УДК 338-2
DOI 10.30914/2411-9687-2021-7-1-89-95

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРУПНЫХ СУБЪЕКТОВ ОТЕЧЕСТВЕННОЙ ЭКОНОМИКИ

А. В. Швецов, Н. К. Швецова

Марийский государственный университет, г. Йошкар-Ола, Российская Федерация

Аннотация. ***Введение.*** С развитием систем передачи и обработки данных и переводом все большего числа бизнес-процессов предприятий и организаций в онлайн-режим возникает проблема защиты данных. Наибольшие риски сопутствуют финансовым организациям, оперирующим существенным объемом финансовых ресурсов. Удобство и экономия цифровых банковских услуг несут определенные риски: теперь для того, чтобы ограбить банк, достаточно найти лазейку в банковском программном обеспечении. В свою очередь банки теперь охраняют не только свои физические отделения, но и виртуальные. ***Цель*****:** исследовать современные тенденции влияния угроз информационной безопасности на крупнейшие субъекты российской экономики с учетом развития отечественных и мировых технологических решений. ***Материалы и методы.*** В работе использованы материалы периодической печати, данные о финансово-хозяйственной деятельности отдельных предприятий отечественной экономики. ***Результаты исследования, обсуждения.*** Рост спроса на системы защиты связан с заметным ростом киберпреступности. Число хакерских атак в мире продолжает стремительно расти, особенно на фоне спешного перехода многих компаний на удаленную работу. Работающие в сфере ИБ российские компании жалуются на нехватку инвестиций для создания новых продуктов. Емкость внутреннего российского ИТ-рынка не позволяет отечественным компаниям масштабировать бизнес и привлекать средства инвесторов для развития. Эволюция киберугроз идет быстрыми темпами, сейчас киберпреступники – это технически очень продвинутые группировки, их бизнес исчисляется миллиардами долларов. Чтобы противостоять столь мощному теневому бизнесу, компаниям в сфере информационной защиты самим нужны значимые инвестиции. Кража, утечка, уничтожение данных могут иметь серьезные последствия как для граждан, бизнеса, так и государства в целом. Одним из решений по защите информации является развитие квантовых коммуникаций, обеспечивающих наивысшую из существующих на сегодня степень защиты передачи данных. ***Заключение.*** Несмотря на объективные сложности, работа в направлении средств защиты информации в банковской и телекоммуникационной сферах ведется достаточно активно, однако, на наш взгляд, необходимо более активное участие государства, в том числе с учетом значительных, но неиспользуемых в экономике ресурсов фонда национального благосостояния.

Ключевые слова: информационная безопасность, экономический ущерб, киберугроза, киберпреступность, скимминг, процессинг, квантовый генератор, виртуальные частные сети, дата-центр

Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: *Швецов А.В., Швецова Н.К.* Проблемы и перспективы информационной безопасности крупных субъектов отечественной экономики // Вестник Марийского государственного университета. Серия «Сельскохозяйственные науки. Экономические науки». 2021. Т. 7. № 1. С. 89–95. DOI: https://doi.org/10.30914/2411-9687-2021-7-1-89-95

PROBLEMS AND PROSPECTS OF INFORMATION SECURITY OF LARGE SUBJECTS OF THE DOMESTIC ECONOMY

A. V. Shvetsov, N. K. Shvetsova

Mari State University, Yoshkar-Ola, Russian Federation

Abstract. ***Introduction.*** With the development of data transmission and processing systems and the transfer of an increasing number of business processes of enterprises and organizations to the online mode, the problem of data protection arises. The greatest risks are associated with financial organizations that operate with a significant amount of financial resources. The convenience and economy of digital banking services carry certain risks: now, in order to rob a bank, it is enough to find a loophole in the banking software. In turn, banks now protect not only their physical branches, but also virtual ones. ***Purpose*****:** to study the current trends in the impact of information security threats on the largest subjects of the Russian economy, taking into account the development

of domestic and global technological solutions. ***Materials and methods.*** The paper uses materials from periodicals, data on the financial and economic activities of individual enterprises of the domestic economy. ***Research results, discussion.*** The growing demand for security systems is associated with a noticeable increase in cybercrime. The number of hacker attacks in the world continues to grow rapidly, especially against the background of the hasty transition of many companies to remote work. Russian companies working in the field of information security complain about the lack of investment to create new products. The capacity of the domestic Russian IT market does not allow domestic companies to scale their business and attract investor funds for development. Cyber threats are evolving at a rapid pace, now cybercriminals are technically very advanced groups, their business is estimated at billions of dollars. To counter such a powerful shadow business, information security companies themselves need significant investments. Theft, leakage, and destruction of data can have serious consequences for citizens, businesses, and the state as a whole. One of the solutions for the protection of information is the development of quantum communications, which provide the highest degree of data transmission protection available today. ***Conclusion.*** Despite the objective difficulties, work in the direction of information security in the banking and telecommunications sectors is quite active, but in our opinion, more active participation of the state is necessary, including taking into account the significant, but unused resources of the National welfare fund in the economy.

Keywords: information security, economic damage, cyber threat, cybercrime, skimming, processing, quantum generator, virtual private networks, data center

The authors declare no conflict of interests.

For citation: *Shvetsov A.V., Shvetsova N.K.* Problems and prospects of information security of large subjects of the domestic economy. *Vestnik of the Mari State University. Chapter "Agriculture. Economics"*. 2021, vol. 7, no. 1, pp. 89–95. (In Russ.). DOI: https://doi.org/10.30914/2411-9687-2021-7-1-89-95

Введение

Все большее использование интернет-технологий для осуществления торговли ценными бумагами, расширения сферы электронных расчетов, интернет-коммерции, автоматизации многочисленных функций в сфере бизнеса приводит к новой специфической области криминальной активности. При растущей в мире глобализации и создании «информационного общества» формируется новый фактор, который способен подвергать угрозе экономическую безопасность – «киберпреступность» [6].

Цель работы: провести анализ современных тенденций влияния угроз информационной безопасности на крупнейшие субъекты российской экономики с учетом развития отечественных и мировых технологических решений, в том числе в рамках противодействия данным угрозам.

Основная часть

Специалисты по информационной безопасности банковской сферы рассматривают четыре основные группы угроз. Во-первых, это угрозы, связанные с атаками непосредственно на банк, когда злоумышленники ищут доступные для несанкционированных операций платежные системы и шлюзы, стараясь либо добавить туда платежи, либо модифицировать уже существующие[1].

Ко второй группе угроз следует отнести атаки на клиентов банка посредством получения доступа к личным кабинетам клиентов в дистанционном банковском обслуживании (ДБО), а также совершение переводов с карты на карту от имени клиентов.

Еще одна группа угроз – атаки на банкоматы и терминалы для приема денежных средств. Технически это либо использование программных средств, которые выдают деньги без карт, либо какие-то программы, которые говорят от имени терминала. Использование чиповых карт снизило вероятность угрозы, связанны со скиммингом, когда в устройство для работы с картами встраивается специальная накладка, которая копирует карту, после чего остается только узнать пин-код и можно карточку использовать, создав дубликат, что было распространено десятилетие назад.

К четвертой группе угроз следует отнести разглашение клиентских данных. Подобным противоправным деяниям противостоит законодательство,

[1] Угрозы информационной безопасности банка [Электронный ресурс]. URL: http://www.market-pages.ru/uprbez/8.html (дата обращения: 10.02.2021).

связанное с соблюдением банковской тайны, в том числе с защитой персональных данных, как наше отечественное, так и требования Еврокомиссии (GDPR). Правовая сторона регулирования интернет-услуг заключается в том, что они развиваются исключительно быстро, вследствие чего нормативно-правовая база регулирования данной сферы практически всегда отстает от потребностей самого государства и общества. Вместе с тем недостаточность правового регулирования сферы оказания интернет-услуг связана с отсутствием единого подхода к сущности виртуального пространства сети Интернет с правовой точки зрения [4].

Если рассматривать подобные преступления во временном аспекте, то нужно вспомнить, что злоумышленники начали активно атаковать банки в 2014 году. Эти преступления были связаны с изменениями платежной информации, когда во внешние платежи платежной системы корреспондентских счетов добавлялись платежи злоумышленников. Так как «приказы» приходили от имени банка, они исполнялись, происходило зачисление денежных средств в других банках. При этом было понятно, что виновен тот банк, который взломали и от имени которого были направлены соответствующие платежные инструкции. В таком состоянии банковская сфера прожила несколько лет. Затем технология преступлений поменялась и в 2016 году злоумышленники стали атаковать процессинги, то есть внутренние банковские системы совершения операций. В этом случае на картах искусственно увеличивали баланс, а затем с карт снимались приписанные денежные средства. Через год целью стал SWIFT – с валютных счетов деньги перечислялись на специально подготовленные счета юридических лиц в других банках. За эти нелегальные операции также платил атакованный банк, потому что, по сути, списания проводились с его счетов. Потом общими усилиями служб информационной безопасности в банках и «ФинЦЕРТа» (орган в ЦБ по информационной безопасности.) этот тренд удалось переломить. На сегодняшний день 98,5 % преступлений, совершенных в финансовой среде, составляют киберпреступления. При этом способами их совершения наиболее часто выступают социальная инженерия, скимминг и фишинг [1].

В настоящее время проникновение в банк происходит как правило, через электронную почту, когда злоумышленник отправляет вредоносное вложение работнику банка и определенным способом вынуждают открыть его. В результате зараженный компьютер выбирает некоторую цель для финансовой атаки.

В целом для успешной борьбы с банковскими преступлениями соответствующие подразделения банка должны выработать стратегию, основанную на анализе существующих угроз и рисков с учетом развития технологий, обеспечивающих информационную безопасность и тех ресурсов, которыми обладает данное финансовое учреждение.

При создании или модификации какого-либо информационного продукта в банковской сфере необходимо не только предусмотреть его безопасность с точки зрения уязвимости кода, но и сделать его удобным для клиента.

Помимо электронной почты существует большое количество различных сервисов, которые доступны из глобальной сети, которые можно использовать как потенциальные платформы для атак. Кроме того, возможна организация атак через третьи стороны, когда у финансовой организации есть интеграция с каким-то партнером. В том случае если банковский контрагент менее защищен, а банк не подумал о том, что нужно защищаться еще и от него, можно ждать атаки с этой стороны. При организации злоумышленниками целенаправленных атак используются вредоносы, которые не определяются стандартным антивирусным ПО. У преступников есть специальные сервисы, которые не сообщают вендорам о найденных вредоносах, на них мошенники тестируют свои вложения, и поэтому стандартные антивирусы уже не спасают. В банках используются достаточно сложные решения под названием «песочницы», работа которых построена на моделировании ситуации с открытием вложения или пользователь пройдет по указанной в письме ссылке. Если «песочница» видит, что происходят действия, которые не должны происходить от обычного текстового файла или при визите на определенный сайт, письмо помещается на карантин для ручного анализа.

Одной из угроз для клиента финансовой организации является угроза раскрытия персональных данных для третьих лиц. С этой целью действия организации должны быть нацелены на минимизацию количества работников, имеющих доступ к персональным данным. Основным требованием к отчетным данным или оперативным

запросам является отсутствие персональных данных клиентов. Если мы говорить про уровень прикладных информационных систем, то это управление доступом, то есть определение сотрудникам доступа, только необходимого для работы функционала.

В дополнение к стандартным мерам безопасности, принимаемых банками, их клиенты или пользователи банковских информационных продуктов также должны предпринимать определенные меры для снижения рисков потери в конечном итоге своих денежных средств. К таким мерам следует отнести обновление операционных систем, отказ от установки непроверенных приложений, визуальную проверку ссылок от неизвестных источников, отказ от открытия неизвестных вложений. При скачивании и установке мобильного сервиса следует обратить внимание на количество скачиваний и рейтинги приложений, чтобы понять, насколько они легитимны и востребованы. Это избавляет от установки фальшивого банковского приложения.

Подобные преступления характерны не только для банковской сферы. В зависимости от экономической выгоды киберпреступники могут потратить на одну хакерскую атаку полтора-два миллиона долларов.

Телекоммуникационные компании, являясь информационными площадками, интегрирующими большие объемы информации, вынуждены уделять серьезное внимание безопасности. Одним из способов является приобретение технологий информационной безопасности, в том числе путем слияния или поглощения компаний, занимающихся разработкой соответствующего ПО. В качестве примера можно привести сделку о приобретении компанией «Ростелеком» 49 % акций «Элвис-Плюс». Поглощаемая компания является одним из старейших российских разработчиков и интеграторов решений в области информационной безопасности: она была основана в 1991 году в Зеленограде технологическим предпринимателем Александром Галицким, который позже стал видным венчурным инвестором. Созданный им в 2008 году фонд Almaz Capital успешно инвестировал в «Яндекс» и другие перспективные российские ИТ-компании.

Компания «Элвис-Плюс» занималась разработкой систем передачи данных для спутников дистанционного зондирования поверхности Земли, компьютерных системы для орбитальной станции «Мир», систем космической связи. Партнером и инвестором компании стал американский хайтек-гигант Sun Microsystems, поглощенный в 2010 году компанией Oracle.

В рамках сотрудничества с американской компанией «Элвис-Плюс» разработала уникальные технологии беспроводной передачи данных (предвестник нынешнего Wi-Fi), а также успешный первый продукт виртуальных частных сетей (VPN) для Windows, лицензия на продажу которого была приобретена Sun Microsystems. В последние годы «Элвис-Плюс» занималась реализацией крупных проектов по интеграции решений по защите информационных систем у таких весомых заказчиков, как Банк России и «ЛУКойл». Согласно независимым оценкам, годовая выручка «Элвис-Плюс» на момент поглощения составляла более 500 млн рублей, что является неплохим результатом для IT-компаний сектора ИБ, хотя и сильно отстает от оборотов лидеров рынка: например, «Лаборатория Касперского» имеет годовой оборот порядка 50 млрд рублей (сюда входит не только российская, но и зарубежная деятельность компании), «Информзащита» – 8 млрд рублей.

По данным Tadviser, рынок решений для информационной безопасности в прошлом году достиг 90 млрд рублей, это более чем на 80 % превышает показатель 2014 года. Эксперты делят рынок информационной безопасности на такие ключевые сегменты, как программное обеспечение (ПО), аппаратные комплексы («железо») и сервисы. Лидеры рынка, например, «Лаборатория Касперского», успешно продвигают массовые продукты – ПО для конечных пользователей (антивирусные программы и проч.). Компания «Элвис-Плюс» успешно заняла на рынке ИБ нишу, связанную с защитой сетей клиентов (в частности, с помощью технологий виртуальных частных сетей VPN), которая находится на стыке разработки собственных программных продуктов, предоставления сервисов клиентам и продажи компьютерной техники (основными конкурентами компании сейчас являются «ИнфоТеКС» и «Код безопасности», которые также активно предлагают ИБ-решения на основе VPN, в том числе в крупных госструктурах). В частности, визитной карточкой «Элвис-Плюс» является семейство продуктов «Застава», которые обеспечивают защиту сетей корпоративных информационных систем (с помощью технологий VPN и так называемого межсетевого экранирования),

поэтому не случайно «Ростелеком», чей бизнес прежде всего связан с сетевыми решениями, обратил внимание именно на «Элвис-Плюс».

В ближайшие три года «Ростелеком» намерен вложить в развитие систем информационной безопасности более четырех миллиардов рублей, при этом компания не исключает поглощения других значимых игроков рынка. В результате «Ростелеком» планирует формировать внутри своей компании новый кластер услуг информационной безопасности. Проблема заключается в том, что, по словам специалистов по ИБ, компания отражает порядка трех тысяч кибератак в день, и число нападений быстро растет. И так как в настоящее время информационная безопасность является одним из самых быстрорастущих направлений ИТ-сферы, в перспективе компания планирует сделать его одним из трех ключевых видов бизнеса наряду с телекоммуникационными услугами и сервисами центров обработки данных.

В случае с «Элвис-Плюс» в результате продажи пакета акций российская компания получит важные для ее развития финансовые вливания, и объявленная сделка принесет пользу обеим сторонам. Появление на рынке нового системного интегратора в области информационной безопасности приведет к консолидации рынка информационной безопасности для оказания услуг в первую очередь клиентам из бюджетного сектора и государственным корпорациям.

Компания «Ростелеком», получившая в свое распоряжение мощный приток квалифицированных специалистов от «Элвис-Плюс», сможет реализовать гораздо большее число проектов, так как именно ресурсные ограничения выступали сдерживающим фактором роста при наличии высоких административных и лоббистских возможностей главного поставщика ИТ-услуг для госструктур. Таким образом, вероятно, на рынке может сложиться еще одна отраслевая госмонополия в сфере технологий информационной безопасности и такое партнерство будет полезно для защиты прежде всего государственных интересов.

В последнее время было объявлено сразу о нескольких отечественных проектах в отрасли высокотехнологичных методов защиты информации.

Квантовый генератор случайных чисел, о разработке которого заявлено учеными НИТУ МИСиС и Российского квантового центра в составе международной исследовательской группы, на сегодня самый быстрый в мире. Генерация случайных чисел является важнейшей задачей для различных областей, таких как криптография или моделирование сложных систем. Существующие генераторы случайных чисел достаточно медленны, что делает шифры уязвимыми [5].

В этом смысле только квантовые генераторы случайных чисел, представляющие отдельный тип физических генераторов, могут производить истинную случайную последовательность. Результаты измерений над квантовой системой, приготовленной каждый раз в одном и том же состоянии, носят принципиально случайный характер, поэтому истинная случайность имеет место только в квантовой области [2]. Он передает ключи шифрования через квантовую сеть, созданную для передачи закодированной информации в квантовых состояниях из одной точки в другую. По ней ключи шифрования передаются с помощью одиночных частиц – фотонов. Взломать такую связь незаметно не получится, поскольку зашифрованные данные по каналам этой связи передаются только тогда, когда квантово распределенные ключи переданы без ошибок и признаков перехвата. Одно из преимуществ такой связи состоит в том, что наладить ее можно на уже существующих оптоволоконных коммуникациях.

Подобные линии обеспечивают сверхнадежную защиту каналов передачи данных между дата-центрами, где размещены важнейшие информационные системы как внутренних, так и внешних заказчиков, в том числе государственные ИТ-системы. Центры обработки данных – высокотехнологичные сооружения для размещения вычислительного оборудования, предназначенного для обработки, хранения и распространения информации [3; 8; 7].

Следует отметить, что, несмотря на разработку и внедрение подобных проектов, их объем существенно уступает зарубежным, в частности китайским, проектам.

В начале этого года Университет науки и технологий КНР объявил о пуске первой в мире интегрированной сети квантовой связи протяженностью около 4600 километров, связавшей Пекин и Шанхай через узлы магистральной связи. К данной сети подключен ряд абонентов, нуждающихся в суперзащищенной связи – банки, крупные госкорпорации, промышленные предприятия и так далее.

К сожалению, пока в нашей стране крайне мало проектов, которые эксплуатировались бы сколько-нибудь длительное время. Пока квантовое шифрование находится на экспериментальной стадии,

участники развивают уже существующие способы математического шифрования.

На данный момент ключевые сферы, где необходимо внедрение технологии КРК, связаны с защитой особо важной информации, например персональных и биометрических данных. Но ее можно применять везде, где ценность информации высока, например в банковской сфере.

В ИТ-инфраструктуре крупных банков есть центры обработки данных, где хранится и резервируется важная информация, в том числе о клиентах и об операциях. Однако при появлении в распоряжении злоумышленников достаточно мощного квантового компьютера данная информация может быть скомпрометирована, если не будет предусмотрена ее соответствующая защита.

Еще одним практическим примером использования КРК-технологии может быть обновление ключей шифрования в банкоматах [9]. Традиционно это выполняется вручную доверенным персоналом и напоминает сеанс инкассации, но при использовании КРК в сети становится возможным обновлять ключи дистанционно, сократив расходы на выезд к каждому банкомату.

Выводы

Новые способы совершения противоправных действий основаны на использовании современных технологий, поэтому противодействовать данным угроза должны еще более современные технологии защиты информации. Над созданием квантово защищенных линий работают все крупные государства. Технологическими лидерами являются Китай и США. В России такие работы ведутся, но до их реализации еще далеко. Но здесь важна динамика процесса. В нашей стране устройства квантовой криптографии внедряются довольно активно, причем разными командами. Устройства для квантового распределения ключей в России разработали несколько команд, и следует говорить о здоровой конкуренции среди ученых и разработчиков. Специалисты данной сферы отмечают, что у России есть все возможности для того, чтобы быть среди ведущих держав в этой области. На старте отечественных разработок в этой сфере разрыв относительно мировых лидеров составлял двадцать лет, сейчас он сократился примерно до пяти лет.

Список литературы

1. Аминов И.И. Предупреждение киберпреступлений в финансовой сфере // Аллея науки. 2018. Т. 5. № 6 (22). С. 754–758.

2. Балыгин К.А., Зайцев В.И., Климов А.Н., Кулик С.П., Молотков С.Н. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов // Письма в Журнал экспериментальной и теоретической физики. 2017. Т. 106. № 7-8. С. 451–458.

3. Богданов С.В. Факторы, влияющие на рынок дата-центров в России // Вектор экономики. 2017. № 12 (18). С. 33.

4. Буланкина Е.В. Особенности современного этапа государственного регулирования сферы интернет-услуг в Российской Федерации // Бизнес. Образование. Право. 2018. № 1 (42). С. 69–73.

5. Втюрина А.Г., Елисеев В.Л., Жиляев А.Е., Николаева А.С., Сергеев В.Н., Уривский А.В. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 2. С. 15–21.

6. Коновалов А.А., Наумов С.А., Колесникова Д.Д. Киберпреступность как глобальная угроза экономичсекой безопасности: виды, особенности, проблемы противодействия // Ростовский научный журнал. 2018. № 1. С. 20–27.

7. Круглов В.И. Инструменты реализации информационной безопасности цифровой экономики России на примере ЗАО «КРОК» // Инновационная экономика. 2019. № 4 (21). С. 4–13.

8. Ларин А.А., Абросимов Л.И. Методика перераспределения функционирующих виртуальных машин по серверам в дата-центре // Вестник Московского энергетического института. 2018. № 1. С. 98–105.

9. Шевко Н.Р. Особенности обеспечения информационной безопасности банковской сферы // Ученые записки Казанского филиала «Российского государственного университета правосудия». 2020. Т. 16. С. 481–487.

Статья поступила в редакцию 18.02.2021; одобрена после рецензирования 15.03.2021; принята к публикации 5.04.2021.

Об авторах

Швецов Андрей Владимирович
доктор экономических наук, профессор, Марийский государственный университет (424000, Российская Федерация, г. Йошкар-Ола, пл. Ленина, д. 1), ORCID: https://orcid.org/0000-0003-3594-0636, *av.shvetsov@yandex.ru*

Швецова Наталия Кимовна
кандидат экономических наук, доцент, Марийский государственный университет (424000, Российская Федерация, г. Йошкар-Ола, пл. Ленина, д. 1), ORCID: https://orcid.org/0000-0002-0449-3864, *shvetsoff@rambler.ru*

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

1. Aminov I.I. Preduprezhdenie kiberprestuplenii v finansovoi sfere [The prevention of cybercrime in the financial sphere]. *Alleya nauki* = Alley of Science, 2018, vol. 5, no. 6(22), pp. 754–758. (In Russ.).

2. Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N. Realizatsiya kvantovogo generatora sluchainykh chisel, osnovannogo na optimal'noi gruppirovke fotootschetov [Implementation of a quantum random number generator based on the optimal clustering of photocounts]. *Pis'ma v Zhurnal eksperimental'noi i teoreticheskoi fiziki* = JETP Letters, 2017, vol. 106, no. 7–8, pp. 451–458. (In Russ.).

3. Bogdanov S.V. Faktory, vliyayushchie na rynok data-tsentrov v Rossii [Factors which influence the market of data centers in Russia]. *Vektor ekonomiki* = Vector economy, 2017, no. 12 (18), p. 33. (In Russ.).

4. Bulankina E.V. Osobennosti sovremennogo etapa gosudarstvennogo regulirovaniya sfery internet-uslug v Rossiiskoi Federatsii [Features of the modern stage of state regulation of Internet services sphere in the Russian Federation]. *Biznes. Obrazovanie. Pravo* = Business. Education. Law, 2018, no. 1 (42), pp. 69–73. (In Russ.).

5. Vtyurina A.G., Eliseev V.L., Zhilyaev A.E., Nikolaeva A.S., Sergeev V.N., Urivskii A.V. Realizatsiya sredstva kriptograficheskoi zashchity informatsii, ispol'zuyushchego kvantovoe raspredelenie klyuchei [On the principal decisions of the practical implementation of the cryptographic devices with quantum key distribution]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* = Proceedings of TUSUR University, 2018, vol. 21, no. 2, pp. 15–21. (In Russ.).

6. Konovalov A.A., Naumov S.A., Kolesnikova D.D. Kiberprestupnost' kak global'naya ugroza ekonomichsekoi bezopasnosti: vidy, osobennosti, problemy protivodeistviya [Cybercrime as a global threat to economic security: types, features, problems of counteraction]. *Rostovskii nauchnyi zhurnal* = Rostov Scientific Journal, 2018, no. 1, pp. 20–27. (In Russ.).

7. Kruglov V.I. Instrumenty realizatsii informatsionnoi bezopasnosti tsifrovoi ekonomiki Rossii na primere ZAO «KROK» [Tools for ensuring information security in the framework of the development of the digital economy of Russia]. *Innovatsionnaya ekonomika* = Innovative Economy, 2019, no. 4 (21), pp. 4–13. (In Russ.).

8. Larin A.A., Abrosimov L.I. Metodika pereraspredeleniya funktsioniruyushchikh virtual'nykh mashin po serveram v data-tsentre [A methodology for redistributing the operational virtual machines among the servers in a data center]. *Vestnik Moskovskogo energeticheskogo instituta* = Bulletin of MPEI, 2018, no. 1, pp. 98–105. (In Russ.).

9. Shevko N.R. Osobennosti obespecheniya informatsionnoi bezopasnosti bankovskoi sfery [Features of information security in the banking sector]. *Uchenye zapiski Kazanskogo filiala «Rossiiskogo gosudarstvennogo universiteta pravosudiya»* = Scientific Notes of the Kazan branch of the "Russian State University of Justice", 2020, vol. 16, pp. 481–487. (In Russ.).

The article was submitted 18.02.2021; approved after reviewing 15.03.2021; accepted for publication 5.04.2021.

About the authors

Andrey V. Shvetsov
Dr. Sci. (Economics), Professor, Mari State University (1. Lenin Sq., 424000 Yoshkar-Ola, Russian Federation), ORCID: https://orcid.org/0000-0003-3594-0636, *av.shvetsov@yandex.ru*

Natalia K. Shvetsova
Ph. D. (Economics), Associate Professor, Mari State University (1. Lenin Sq., 424000 Yoshkar-Ola, Russian Federation), ORCID: https://orcid.org/0000-0002-0449-3864, *shvetsoff@rambler.ru*

All authors have read and approved the final manuscript.