезд или самолет не является операцией конвертации ЭД в вещественный объект, хотя пользователями таких услуг обычно воспринимается именно так.

Важность для общества различных объектов и технологий отражается в частоте встречаемости соответствующих терминов в Интернет-пространстве. Поэтому в таблице 2 приводятся количества раз, которые ключевые термины по теме статьи были обнаружены различными поисковыми системами Интернета (на 06.03.2016).

Таблица 2

Количества объектов, которые обнаруживают поисковые системы Интернета (ПСИ) для терминов (в млн единиц)

Термин	Google	Bing	Rambler	Yahoo	Lycos	Яндекс	Aol	Metabot (русский поиск / мировой поиск)
Наличные деньги	0,481	0,33	0,142	0,328	0,376	49,0	0,377	0,515/0,376
Cash	1100	63,9	35,0	63,4	63,4	26,0	63,4	149,9/62,9
Безналичные деньги	0,421	0,286	3,0	0,102	0,102	2,0	0,102	0,07/0,07
Non-cash resources	50,3	0,71	3,0	11,3	11,3	2,0	1,2	42,0/42,0
Non-cash money	58,4	1,3	3,0	10,5	10,5	3,0	0,882	52,0/52,0
Электронные деньги	0,368	2,16	57,0	0,457	0,457	56,0	0,457	0,088/0,088
Electronic money	19,0	54,3	41,5	13,7	13,8	45,0	13,8	94,0/87,0
E-money	51,7	0,785	0,464	2,22	2,22	0,44	2,22	187,2/220,0
Electronic found	1190	18,5	497,0	14,4	13,3	459,0	14,4	102,0/98,0
Electronic currency	4,14	4,74	7,0	89,6	93,2	5,0	89,6	30,0/24,0

Программно-аппаратные средства: цели использования и место в системе денежного обращения. Все банкноты имеют индивидуальные пары «шифр серии – номер» (ШСН), которыми они маркируются при выпуске в автоматическом режиме. В дальнейшем это позволяет выявлять поддельные банкноты с повторяющимися парами ШСН и включать их в соответствующие базы данных («черные списки»). Для изготовления банкнот применяется специальная бумага, используются несколько степеней защиты, разные способы печати.

Одно из средств обеспечения безопасности работы с наличными ДС для населения – плакаты с изображениями банкнот и описаниями элементов защиты. Однако большинство плательщиков, использующих в качестве средства платежа банкноты и монеты, наличие этих элементов не проверяют, а получатели – проверяют лишь частично (в т.ч. из-за отсутствия специального оборудования - за исключением кредитных организаций). Полезность в магазинах плакатов с номерами серий поддельных банкнот сомнительна, потому что продавцы (а тем более покупатели), не могут удерживать в голове десятки таких серий.

Для населения в продаже есть миниатюрные фонарики с УФ-светодиодами. Они позиционируются как «детекторы подлинности банкнот», но дают возможность проверить лишь некоторые степени защиты (при условии, если хорошо известно, что именно должно проверяться).

При наличии у пользователей сомнений в подлинности банкноты может быть полезным такой сервис (в т.ч. и для зарубежных банкнот): фотосъемка банкноты с двух сторон (возможно, в разных ракурсах) на камеру смартфона или компьютерного планшета (при наличии достаточно высокого разрешения такой камеры и короткофокусного объектива); передача изображений на специальный сайт для автоматической проверки; получение ответа в онлайн режиме. Такая технология дает возможность проверить часть степеней защиты; автоматически распознать серию и номер банкноты, а также определить их наличие в «черном списке».

При профессиональной работе с ДС в кредитных организациях проверка подлинности НД обеспечивается их визуальным просмотром: проверка наличия оптически изменяющейся краски, водяных знаков, защитных волокон, металлизированной ныряющей защитной нити, микроперфорации. При этом могут быть использованы аппараты с увеличением (лупа); с инфракрасной и / или ультрафиолетовой подсветкой, с белым отраженным косо-падающим и белым проходящим светом.

Информацию об использовании в банках ЭТ для проверки подлинности банкнот (в т.ч. с проверкой через Интернет их изображений и ШСН) нам найти не удалось. Алгоритмы распознавания подлинности банкнот при их приеме в ЭТ держатся производителями этих устройств в тайне. На практике иногда такие автоматы отказываются принимать подлинные банкноты с первого раза, что можно считать ошибками второго рода. Кроме того, ЭТ не принимают банкноты, эмитированные с новыми степенями защиты, до внесения корректив в «распознающее» ПО. Вопросы включения чипов в банкноты крупных номиналов пока не обсуждаются, хотя это было бы логичным и позволило бы улучшить защиту. Сказывается, видимо, определенная инерция восприятия банкнот как объектов, которые можно сгибать произвольным образом.

Отметим также, что прогресс в области информационных технологий (ИТ) приводит к улучшению качества (совершенствованию) фальсификации НД. При этом в ряде случаев распознающие системы ЭТ по приему банкнот и монет различить подделки не могут.

Считается, что использование банкнот носит анонимный характер. Однако современные ИТ позволяют отследить ФЛ, получивших из ЭТ банкноты с конкретными парами ШСН (по кодам их БК) и затем выяснить путем автоматического распознавания ШСН номер и местоположение ЭТ, в который эти банкноты в дальнейшем были внесены. Таким образом, анонимность использования банкнот носит относительный характер.

Монеты традиционно имеют круглую форму (хотя есть и исключения). Их основными элементами визуально различимой защиты от подделок являются изображения на аверсе и реверсе монеты, а также, как правило, дополнительная накатка по боковой поверхности (гурту): рубчатая, сетчатая, узорная, текстовая. В автоматах по приему монет их различение может осуществляться по диаметрам, весу, магнитным свойствам. Себестоимости изготовления монет (особенно из медно-никелевых сплавов) зачастую превышают их номиналы, поэтому введение в монеты дополнительных степеней защиты экономически не эффективно.

Возможны несколько вариантов приема автоматическими устройствами НД и их последующего использования.

1. Оплата товаров и услуг НД без зачисления средств на какие-либо счета. При этом информация о ДС может перемещаться только в рамках устройства или локальной вычислительной сети (ЛВС). Это снижает риски информационной безопасности (ИБ) для пользователей, в т.ч. и в отношении персональных данных. Примеры: выдача в медицинских учреждениях одноразовых бахил в обмен на 5-ти рублевые монеты без каких-либо чеков; выдача стаканчиков с кофе или чаем, сладостей в обмен на наборы монет, опускаемые в соответствующий автомат и пр.

В других вариантах используются ЭТ ОТС – таблица 3 (информация – с сайтов ОТС). Типичный ЭТ способен обслуживать до нескольких десятков ЭРПС. Терминальные системы (ЭТ) используют собственные операционные системы (ОС) реального времени, которые потенциально подвержены угрозам ИБ. При приеме платежей НД в конкретных ЭТ комиссионные сборы для каждого сочетаний «ОТС – ЭРПС» могут быть разными.

Таблица 3

Количества ЭТ операторов терминальных сетей на 10.03.2016

Название оператора	Количество ЭТ в России
QIWI	180000
ComePay	40000
Contact	60000
Рапида	30000
Киберплат	190000
DeltaPay	30000

2, Вносимые НД зачисляются на индивидуальные банковские счета ЮЛ, при этом должен быть выдан чек. Однако на практике ЭТ нередко выдают сообщения типа «Лента для печати чеков закончилась. Продолжить без печати чека. Да или Нет?». При ответе «Да» операция завершается без печати чека. Таким образом, отправитель ДС оказывается без подтверждающего документа. Однако операторы сотовой связи (ОСС) при пополнении счетов пользователей мобильной связи высылают им SMS-оповещения о «пополнении баланса».

Получение НД в ЭТ с помощью БК обычно не вызывает трудностей у владельцев (держателей) таких карт. При оплате коммунальных услуг для ввода назначения платежа и счета получателя ДС используется считывание штрих-кодов с квитанций на ЭТ ОТС, набор числовых кодов на сенсорных экранах ЭТ и пр. Осуществление таких операций требует определенной ИТКК от отправителя ДС (плательщика). Однако на практике их ИТКК часто недостаточна, поэтому помощь клиентам при работе с ЭТ (особенно в отделениях Сбербанка) оказывают специально обученные сотрудники-консультанты. Это снижает нагрузку на персонал, принимающий соответствующие виды оплаты НД. Такие меры для банков являются экономически эффективными. Несмотря на это, на сегодняшний день кредитные организации специальные обучающие занятия с плательщиками по крайней мере в Астраханской области не проводят. Подчеркнем, что платежи НД на сумму до 15 тыс. руб. могут быть анонимными.

3). Внесенные через ЭТ НД отражаются на индивидуальных счетах ФЛ (при пополнении / списании со счета пользователь при условии подключения к услуге информирования получает SMS-оповещения). В дальнейшем ФЛ предоставляется возможность управления остатками средств на счетах через офис и (или) дистанционно с использованием ПЭВМ, сотовых телефонов (смартфонов), компьютерных планшетов и пр.

Сейчас ОС мобильных устройств считаются защищенными от угроз ИБ значительно хуже, чем на ПЭВМ. Как свежий пример, укажем на распространение троянской программы Spy.Agent.SI, которое было зафиксировано экспертами компании ESET [29]. Специалисты этой организации отмечают, что «троян успешно обходит двухфакторную аутентификацию и крадет данные из банковских приложений». Согласно [29] «троян маскируется под мобильное приложение Flash Player и после загрузки запрашивает доступ к функциям администратора устройства. Таким образом, он защищает себя от удаления со смартфона или планшета под управлением Android». По [29] «данные об устройстве жертвы вредоносное ПО каждые 25 секунд отправляет на удаленный сервер». В результате разработчики (или эксплуатанты) трояна получают название модели смартфона, его IMEI-код, данные об активации прав администратора и используемом языке. Согласно [29] «после этого троянская программа выполняет поиск в памяти Android-девайса банковских мобильных приложений. С удаленного сервера она загружает поддельные экраны ввода логина и пароля, которые появляются поверх реальных и блокируют их до ввода действительных логина и пароля пользователем. Личная информация отправляется на удаленный сервер, откуда совершается попытка входа в банковский аккаунт. Параллельно приложение перехватывает на зараженном устройстве SMS-сообщение с одноразовым паролем, который выдается банком».

Для некоторых видов платежей направления расходования зачисленных средств ограничены. Например, при оплате заказов «Книга-почтой», остатки средств на счетах покупателей могут быть использованы ими исключительно для приобретения книг в том же магазине. Возможность возврата излишне внесенных средств покупателям (например, при отсутствии товара в продаже) регулируется внутренними правилами организаций оказывающих услуги. В таких случаях зачисленные ДС не являются ЭД.

Работа с безналичными средствами.

1. Конвертирование безналичных ДС в НД через ЭТ и кассы. Держатель (владелец) БК должен вставить БК в ЭТ (картридер) и затем ввести PIN-код. Ряд банков предлагает также услугу подтверждения владельцами БК операций снятия ДС со счетов с использованием сотового телефона (SMS-оповещение и ввод пользователем индивидуальных кодов в ЭТ по его запросу). При этом информация об уменьшении остатка на счете ФЛ (владельца определенной SIM-карты) проходит еще и через сервера ОСС и сохраняется в их базах данных. Таким образом, обеспечивается дополнительная защита от несанкционированного использования ДС на счете, но одновременно снижается уровень ИБ пользователей (владельцев БК).

2. Зачисление ДС на индивидуальные счета ФЛ. При этом ФЛ могут получать на сотовые телефоны SMS-оповещения о таких операциях, но не на адреса электронной почты. Возможен перевод безналичных ДС с личного банковского счета ФЛ на банковский счет ФЛ или ЮЛ.

3. Переводы денег от одних ФЛ другим ФЛ на сегодняшний день широко осуществляются не только через почтовые отделения, но и системы быстрой доставки (Western Union, ВТБ Спринт, Анелик, Мигом и пр.).

4. Движение (зачисление на счет и списание со счета в пользу ФиЮЛ) денег в безналичной форме по счету ЮЛ с использованием специального ПО и, как правило, с применением ПЭВМ. При этом помимо «Логинов-паролей» обычно используются и «электронные ключи», вставляемые в USB-порты ПЭВМ – это увеличивает уровень защиты транзакций.

5. Межбанковские переводы. Уровень защиты таких операций считается наиболее высоким, в т.ч. и за счет использования специальной межбанковской сети SWIFT, в которой каждый банк имеет свой код; специальных средств защиты ЛВС банков [4,16], их зданий [7,10] и пр.

Меры государственного управления безопасностью использования ПАС, обеспечивающих процессы денежного обращения. Основные цели управления использованием ПАС: обеспечение информационной, финансовой и юридической безопасности ФиЮЛ, совершающих операции с наличными и безналичными деньгами и применяющих формы безналичных расчетов – в т.ч. переводы электронных ДС; снижение объема НД; ускорение денежного оборота и др.

Методы управления разделим на следующие группы: юридические (издание нормативных документов и контроль их выполнения); административные (прямое административное регулирование деятельности кредитных организаций, операторов ЭРПС и пр.); инженерно-технические (напри-

мер, в отношении сертификации ПАС, используемых в системе денежного обращения и пр.); экономические (например, в отношении налогообложения операторов ЭРПС и пр.); правоохранительного характера (выявление и наказание изготовителей поддельных денег; хакеров, взламывающих информационные системы банков, операторов ЭРПС и пр.).

Номенклатура и содержание нормативных документов, регулирующих внедрение и использование ПАС в сфере денежного обращения, в целом адекватны существующим реалиям рыночной экономики в России.

Основная проблема в использовании ЭРПС заключается в том, что обработка информации в основном осуществляется с привлечением организаций зарубежной платежной инфраструктуры (например, процессинговых центров), которые не контролируются российским законодательством. Следствия этого: снижение уровня ИБ ФиЮЛ; возможность отключения от ЭРПС ЮЛ при введении зарубежными странами санкций в отношении России или отдельных банков. В последнем случае ДС, находящие на счетах «заблокированных» банков, могут оказаться недоступными для использования. При этом возможности представления ЮЛ и, особенно, ФЛ юридически значимых подтверждающих документов об остатках ДС на счетах достаточно ограничены. Поэтому весьма актуальна выдвинутая инициатива по созданию национальной платежной системы, не зависящей от субъектов зарубежной платежной инфраструктуры, в.ч. процессинговых центров. К сожалению, при создании такой системы, скорее всего, будут использоваться (по крайней мере, частично) зарубежные комплектующие и ПО, что потенциально снизит ее уровень ИБ [20].

Основные виды угроз и меры риск-менеджмента при работе юридических лиц с ПАС. В качестве ЮЛ при совершении операций с ДС могут выступать такие категории организаций: банки; страховые фирмы; микрофинансовые организации; органы государственного и муниципального управления; казначейство; бюджетные организации; коммерческие организации; некоммерческие организации, не относящиеся к категории бюджетных и др.

Использование ЭРПС (в т.ч. систем ЭД) приводит к целому ряду рисков ИБ [8,21] – как операторов ЭРПС, так и их пользователей. Эти риски зависят не только от ПАС, применяемых в ЭРПС, но и надежности ЭТ, каналов связи, квалификации специалистов и пр. Эффективность затрат на улучшение ИБ нуждается в объективной оценке [33], которая затрудняется нечеткостью условий оценивания, а также неполнотой информации.

Риски при совершении операций с ДС для ЮЛ имеют общие причины и специфические, определяемые особенностями их деятельности.

Общие причины. 1) Несовершенство используемых ПАС, включая недостаточно высокую эксплуатационную надежность ЭТ ОТС [31]; зависимость их от внешних источников энергоснабжения; относительно низкий уровень защищенности от хакерских атак и пр. 2) Недостаточная функциональность некоторых ЭТ и не всегда интуитивно понятный интерфейс пользователя, который в ряде случаев слабо унифицирован в терминальных системах разных ОТС. 3) Высокий уровень зависимости работы многих ЭРПС от размещенных за пределами России зарубежных организаций и их подразделений [8], в т.ч. владеющих значительными долями в капиталах ОТС, фирм, эксплуатирующих ЭРПС. 4) Недостаточная квалификация сотрудников организаций, в т.ч. ИТ-специалистов, занимающихся вопросами ИБ при эксплуатации ЭТ, ЭРПС, ЛВС организаций. Возможные причины: невысокий уровень подготовки специалистов в вузах; неэффективности отбора сотрудников при приеме на работу, неадекватность мер стимулирования повышения их квалификации. 5) Недостаточная мотивация сотрудников организаций к качественному выполнению своих служебных обязанностей, а также низкий «уровень лояльности» сотрудников к работодателям и пр. 6) Недочеты в системах защиты информации организаций, в т.ч. относящихся к банковской сфере, страхованию рисков Как правило, компьютерные атаки на компании приводят к ущербу двух видов: материальному и репутационному. Так в 2015 году была совершена серия атак на сети отелей Hyatt Hotels Corporation, Trump Hotel Collection и Hilton. При этом Hyatt Hotels Corporation предупредила клиентов о вероятной компрометации их БК. Подозрительная активность была замечена 30 ноября 2015 года и на официальном сайте было вывешено объявление об инциденте. Однако не сообщается, как долго вредоносное ПО существовало в сети, и какой именно ущерб был нанесен [22]. В литературе описаны и вирусы, действия которых направлены не на финансы компании, а на ее производственную деятельность. Есть также сообщения о хакерских атаках на банки – в т.ч. путем присылки их сотрудникам писем, имитирующих рассылки FinCert и содержащих корректные фамилию, имя, отчество получателей [28].

Типичные меры риск-менеджмента организаций, направленные на снижение вероятностей реализации неблагоприятных событий, связанных с использованием ДС. 1) Строгое соблюдение мер ИБ, включая регламенты деятельности подразделений и должностные инструкции специалистов. 2) Своевременное обновление программных средств, включая базы данных антивирусных программ, ОС серверов и пользовательских ПЭВМ. 3) В технически целесообразных случаях использование в ЛВС организаций пользовательских терминалов вместо полнофункциональных ПЭВМ. 4) Систематическое повышение квалификации специалистов (работников), обеспечение их лояльности к работодателям за счет мер материального и морального воздействия. 5) Оптимизация распределения персонала между подразделениями организации с учетом его компетентности, мотивации, показателей деятельности [9]. В общем случае могут быть использованы меры как индивидуального, так и группового управления рисками [12].

Для снижения ущербов в случае реализации неблагоприятных событий могут применяться такие меры: превентивная разработка планов действий в «аварийных» ситуациях, включая выходы из строя ПАС, хакерские атаки, отказы каналов связи и пр.; создание необходимых резервов ДС; страхование рисков и пр. [1].

Основные виды угроз и меры риск-менеджмента при работе физических лиц с ПАС. Номенклатура ПАС, применяемых ФЛ при работе с ДС: специальные программные средства, устанавливаемые на ПЭВМ, смартфонах, планшетах; наборы «логинов-паролей»; «электронные ключи» для выполнения операций Интернет-банкинга (в прошлом использовались «ключевые дискеты»); платежные карты со встроенными чипами (микросхемами).

Основные причины угроз для ФЛ при работе с ДС: 1) Недостаточное внимание, в т.ч. в отношении распознавания фальсифицированных монет и банкнот. 2) Невысокий уровень ИТКК, приводящий к слабой доступности ряда услуг. 3) Возможность получения инфекционных заболеваний при работе с НД и пр. 4) Недостаточная защищенность ОС используемых ПАС – особенно мобильных устройств. 5) Постоянное появление новых угроз, основанных на выявившихся уязвимых местах в используемых программных средствах, включая ОС. 6) Обновление операторами ЭРПС, в т.ч. операторами систем ЭД, интерфейсов может разрушать у пользователей сложившиеся динамические стереотипы выполнения типичных операций. 7) Невнимательное отношение пользователей к средствам защиты (хранение логинов-паролей на устройствах и записей о PIN-кодах вместе с БК, разглашение информации о защитных средствах третьим лицам и пр.). 8) Не всегда оперативная работа служб технической поддержки. 9) Невнимательное отношение к чекам, выдаваемым ЭТ (чеки зачастую попадают в урны около ЭТ или даже остаются прямо в устройствах самообслуживания – это может привести к утечке персональных данных, включая финансовую информацию).

В современных ЭТ устанавливаются боковые щитки, ограничивающие возможность просмотра вводимых PIN-кодов сбоку и сверху. Однако, в специальной литературе и материалах, размещенных в Интернете, описаны способы, направленные на незаконное получение вводимых в ЭТ PIN-кодов (например, использование накладных клавиатур [13], миниатюрных видеокамер, зеркал и пр). Проще всего можно узнать PIN-код БК в торговых точках, т.к. используемые там картридеры не предусматривают какой-либо защиты от постороннего наблюдения при вводе владельцами БК PIN-кодов. Для несанкционированного списания ДС с карточного счета мошенникам достаточно получить PIN-код и завладеть БК (при условии, что она не заблокирована) или узнать только номер БК, срок ее действия и CVV/CVC, размещенные на пластике БК (при условии отсутствия дополнительных средств защиты, например, 3D-Secure).

Иногда злоумышленниками используются «фантомные банкоматы» (ФБ) – имитации реальных банкоматов, устанавливаемые на временной основе. Пользователь, вставив БК в ФБ и введя PIN-код, получает сообщение об ошибке. За это время ФБ считывает всю необходимую информацию и передает ее по беспроводному каналу связи. Злоумышленники изготавливают дубликат БК и обналичивают хранящиеся на ней средства. Характерные признаки ФБ: ненадежное крепление конструкции; располагаются в местах, где вблизи отсутствует источник энергопитания и др. [13]; используются названия вымышленных банков или банков, которые не работают в конкретном регионе. Такая же схема используется при получения доступа к ЭС в системе ЭД – злоумышленниками создаются «фантомные сайты».

Один из распространенных способов краж ДС со счетов – использование злоумышленниками вставных устройств для картоприемников в ЭТ, которые задерживают БК и не возвращают их владельцам [13].

Типичные виды неблагоприятных событий для ФиЮЛ. 1) Утрата или повреждение БК, которые делают невозможным их дальнейшее использование. 2) Необоснованные задержки БК в ЭТ, особенно находящихся далеко от офисов кредитных организаций. 3) Результативные хакерские атаки на банковские системы, приводящие к несанкционированным снятиям средств со счетов клиентов, связанных с БК. 4) Неработоспособность ЭТ, каналов связи или устройств пользователей именно в те моменты, когда необходимо провести операции с ДС и пр.

Методы риск-менеджмента: 1) соблюдение мер предосторожности при работе с ЭТ и- в т.ч. при введении PIN-кодов; 2) использование SMS-оповещений для информирования о движении средств по счетам; 3) исключение возможностей передачи (даже кратковременной) БК в «чужие руки»; 4) повышение личной ИТКК пользователей; 5) соблюдение мер предосторожности при загрузке неизвестного ПО на мобильные устройства и стационарные ПЭВМ; 6) своевременное обновление антивирусных программ для ПАС и их баз вирусов; 7) организация эффективной работы служб технической поддержки со стороны эмитентов БК и пр.

Влияние квалификации специалистов и ИТКК населения на эффективность использования ЭРПС. Подготовка профильных специалистов для работы в экономической сфере осуществляется в вузах и средних специальных учебных заведениях.

Однако во многих организациях работает достаточно много специалистов, которые окончили вузы не по экономическим специальностям. Это касается, в первую очередь, тех лиц, которые непосредственно работают с деньгами, осуществляя их прием в наличной форме и проведение платежей с применением предусмотренных законом форм безналичных расчетов.

В тоже время на инженерно-технических должностях трудятся преимущественно лица, получившие профильное вузовское образование. Обращаем внимание на тот факт, что на всероссийском уровне не предусмотрено какой-то унифицированной системы аттестации специалистов по ИБ, работающих в финансовом секторе.

В отношении населения отметим, отсутствие системы обучения работе с ДС, интерфейсами ЭТ и ЭРПС – в т.ч. в школах, техникумах и вузах. Как следствие, соответствующие знания и умения молодежь и лица среднего возраста приобретают «на практике», а также путем получения консультаций друг у друга. Именно поэтому представляется целесообразной реализация в образовательных учреждениях специальных программ (проектов) повышения ИТКК, связанной с использованием ДС.

Направления таких проектов для населения. 1) Разработка мультимедийных учебных курсов, имеющих целью приобретение практических навыков работы с ДС, устройствами самообслуживания, интерфейсами ЭТ и ЭРПС (в т.ч. с системами ЭД) и пр. 2) Разработка устройств-имитаторов ЭТ, позволяющих практически отработать навыки их использования путем многократного повторения типовых операций. 3) Разработка игровых программ по обучению использования средств управления ЭД. 4) Создание игровых программ, позволяющих имитировать различные виды угроз информационной, криминальной и физической безопасности в отношении пользователей ДС, а также действия по защите от них.

Для будущих специалистов инженерно-технического профиля этот перечень может быть расширен за счет проектов, связанных с обеспечением надежности использования ПАС в условиях различных внешних угроз, включая хакерские атаки; проектирования различных устройств с использованием компьютерных САПР и пр. [2].

Для работников кредитно-финансовой сферы также могут реализовываться специальные проекты в отношении использования ПАС, которые будут обеспечивать повышение их профессиональной квалификации; отработку навыков работы с электронными системами управления ДС.

Планирование и реализация таких проектов могут осуществляться с использованием «методологии управления проектами»; специальных программных средств, в т.ч. эксплуатируемых по модели SaaS.

В особенно неблагоприятном положении в отношении использования ЭТ и ЭРПС (в т.ч. систем ЭД), в настоящее время оказались многие лица пожилого возраста. Растущие требования к ИТКК, квалификации пользователей ЭТ и программ Интернет-банкинга вынуждают таких лиц пользоваться услугами в лучшем случае консультантов организаций и родственников, а в худшем – посторонних лиц. Это снижает уровень ИБ проводимых ими транзакций и использования ЭРПС в целом.

Отметим, что в ряде регионов России, включая Астраханскую область, реализуются программы повышения «компьютерной грамотности» для пенсионеров. За рубежом также существуют специальные программы повышения ИТКК населения - в ряде стран они весьма эффективны [18].

Выводы. 1. Использование информационных технологий при работе с наличными, безналичными и ЭД обеспечивает дополнительные возможности для ФиЮЛ. 2. Однако одновременно для ФиЮЛ возникает целый ряд рисков, который необходимо учитывать при принятии и реализации решений. В частности необходимо разрабатывать и реализовывать меры по снижению вероятностей возникновения неблагоприятных событий, а также ущербов от этих событий. 3. Такие меры могут осуществляться как на макроуровне (государство), так и на микроуровне (ФиЮЛ). 4. При использовании современных средств работы с ДС важное значение имеет квалификация не только ИТ-специалистов, но и населения. 5. Повышение уровня ИТКК населения можно обеспечить, разрабатывая и реализуя целевые программы – как общегосударственные, так и внутрирегиональные.

Список литературы

1. Ажмухамедов И. М., Князева О. М., Большакова Л. В. Оценка уровня информационной безопасности финансовых учреждений / И. М. Ажмухамедов, О. М. Князева, Л. В. Большакова // Современные проблемы науки и образования. – 2015. – № 1. – Режим доступа: http://www.science-education.ru/121-18408 (дата обращения 14.03.2016), свободный. – Заглавие с экрана. – Яз. рус.

2. Ажмухамедов И. М. Методика оценки компетенций специалиста в области информационной безопасности / И. М. Ажмухамедов // Проблемы информационной безопасности. Компьютерные системы. – № 4. – 2010. – С. 65–70.

3. Аксенов В. С. К вопросу об интерпретации электронных денег / В. С. Аксенов // Вестник Российского государственного гуманитарного университета – 2011. – № 10 – С. 14–22.

4. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных системах : монография / И. В. Аникин. – Казань : Редакционно-издательский центр «Школа», 2015. – 224 с.

5. Банковский кодекс Республики Беларусь. – Режим доступа: http://www.pravo.by/main.aspx?guid=6361 (дата обращения 01.03.2016) , свободный. – Заглавие с экрана. – Яз. рус.

6. Бабаева О. Б. Электронные деньги и платежные системы / О. Б. Бабаева // Economics. – 2015. – № 3 (4). – С. 33–36.

7. Бецков А. В. Безопасность и надежность системы защиты объекта / А. В. Бецков // Надежность и качество сложных систем. – 2013. – № 1. – С. 35–40.

8. Бойченко О.В. Проблемы информационной безопасности платежных средств / О. В. Бойченко // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. – 2014. – Т. 1, № 27 (66). – С. 12–17.

9. Брумштейн Ю. М. Анализ некоторых моделей группового управления рисками / Ю. М. Брумштейн, О. Н. Выборнова // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 4. – С. 64–72.

10. Брумштейн Ю. М. Анализ рисков информационной безопасности организаций, связанных с расположением, конструкциями и особенностями эксплуатации зданий / Ю. М. Брумштейн, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 4. – С. 148–167.

11. Брумштейн Ю. М. ИКТ-компетентность стран, регионов, организаций и физических лиц: системный анализ целей, направлений и методов оценки / Ю. М. Брумштейн, А. Б. Кузьмина // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 2. – С. 47–63.

12. Брумштейн Ю. М. Оптимизация распределения персонала между подразделениями организаций на основе компетентностного подхода / Ю. М. Брумштейн, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 2 – С. 45–58.

13. Виды мошенничества с банковскими картами. – Режим доступа: http://www.moneybanki.ru/article/vidy-moshennichestva-s-bankovskimi-kartami/ (дата обращения 10.03.2016), свободный. – Заглавие с экрана. – Яз. рус.

14. Директива 2007/64/ЕС Европейского парламента и Совета ЕС от 13 ноября 2007 года о платежных услугах на внутреннем рынке, вносящая изменения в Директивы 97/7/ЕС, 2002/65/ЕС, 2005/60/ЕС и 2006/48/ЕС и отменяющая Директиву 97/5/ЕС / // Платежные и расчетные системы. Международный опыт – 2009. – № 18 – 48 с.

15. Директива 2009/110/ЕС Европейского парламента и Совета ЕС от 16 сентября 2009 года об организации, деятельности и пруденциальном надзоре за деятельностью учреждений электронных денег, вносящая изменения в Директивы 2005/60/ЕС и 2006/48/ЕС и отменяющая Директиву 2000/46/ЕС // Платежные и расчетные системы. Международный опыт – 2011. – № 25 – 74 с.

16. Журавлева В. В. Особенности информационной безопасности банковских систем и меры по ее обеспечению / В. В. Журавлева, А. Н. Целых // Альманах современной науки и образования. – 2015. – № 9 (99). – С. 67–71.

17. Иванов А. П. Информационная безопасность электронных платежных систем / А. П. Иванов, Е. А. Войнова, М. С. Тикин // Информация и безопасность. – 2012. – Т. 15, № 3. – С. 437–438.

18. Кузьмина А. Б. Анализ опыта управления ИТ-компетентностью физических и юридических лиц в некоторых зарубежных странах / А. Б. Кузьмина // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 2. – С. 63–76.

19. Курбатов А. Я. Правовое регулирование электронных платежных систем по законодательству Российской Федерации / А. Я. Курбатов // Хозяйство и право. – 2007. – № 9. – С. 68–84.

20. Лившиц И. И. Анализ уязвимостей и угроз национальной платежной системы Российской Федерации / И. И. Лившиц // Вопросы защиты информации. – 2015. – № 1 (108). – С. 75–80.

21. Мазур В. И. Обзор проблем информационной безопасности международных платежных систем / В. И. Мазур, А. В. Иванкевич // Безпека інформації. – 2014. – Т. 1, № 20. – С. 97–101.

22. Нефедова М. Платежная система отелей Хайятт подверглась взлому / М. Нефедова. – Режим доступа: https://xakep.ru/2015/12/25/hyatt-hotels-corporation-hack/, свободный. – Заглавие с экрана. – Яз. рус.

23. О предоставлении клиентам – физическим лицам информации об особенностях оказания услуг по переводу электронных денежных средств от 20.12.2013 : письмо Банка России № 249-Т // Вестник Банка России. – 2014. – № 2 (1480). – С. 20–22.

24. Российская Федерация. О национальной платежной системе от 27.06.2011 : федеральный закон № 161-ФЗ : [принят Государственной Думой 14 июня 2011 г. ; одобрен Советом Федерации 22 июня 2011 г. ; с изменениями и дополнениями от 01.03.2015] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru/document/cons_ doc_LAW_115625/ (дата обращения 02.03.2016), свободный. – Заглавие с экрана. – Яз. рус.

25. Смольянинова Е. Н. Проблемы безопасности расчетов пластиковыми картами / Е. Н. Смольянинова, Н. А. Духанина, А. Ц. Дашидондокова // Фундаментальные исследования. – 2015. – № 2–22. – С. 4969–4973.

26. Современный экономический словарь / Б. А. Райзберг, Л. Ш. Лозовский, Е. Б. Стародубцева / под ред. Б. А. Райзберг. – 6-е изд., перераб. и доп. – Москва : ИНФРА-М, 2011. – 512 с.

27. Танющева Н. Ю. Дискуссионные вопросы финансовой сущности электронных денег / Н. Ю. Танющева, Е. И. Дюдикова // Экономические науки. – 2015. – № 8 (129). – С. 134–137.

28. Хакеры внимательнее банкиров. – Режим доступа: https://news.mail.ru/economics/25154687/?frommail=102:11 (дата обращения 17.03.2016), свободный. – Заглавие с экрана. – Яз. рус.

29. Шаров А. Н. Эволюция денег при капитализме / А. Н. Шаров. – Москва : Финансы и статистика, 1990. – 139 с.

30. Шестакова К. Осторожно: новый Android-троян крадет данные из банковских приложений / К. Шестакова. – Режим доступа: https://hi-tech.mail.ru/news/spy-agent-si-android-trojan/ (дата обращения 12.03.2016), свободный. – Заглавие с экрана. – Яз. рус.

31. Юрков Н. К. Риски отказов сложных технических систем / Н. К. Юрков // Надежность и качество сложных систем. – 2014. – № 1. – С. 18–24.

32. Electronic money institutions current trends, regulatory issues and future prospects // Legal Working Paper Series European Central Bank – 2008. – № 7 – P. 48.

33. Yuzevych V. M. Economic analysis of the levels of efficiency and quality of Internet payment systems of enterprise / V. M. Yuzevych, O. V. Klyuvak // Бизнес-информ. – 2015. – № 1. – С. 160–164.

References

1. Azhmukhamedov I. M., Knyazeva O. M., Bolshakova L. V. Otsenka urovnya informatsionnoy bezopasnosti finansovykh uchrezhdeniy [Assessment of financial institutions information security level]. *Sovremennye problemy nauki i obrazovaniya* [Modern Problems of Science and Education], 2015, no. 1. Available at: http://www.science-education.ru/121-18408 (accessed 14.03.2016).

2. Azhmukhamedov I. M. Metodika otsenki kompetentsiy spetsialista v oblasti informatsionnoy bezopasnosti [A technique of an assessment of competences of the expert in information security field]. *Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy* [Problems of Information Security. Computer Systems], 2010, no. 4, pp. 65–70.

3. Aksenov V. S. K voprosu ob interpretatsii elektronnykh deneg [To a question of electronic money interpretation]. *Vestnik Rossiyskogo gosudarstvennogo gumanitarnogo universiteta* [Bulletin of the Russian State Humanitarian University], 2011, no. 10, pp. 14–22.

4. Anikin I. V. *Metody otsenki i upravleniya riskami informatsionnoy bezopasnosti v korporativnykh informatsionnykh sistemakh* [Methods of an assessment and risk management of information security in corporate information systems], Kazan, Redaktsionno-izdatelskiy tsentr «Shkola» Publ., 2015. 224 p.

5. *Bankovskiy kodeks Respubliki Belarus* [Bank code of Belarus Republic]. Available at: http://www.pravo.by/main.aspx?guid=6361 (accessed 01.03.2016).

6. Babaeva O. B. Elektronnye dengi i platezhnye sistemy [Electronic money and payment service providers]. *Economics*, 2015, no. 3 (4), pp. 33–36.

7. Betskov A. V. Bezopasnost i nadezhnost sistemy zashchity obekta [Safety and reliability of object protection system]. *Nadezhnost i kachestvo slozhnykh system* [Reliability and Quality of Difficult Systems], 2013, no. 1, pp. 35–40.

8. Boychenko O. V. Problemy informatsionnoy bezopasnosti platezhnykh sredstv [Information security problems of payment means]. *Uchenye zapiski Krymskogo federalnogo universiteta imeni V. I. Vernadskogo. Ekonomika i upravlenie* [Proceedings of the Crimean Federal University of V. I. Vernadsky. Economics and Management], 2014, vol. 1, no. 27 (66), pp. 12–17.

9. Brumshteyn Yu. M., Vybornova O. N. Analiz nekotorykh modeley gruppovo-go upravleniya riskami [Analysis of some models of group risk management]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [The Caspian Journal: Management and High Technologies], 2015, no. 4, pp. 64–72.

10. Brumshteyn Yu. M., Dyudikov I. A. Analiz riskov informatsionnoy bezopas-nosti organizatsiy, svyazannykh s raspolozheniem, konstruktsiyami i osobennostyami eks-pluatatsii zdaniy [Risk analysis of organizations information safety, connected with an arrangement, designs and features of buildings exploitation]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [The Caspian Journal: Management and High Technologies], 2015, no. 4, pp. 148–167.

11. Brumshteyn Yu. M., Kuzmina A. B. IKT-kompetentnost stran, regionov, organizatsiy i fizicheskikh lits: sistemnyy analiz tseley, napravleniy i metodov otsenki [IKT-competence of the countries, regions, organizations and natural persons: system analysis of the purposes, directions and assessment methods]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [The Caspian Journal: Management and High Technologies], 2014, no. 2, pp. 47–63.

12. Brumshteyn Yu. M., Dyudikov I. A. Optimizatsiya raspredeleniya personala mezhdu podrazdeleniyami organizatsiy na osnove kompetentnostnogo podkhoda [Optimization of distribution of personnel between divisions of the organizations on the basis of competence-based approach]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [The Caspian Journal: Management and High Technologies], 2015, no. 2, pp. 45–58.

13. *Vidy moshennichestva s bankovskimi kartami* [Types of fraud with cash cards]. Available at: http://www.moneybanki.ru/article/vidy-moshennichestva-s-bankovskimi-kartami/ (accessed 10.03.2016).

14. Direktiva 2007/64/YeS Yevropeyskogo parlamenta i Soveta YeS ot 13 noyabrya 2007 goda o platezhnykh uslugakh na vnutrennem rynke, vnosyashchaya izmeneniya v Direktivy 97/7/YeS, 2002/65/YeS, 2005/60/YeS i 2006/48/YeS i otmenyayushchaya Direktivu 97/5/YeS / [The directive 2007/64/EU of the European parliament and Council of November 13, 2007 about payment services in domestic market making changes to Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and canceling the Directive 97/5/EU]. *Platezhnye i raschetnye sistemy. Mezhdunarodnyy opyt* [Payment Service and Settlement Providers. The International Experience], 2009, no. 18. 48 p.

15. Direktiva 2009/110/YeS Yevropeyskogo parlamenta i Soveta YeS ot 16 sentyabrya 2009 goda ob organizatsii, deyatelnosti i prudentsialnom nadzore za deyatelnostyu uchrezhdeniy elektronnykh deneg, vnosyashchaya izmeneniya v Direktivy 2005/60/YeS i 2006/48/YeS i otmenyayushchaya Direktivu 2000/46/EC [The directive 2009/110/EU of the European parliament and EU Council of September 16, 2009 about the organization, activity and prudential supervision of activity of establishments of electronic money making changes to Directives 2005/60/EU and 2006/48/EU and canceling the Directive 2000/46/EC]. *Platezhnye i raschetnye sistemy. Mezhdunarodnyy opyt* [Payment Service and Settlement Providers. The International Experience], 2011, no. 25. 74 p.

16. Zhuravleva V. V., Tselykh A. N. Osobennosti informatsionnoy bezopasnosti bankovskikh sistem i mery po ee obespecheniyu [Features of information security of banking systems and measure for her providing]. *Almanakh sovremennoy nauki i obrazovaniya* [Almanac of the Modern Science and Education], 2015, no. 9 (99), pp. 67–71.

17. Ivanov A. P., Voynova Ye. A., Tikin M. S. Informatsionnaya bezopasnost elektronnykh platezhnykh sistem [Information security of electronic payment service providers]. *Informatsiya i bezopasnost* [Information and Safety], 2012, vol. 15, no. 3, pp. 437–438.

18. Kuzmina A. B. Analiz opyta upravleniya IT-kompetentnostyu fizicheskikh i yuridicheskikh lits v nekotorykh zarubezhnykh stranakh [Analysis of experience of management of IT competence of physical and legal entities in some foreign countries]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [The Caspian Journal: Management and High Technologies], 2014, no. 2, pp. 63–76.

19. Kurbatov A. Ya. Pravovoe regulirovanie elektronnykh platezhnykh sistem po zakonodatelstvu Rossiyskoy Federatsii [Legal regulation of electronic payment service providers by the legislation of the Russian Federation]. *Khozyaystvo i pravo* [Economy and the Law], 2007, no. 9, pp. 68–84.

20. Livshits I. I. Analiz uyazvimostey i i ugroz natsionalnoy platezhnoy sistemy Rossiyskoy Federatsii [Analysis of vulnerabilities and and threats of national payment service provider of the Russian Federation]. *Voprosy zashchity informatsii* [Questions of Information Security], 2015, no. 1 (108), pp. 75–80.

21. Mazur V. I., Ivankevich A. V. Obzor problem informatsionnoy bezopas-nosti mezhdunarodnykh platezhnykh sistem [Review of information safety problems of the international payment service providers]. *Bezpeka informatsii* [Information Safety], 2014, vol. 1, no. 20, pp. 97–101.

22. Nefedova M. Platezhnaya sistema oteley Khayyatt podverglas vzlomu [The payment service provider of hotels Hyatt has undergone breaking]. Available at: https://xakep.ru/2015/12/25/hyatt-hotels-corporation-hack/.

23. About granting to clients - to natural persons of information on features of rendering services in the translation of electronic money of December 20, 2013. The Letter of the Bank of Russia no. 249-T]. *Vestnik Banka Rossii* [Bulletin of the Bank Russia], 2014, no. 2 (1480), pp. 20–22.

24. Russian Federation. About national payment service provider of June 27, 2011. Federal Law no. 161-FZ. Adopted by the State Duma on June 14, 2011, approved by Federation Council June 22, 2011, amended on March 1, 2015. *ConsultantPlyus* [ConsultantPlus]. Available at: http://www.consultant.ru/document/cons_doc_LAW_115625/ (accessed 02.03.2016).

25. Smolyaninova Ye. N., Dukhanina N. A., Dashidondokova A. Ts. Problemy bezopasnosti raschetov plastikovymi kartami [Safety Problems of payments with plastic cards]. *Fundamentalnye issledovaniya* [Fundamental Researches], 2015, no. 2–22, pp. 4969–4973.

26. Rayzberg B. A., Lozovskiy L. Sh., Starodubtseva Ye. B. *Sovremennyy ekonomicheskiy slovar* [Modern economic dictionary], 6th ed., Moscow, INFRA-M Publ., 2011. 512 p.

27. Tanyushcheva N. Yu., Dyudikova Ye. I. Diskussionnye voprosy finansovoy sushchnosti elektronnykh deneg [Debatable questions of financial essence of electronic money]. *Ekonomicheskie nauki* [Economic Sciences], 2015, no. 8 (129), pp. 134–137.

28. *Khakery vnimatelnee bankirov* [Hackers are more attentive than bankers]. Available at: https://news.mail.ru/economics/25154687/?frommail=102:11 (accessed 17.03.2016).

29. Sharov A. N. *Evolyutsiya deneg pri kapitalizme* [Evolyution of money under capitalism], Moscow, Finansy i statistika Publ., 1990. 139 p.

30. Shestakova K. *Ostorozhno: novyy Android-troyan kradet dannye iz ban-kovskikh prilozheniy* [Be carefully: the new Android-trojan steals data from banking applications]. Available at: https://hi-tech.mail.ru/news/spy-agent-si-android-trojan/ (accessed 12.03.2016).

31. Yurkov N. K. Riski otkazov slozhnykh tekhnicheskikh sistem [Risks of complex technical systems refusals]. *Nadezhnost i kachestvo slozhnykh system* [Reliability and Quality of Complex Systems], 2014, no. 1, pp. 18–24.

32. Electronic money institutions current trends, regulatory issues and future prospects [Electronic money institutions current trends, regulatory issues and future prospects]. *Legal Working Paper Series European Central Bank* [Legal Working Paper Series European Central Bank], 2008, no. 7, pp. 48.

33. Yuzevych V. M., Klyuvak O. V. Economic analysis of the levels of efficiency and quality of Internet payment systems of enterprise. *Biznes-inform* [Business Inform], 2015, no. 1, pp. 160–164.

УДК 338.2+65

АНАЛИЗ ПОДХОДОВ К ВОПРОСАМ РИСК-МЕНЕДЖМЕНТА В КОРПОРАТИВНОМ УПРАВЛЕНИИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ РОССИИ

Статья поступила в редакцию 03.02.2016, в окончательном варианте 22.03.2016

Лозовая Ирина Сергеевна, начальник отдела по обеспечению управления имущественным комплексом, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: zlata_bully@inbox.ru

Рассмотрены международный и отечественный опыт использования организационных решений в системе риск-менеджмента (РМ) промышленных предприятий (ПП). Приведены определения риска с точки зрения международных и российских стандартов в области РМ. Выполнен анализ использования инструментов РМ в корпоративном управлении 23-х крупных российских ПП и 9 ПП Астраханской области. На основе проведенного анализа данных по ПП предложена оригинальная общая классификация рисков. Для процесса планирования и реализации системы РМ показан типичный вариант взаимодействия между советом директоров предприятия и «комитетом по рискам при совете директоров». Выявлены региональные особенности управления рисками на ПП Астраханской области. Показана целесообразность создания комитетов по рискам при советах директоров ПП.

Ключевые слова: риск-менеджмент, корпоративное управление, международный опыт, российские промышленные предприятия, совет директоров, комитет по рискам, акционерные общества, организация экономического сотрудничества и развития, Астраханская область

THE ANALYSIS OF THE MAIN DIRECTIONS AND THE EXISTING QUESTIONS OF RISK-MANAGEMENT AT THE LARGE INDUSTRIAL ENTERPRISES OF RUSSIA

Lozovaja Irina S., head of the Department of Ensure the Property Complex Management, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: zlata_bully@inbox.ru

In article are considered international and domestic experience of organizational decisions usage in risk-management (RM) systems at industrial enterprises (IE). The paper proposes definitions of risk from the point of view of the International and Russian standards in the field of RM. The author dwells on the analysis of RM tools usage in corporate board of 23 large Russian IE and 9 IE of the Astrakhan region – on the basis of enterprises data analysis. According to this analysis in article is offered the original general classification of risks. Author is shown the typical variant of interaction between enterprises directors' board and «committee by risks at directors' board» – for planning and realization of