УДК 004.056
DOI: 10.28995/2782-2222-2022-3-53-68

Влияние сферы информационных технологий на экономическую безопасность государства и личности в новых реалиях

Владимир К. Спильниченко
Российский государственный гуманитарный университет, Москва, Россия, Spilnvladimir@yandex.ru

Аннотация. В статье предпринята попытка проанализировать влияние угроз безопасности в информационной сфере на экономическую безопасность. Рассматриваются пять групп изменений методов реализации угроз информационной безопасности, оказывающих значительное воздействие на экономическую безопасность государства и личности и нарушающих экономические процессы.

Ключевые слова: экономическая безопасность, методы реализации угроз безопасности в информационной сфере, финансовые угрозы информационной безопасности личности, кибератаки, социальная инжинирия, фишинг, атаки на банковские информационные системы, новые инфоповоды для мошеннических действий, программы вымогатели, вредоносные вирусы

Для цитирования: *Спильниченко В.К.* Влияние сферы информационных технологий на экономическую безопасность государства и личности в новых реалиях // Наука и искусство управления / Вестник Института экономики, управления и права Российского государственного гуманитарного университета. 2022. № 3. С. 53–68. DOI: 10.28995/2782-2222-2022-3-53-68

The impact of the information technology sphere on the economic security of the state and the individual in the new realities

Vladimir K. Spilnichenko
Russian State University of the Humanities, Moscow, Russia,
Spilnvladimir@yandex.ru

Abstract. This article attempts to analyze the methods of implementing security threats in the information sphere on economic security. It considers five groups of changes in methods of implementing information security threats that have a significant impact on the economic security of the state and the person and violate economic processes.

Keywords: economic security, methods of implementing security threats in the information sphere, financial threats to personal information security, cyber attacks, social engineering, phishing, attacks on banking information systems, new information links for fraudulent actions, ransomware, malicious viruses

For citation: Spilnichenko, V.K. (2022), "The impact of the information technology sphere on the economic security of the state and the individual in the new realities", *Science and Art of Management / Bulletin of the Institute of Economics, Management and Law of the Russian State University for the Humanities,* no. 3, pp. 53–68, DOI: 10.28995/2782-2222-2022-3-53-68

Введение

Принципиальные изменения во всех сферах экономической жизни российского общества повлекли за собой изменения в составе угроз экономической безопасности. В данной статье мы рассмотрим пороговые явления в области влияния угроз информационной безопасности на экономическую безопасность государства и личности в новых реалиях.

В научной литературе достаточно подробно анализируются само понятие «экономическая безопасность» и угрозы экономической безопасности как на уровне государства, так и на уровне регионов, хозяйствующих субъектов и личности. Мы разделяем точку зрения группы авторов, определяющих экономическую безопасность как

> ...показатель степени защищенности субъекта хозяйствования, его производственных и социальных отношений от негативного влияния внешних или внутренних факторов и способность к повышению уровня

> благосостояния народа, возможность определять внешнюю и внутреннюю политику развития хозяйства и формировать национальную безопасность [Кисова, Холчева 2019].

Однако российские исследователи, как правило, упускают из виду влияние на экономическую безопасность угроз, формирующихся в сфере информационных технологий. Причем некоторые авторы, рассматривающие угрозы экономической безопасности личности, вообще упускают аспекты, связанные с информационной безопасностью и безопасностью как таковой. Так, например, О.Н. Пряжникова утверждает,

> ...что касается связи экономического развития и безопасности, то практика показывает отсутствие между ними прямой зависимости [Пряжникова 2017].

Понимая, что именно агентность и самостоятельность человека при принятии жизненно важных экономических решений определяет существенное значение экономической информации в его жизни, стоит особо подчеркнуть умение правильно использовать эту информацию, отделять ложную информацию от реальной.

В условиях современной активной цифровизации экономики России, сопряженной с многочисленными санкциями, с одной стороны, и с существенной активизацией враждебных и мошеннических действий, с другой стороны, стоит более внимательно проанализировать влияние угроз информационной безопасности на экономическую безопасность государства и личности. Вследствие того, что информация, наряду с землей, трудом и капиталом, превращается в четвертый фактор производства, угрозы информационной безопасности могут существенно повлиять на экономические процессы вплоть до их разрушения.

К вопросу об угрозах информационной безопасности

Все угрозы можно разделить на две большие группы: технические угрозы и социальные угрозы. В данной статье мы проанализируем риски, связанные как с техническими, так и с социальными угрозами в новых реалиях. Больший акцент сделан на угрозы безопасности персональных данных. В конечном итоге реализация угроз безопасности персональных данных приводит к возрастанию финансовых угроз информационной безопасности личности и к со-

ответствующим финансовым потерям. При этом под финансовыми угрозами информационной безопасности личности понимается совокупность преступных действий мошенников, нацеленных на хищение финансовых средств человека или на отчуждение его имущественных прав, совершаемых при помощи информационно-коммуникационных технологий [Спильниченко, Соколов 2021].

Официальная трактовка понятия угроз безопасности персональных данных, актуальных при их обработке в информационных системах, дается в постановлении Правительства России от 1 ноября 2012 г. № 1119. Под актуальными угрозами безопасности персональных данных там понимается

> ...совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия[1].

Перечень из 10 таких угроз описывается в Указании Банка России от 10 декабря 2015 г. № 3889-У[2].

Введение санкций против Российской Федерации значительно повлияло на процессы информационного обеспечения экономики. Реализация современных угроз информационной безопасности может значительно ослабить экономический потенциал страны в целом, а также ее отдельных предприятий, граждан. Существует потенциальная опасность не только понести финансовые потери, но и вынужденно остановить работу некоторых предприятий, производящих разнообразную продукцию и услуги, если не принять вовремя экстренных мер по нейтрализации данных угроз.

---

[1] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100020 (дата обращения 15 апреля 2022).

[2] Указание Банка России от 10.12.2015 № 3889-У (ред. от 01.03.2022) «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_195662/ (дата обращения 15 апреля 2022).

Методы реализации угроз информационной безопасности

Нейтрализация отрицательного влияния угроз информационной безопасности на экономическую безопасность предполагает выяснение методов реализации этих угроз для организации действенных мер по их купированию. Под воздействием санкционных мер и изменений общественно-политической ситуации видоизменяются и методы реализации угроз информационной безопасности, оказывающие значительное воздействие на экономическую безопасность государства и личности и нарушающие экономические процессы. Эти изменения можно разделить на несколько групп.

Во-первых, существенно изменились условия ведения бизнеса в области информационных технологий [Наркевич 2022]. С одной стороны, вследствие эмбарго недружественных стран более 400 иностранных компаний приостановили свою деятельность в России. В результате заморожены поставки оборудования, остановлено обновление ПО, прекращена вендорская поддержка – техническая поддержка производителями эксплуатации поставленных ранее из-за рубежа информационных систем.

Для понимания масштабов проблемы приведем обобщающие данные по доле зарубежных ИТ-продуктов, используемых в нашей стране. По данным Ассоциации разработчиков программных продуктов «Отечественный софт», проникновение отечественных ИТ-продуктов в госсектор и госкомпании составляет 30–35%. При этом основа основ – платформенные решения – составляют менее 5%. Офисное ПО – около 10%. Прочее прикладное ПО – от 15 до 60% в отдельных областях. Лучше всего ситуация обстоит с информационной безопасностью – до 90%.

С другой стороны, уход с российского рынка иностранных компаний обусловил расширение возможностей для выхода на рынок отечественных ИТ-компаний, заполняющих образовавшиеся рыночные ниши [Бурлаков, Кемпа 2022]. По данным Минцифры, на российском рынке продаются около 13 тыс. отечественных программных продуктов. Правительство страны приняло ряд экономических и политических мер для скорейшего разрешения проблем, возникших в области ИТ. С позиций объективной оценки стоит отметить, что в целом проблема разработки различных программных продуктов и вендорского сопровождения вполне решаема в течение относительно небольшого промежутка времени.

Так, например, с середины марта 2022 г. к реализации программы ускоренного импортозамещения для российских компаний приступил уже ряд российских фирм [Чистякова, Артемов 2021].

В пакетах их предложений замена зарубежных программных решений на отечественный продукт, а также обеспечение вендорской поддержки используемых решений.

Главной проблемой на сегодняшний день остается поиск новых поставщиков или налаживание производства технических средств сетевой защиты, а в целом по комплексу информационных технологий – дефицит серверного и сетевого оборудования и аналитических систем необходимого класса. Для оперативного поиска российских аналогов зарубежных сервисов Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации опубликовало Перечень российских аналогов интернет-ресурсов и сервисов иностранных IT-компаний [Павлова 2021].

Во-вторых, происходит возврат к ранее используемым методам в условиях общего тревожного эмоционального фона с применением новых инфоповодов для атак. Один из ведущих разработчиков решений в области предотвращения кибератак Group-IB вскрыл активизацию атак на крупные компании русскоязычной группы вымогателей OldGremlin. В первом случае рассылались письма от имени старшего бухгалтера известной финансовой организации о необходимости оформления новых банковских карт для реализации зарплатных проектов в связи с уходом с рынка Visa и Mastercard. В другом случае рассылка производилась под именем одной из ведущих консалтинговых компаний с договором по действиям в условиях санкций, который при открытии заражал информационную сеть предприятия вредоносным вирусом. Ранее за два года вымогатели произвели 13 подобных кампаний.

Заметив подозрительные рассылки, специалисты Group-IB оперативно предупредили о них контрагентов. Однако не исключено, что может быть заражено значительное количество компаний, не сотрудничающих с группой, и поэтому необходимо оперативно произвести на предприятиях антивирусные мероприятия. В противном случае взлом инфраструктуры атакованных компаний может привести к самым неожиданным негативным последствиям – от кражи денег до сбоев технологических процессов, провоцирования технических аварий и катастроф.

На электронные адреса крупных компаний стали приходить письма с требованием оплатить бухгалтерские счета по новым реквизитам, так как, по утверждению авторов писем, ранее они были даны неверно. К письмам прилагаются счета на небольшую сумму в 800–1000 рублей с несущественными темами, например «оплата за доставку технической документации». Сотрудник бухгалтерии может посчитать сумму незначительной и оплатить счет без детального анализа. Если учесть, что только за период с 3 по

9 марта лабораторией Касперского обнаружено несколько тысяч подобных писем в разных компаниях, то можно легко просчитать возможный доход злоумышленников. Интересно, что подобные мошеннические действия не наблюдались уже много лет.

Существенно возросло число потерпевших от приобретения электронных полюсов ОСАГО. По данным Банка России, потери автовладельцев и страховщиков от противоправных действий при удаленном заключении договоров ОСАГО составляют не менее 4,2 млрд рублей в год.

Активно используется метод похищения учетных записей. Так, например, в марте этого года Сбербанк остановил массовое списание средств с карт клиентов при десятке тысяч попыток списаний за минуту. Всего было отклонено несколько сотен тысяч списаний. Списания были инициированы украинской фирмой, похитившей персональные данные клиентов при пользовании ее приложениями.

Наиболее предпочтительным для целевых атак злоумышленников является использование программ-вымогателей (Ransomware). За последние несколько лет средний платеж по вымогательству выкупа вырос с 7 тыс. долл. до 200 тыс., т. е. почти в 30 раз. Для отражения подобных атак достаточно регулярно копировать важную информацию в облако и на автономные локальные носители, производить актуальные обновления операционной системы сразу после их выпуска, круглосуточно мониторить состояние мер защиты – антивирусов, средств резервного копирования и межсетевых экранов.

Изменилась объективная картина применения атак с использованием социальной инженерии. С одной стороны, произошло некоторое сокращение числа звонков мошенников. Это связано с прекращением деятельности их call-центров на территории Украины. Примером такого центра служит помещение, обнаруженное в Бердянске. Вероятно, после передислокации подобных call-центров в западные районы страны или в недружественные страны число звонков может вернуться на прежний уровень или даже превзойти его.

С другой стороны, используются новые инфоповоды, связанные с санкционными действиями и изменением внешнеполитической обстановки. Мошенники предлагают перевести деньги на «безопасный счет» из банков, подвергшихся санкциям, с помощью которого можно перевести деньги за рубеж или просто «спасти» от потери. В связи с блокировкой некоторых приложений активно применяются предложения по приобретению платежных карт с подключением к ApplePay или GooglePay для оплаты покупок с помощью смартфона. Требования мошенников для проведения

указанных операций стандартны – предоставить копию паспорта с пропиской, оплатить первоначальный взнос или «выпуск карты». Такие действия чреваты не только потерей денег, но и тем, что мошенники могут, используя ваши данные, оформить на вас кредит или платежную карту, по которой проводить денежные операции.

Распространены и предложения по обходу санкций и скачиванию по отдельной ссылке файлов «специального приложения» AppStore, PlayMarket и AppGallery на Android после удаления из магазинов приложений мобильных версий некоторых отечественных банков. По состоянию на 25 апреля 2022 г. мера по недоступности для скачивания мобильных приложений в официальных магазинах применяется в отношении приложений Сбера, ВТБ, «ФК Открытие», Совкомбанка, Промсвязьбанка и Новикомбанка. Лучший способ защиты от таких угроз – отказ от скачивания файлов или приложений из незнакомых источников.

Удаление приложений ряда банков из официальных магазинов также используется и в другом виде. При входе в личный кабинет банка не через приложение, а через сайт в Интернете, выпавший первым в поисковой системе Google, пользователи могут попасть на фишинговый сайт. После ввода клиентом на фишинговом сайте логина и пароля личного кабинета в банке поступает сообщение о подключении к личному кабинету какого-то другого айфона. По сути, граждане предоставляют злоумышленникам доступ к личному кабинету. В итоге мошенники оплачивают свои покупки и услуги с помощью СБП из личного кабинета потерпевших или переводят деньги на счета различных дропперов[3].

Еще одним новым инфоповодом является приостановка работы платежных систем Visa и Mastercard и отключение некоторых банков от системы SWIFT. Гражданам предлагается срочно открыть карту «Мир» или перевести деньги с приостановивших работу платежных карт. Путем СМС или телефонных звонков от имени службы безопасности банка сообщается, что имеется угроза потерять деньги или что карта в ближайшее время заблокируется. Предлагается «обезопасить» или «разблокировать» карту путем перевода средств на безопасный счет или открытия карты «Мир».

[3] Дропперы – в данном случае получатели незаконно списанных денег для дальнейшей передачи мошенникам. По сути – посредники между клиентом и мошенниками при получении последними украденных денег. В настоящее время Банк России готовит базу таких клиентов, на операции которых будут вводится ограничения по переводу денег на другие счета и на снятие наличных. В России сегодня число дропперов может достигать 500 тысяч человек.

Для чего опять-таки требуют сообщить данные карты, иные персональные данные. Если вы выполняете эти требования, итог один – потеря денег. В данном случае надо прервать разговор и связаться по официальному телефону с банком. Как правило, сообщения об опасностях – вымысел мошенников.

После повышения ключевой ставки до 20% мошенники стали предлагать от имени клиентского подразделения банка по телефону повышенный кэшбэк в 10% на год. Для это также требуют сообщить данные платежной карты, пользуясь тем, что клиенты при повышенной ставке ожидают повышения доходов и по другим основаниям, верят в возможность получения больших выгод от пользования платежными картами.

Надо иметь в виду, что повышенный кэшбэк действительно существует, но только на отдельные товары и по отдельным акциям, проводимым достаточно редко. Также стоит не забывать о том, что сотрудники банков никогда не звонят клиентам с просьбами сообщить какие-то персональные данные или переводить деньги на какие-то счета. При получении таких звонков надо также прервать разговор и занести номер звонивших в раздел запрещенного спама, сообщить об этом звонке в службу безопасности вашего банка.

Звонки становятся все более целенаправленными. Например, используя данные из поликлиник, звонят пациентам с информацией о возможном исчезновении из аптек нужного лекарства и предлагают его срочно купить по выгодной цене.

Используются и применявшиеся ранее схемы с прикрытием преступных действий под видом различных государственных органов. Например, проводятся массовые обзвоны и рассылки фишинговых писем от имени Федеральной службы судебных приставов о якобы наличии у граждан задолженности, которую надо погасить, иначе будут арестованы банковские счета и имущество. Предлагается погасить долг по указанной ссылке или перейти по ссылке, чтобы подробнее узнать о долге.

При выполнении предлагаемых действий технические средства жертвы заражаются файлом с вирусом, и преступники получают доступ к персональным данным людей, реквизитам их банковских карт. Итог – потеря денег. Причем некоторые граждане даже сами отправляют деньги по указанным мошенниками адресам для того, чтобы погасить «долги». Лучший способ защиты в этом случае – не отвечать на подобные письма и удалять их. А задолженность можно проверить в «Личном кабинете» налогоплательщика на официальном сайте ФНС или на портале «Госуслуги».

Переболевшим COVID-19 рассылаются электронные письма с предложениями направить заявку на получение пособия. Для этого

используется сайт «Портал здравоохранения граждан СНГ» с обсуждениями якобы получивших такие пособия граждан. В заявке надо указать имя, адрес проживания, доход за последний месяц и электронную почту. После получения данных адресат получает на липовом официальном бланке «Постановление о выплате» с указанием значительных сумм, которые можно получить через «единый реестр». Для этого предлагается пройти платную регистрацию и ввести данные банковской карты для получения денег. Могут пропасть все деньги и даже больше, если карта кредитная с овердрафтом. Надо знать, что все пособия получаются только с использованием сайта «Госуслуги» или через МФЦ. Остальные предложения ничтожны и опасны.

Очень опасны фишинговые сайты, нацеленные на предпринимателей и предлагающие различные производственные, логистические или снабженческие услуги. Предприниматели, обратившиеся к таким сайтам, не только теряют деньги, но и возникает опасность остановки производства.

Заметно активизировались фишинговые сайты, имитирующих услуги в интернет-магазинах в условиях ажиотажного спроса в связи с введенным эмбарго на поставки продукции из недружественных стран. Конек этих рассылок – не предложение купить что-либо по заниженным ценам, а предложение купить по старым ценам или купить иностранную технику за рубежом, так как многие маркетплейсы прекратили продажи россиянам. Также активно использовались сообщения об обмене валют по льготному курсу или с предложениями по установке VPN-сервисов, приобретении международных платежных карт, позволяющих оплатить покупки в иностранных государствах. Появились даже экзотические сайты, предлагающие купить офисную бумагу по льготным ценам.

В условиях потери гражданами работы вследствие различных последствий введенных против России санкций, потерявшим работу предлагается выгодная работа на дому после заполнения ряда анкет, направления копий личных документов и использования их личного мобильного приложения банка. Как правило, ссылка на бланк анкеты и дополнительную информацию ведет на фишинговый сайт. Результат – потеря денег.

В других случаях предлагается за определенное вознаграждение для принятия на работу написать тестовую статью, подготовить тестовый логотип или тестовую модель чего-либо, разработать удаленный урок и т. п. В результате поверившие таким предложениям дизайнеры, педагоги, журналисты, менеджеры по продажам, маркетологи и другие специалисты создают бесплатную продукцию для мошенников, так как последние не исполняют обещания ее опла-

тить, а авторы обнаруживают то, что мошенники воспользовались результатами их труда.

В итоге в настоящее время произошло изменение пропорций между фишинговыми атаками и мошенническими звонками в пользу первых. Это объясняется не только сокращением числа мошеннических call-центров на Украине, но и активным использованием антифрод-решений как банками, так и операторами связи. Так, например, только Сбербанк по итогам 2021 г. предотвратил мошенничество с банковскими картами на сумму 112 млрд рублей. Причем в режиме онлайн предотвращается 99% мошеннических операций. «Результативность» фишинговых атак становится выше, чем при телефонном обзвоне, и операции мошенников постепенно перемещаются в сторону этого метода реализации угрозы безопасности персональных данных. Среднемесячная прибыль серьезного фишера сегодня превышает миллион долларов США.

В-третьих, произошло резкое увеличение количества атак с применением угроз информационной безопасности. В первую очередь увеличилось число атак на банковские информационные системы. Так, например, в марте 2022 г. количество отраженных кибератак на банк ВТБ по отношению к марту 2021 г. выросло вдвое. После начала спецоперации России на Украине Сбербанк остановил масштабную атаку украинских разработчиков, имеющих около 50 различных официальных банковских приложений, которые нарушали требования международных платежных систем и собирали данные банковских карт клиентов, пользующихся приложениями. Было остановлено массовое списание средств с карт клиентов при десятке тысяч попыток списаний за минуту. Всего было отклонено несколько сотен тысяч списаний.

Расширена сфера применения методов кибертерроризма и кибератакивизма, к которым прибегают правительства отдельных стран для решения своих экономических и политических целей. Развивая кибератакивизм, его организаторы используют онлайн-версии различных протестов и фейковых сообщений, нарушая работу сайтов государственных органов и различных компаний. О масштабах такой работы говорит тот факт, что к информационным атакам на нашу страну сегодня привлечено более 5 тысяч ИТ-специалистов из разных стран с ежедневной оплатой в 1,4 млн долларов США. Для проведения DDoS-атак на финансовые структуры хакеры используют ботнет-сеты, способные обеспечить лавинообразный рост запросов к онлайн-ресурсу и тем самым вывести его из строя. Размер ботнет-сетей, нацеленных на нашу страну, достигает сотен тысяч устройств. В марте наблюдался четырехкратный рост атак на банковские системы по сравнению с февралем. За период с 24 фев-

раля по 12 апреля количество DDoS-атак на российские финансовые организации выросло в 22 раза по сравнению с началом года.

Резко возросло количество кибератак, направленных на взлом учетных данных или использующих метод «грубой силы» брутфорсинг (метод перебора всех паролей) при помощи ботов. Ботнет-сеты способны обеспечить лавинообразный рост запросов к онлайн-ресурсу и тем самым вывести его из строя. Размер ботнет-сетей, нацеленных на нашу страну, достигает сотен тысяч устройств.

В-четвертых, появляются новые методы реализации угроз. Наиболее активно они генерируются в сфере обращения криптовалют. Стали массовыми ранее являвшиеся экзотическими троянские программы, используемые для кражи с мобильных устройств криптовалют. Появилась массовая рассылка вредоносных приложений или вредоносных обновлений ранее используемых приложений с предложениями уйти от введенных ограничений для пользователей и скачать эти приложения или обновления. Причем троянские версии криптокошельков продвигаются через сайты, которые по внешнему виду и функциональности похожи на оригинальные ресурсы и имеют похожие адреса.

Вредоносные коды уже зафиксированы в ряде известных приложений – imToken, Bitrie и др. Если пользователь устанавливает версию кошелька с использованием платформы Android, то троян загружается сразу при посещении вредоносного ресурса, без перенаправления на другой сайт. После загрузки троянов вредоносная активность незаметна для пользователя. Происходит кража уникальной для каждого криптокошелька мнемонической seed-фразы – аналога мастер-пароля. С помощью полученных данных мошенники крадут криптовалюту из кошелька жертвы. Поэтому загружать программы-криптокошельки можно только из официальных каталогов приложений.

Вводятся в обращение новые мошеннические токены Ukraine и Peace. Иногда эти новые токены предлагаются держателям криптовалют на их кошельки после предварительного уведомления. Иногда криптоинвесторы сами покупают их на децентрализованных торговых площадках. Однако в последующем продать их оказывается невозможно, отображается ошибка. Это означает, что деньги злоумышленникам ушли, а вернуть их нельзя. Как выясняется, функция продажи у этих токенов или отключена, или разрешена только для эмитента и его подельников. Причем при попытках все-таки продать токены злоумышленники могут получить доступ к криптокошельку и украсть с него всю криптовалюту.

С новым видом мошенничества столкнулись и пользователи ныне достаточно популярного криптокошелька MetaMask. К ним

на электронную почту стали поступать письма от имени разработчиков этого криптокошелька с предложением верифицироваться. В противном случае аккаунт заблокируется. Если пользователь кошелька исполнит это требование, то его кошелек будет скомпрометирован и злоумышленники завладеют учетной записью пользователя. В данном случае надо помнить, что в ходе регистрации криптокошелька MetaMask адрес электронной почты не используется и он у его разработчиков отсутствует.

Появились новые схемы обмана частных инвесторов. Например, частным инвесторам обещается высокая прибыль за счет арбитражной торговли (торговли, основанной на разнице цен на разных торговых площадках) на Московской и Лондонской биржах. Для этого предлагается использовать самые разные активы – от иностранной валюты, нефти и драгметаллов до криптовалют. В качестве условий участия в операциях называются оплата аванса в размере 20% дохода, комиссии брокеру и за конвертацию, а также оплата соответствующих налогов. Прибыль обещают вывести через криптобиржу, так как на Лондонской бирже действуют санкции. В результате те, кто принимают условия мошенников, теряют значительные суммы денег.

Рекордными темпами растут блокчейн-взломы и сопутствующие им хищения криптоактивов, которые в той или иной мере затрагивают и россиян, оперирующих криптовалютами. Только за первый квартал 2022 г. хакеры украли криптоактивы на сумму в 1,3 млрд долл., совершив 78 взломов блокчейн-проектов. Потери имелись в таких экосистемах, как Ethereum, Solana, Binance Smart Chain и др. 20 взломов произошло в новейшем направлении – NFT-индустрии. Криптобиржи были ограблены на 42 млн долл. за три взлома.

В-пятых, отмечаются элементы деградации платежной инфраструктуры. Это проявляется в отключении от системы SWIFT ряда банков страны, в отключении или приостановке работы платежных сервисов ApplePayGoogle и Pay, мобильных приложений AppStore, PlayMarket и AppGallery, платежных систем Visa и Mastercard. Примеры действий киберпреступников по данному направлению были рассмотрены выше.

Заключение

Стоит отметить, что принятые ранее и принимаемые в настоящее время меры по защите от подобных действий уже дают определенные результаты. Так, например, запущенный в 2014 г. россий-

ский аналог SWIFT – систему передачи финансовых сообщений СПФС – используют уже 400 пользователей как в России, так и за ее пределами, в том числе 52 иностранные организации в 12 странах мира. Банковскими картами национальной системы платежных карт «Мир» можно воспользоваться сегодня в десяти странах.

Таким образом, анализ происходящих событий в сфере информационных технологий позволяет сделать вывод о том, что неправомерные действия в этой сфере наносят ущерб экономической безопасности как страны в целом, так и отдельных ее граждан. Растет результативность мошеннических действий. По оценке управляющего RTM Group Евгения Царева, в 2022 г. ожидается рост количества результативных атак мошенников не менее, чем на 30–40%, а совокупный ущерб может превысить 165 млрд руб.

Для борьбы с мошенническими действиями, кроме технических мер по внедрению антифрод-решений, Банк России разрешил банкам временно приостанавливать дистанционный доступ к управлению счетом при выявлении нетипичных операций по картам и счетам физических лиц. При этом клиенты уведомляются о приостановлении операций с указанием причины приостановки. Возобновление операций возможно только после личного обращения клиента в банк. Что касается защиты от действий мошенников на рынке криптовалют и фондовом рынке, то все здесь зависит от самого гражданина, участвующего в сделках.

Банк России ограничил операции неквалифицированных инвесторов, но зачастую обманутыми оказываются и опытные игроки, так как иногда простая человеческая жадность ведет к потере бдительности и, как результат, финансовых средств. Кроме того, повышаются требования к технической оснащенности финансовых структур в части обеспечения информационной безопасности. Надо иметь в виду, что мошенники обманывают не только тех, кто имеет слабую экономическую подготовку, но и опытных специалистов. Известно несколько случаев обмана людей, совершенно точно имевших профессиональные знания в области информационной безопасности.

Литература

Бурлаков, Кемпа 2022 – *Бурлаков В.В., Кемпа В.С.* Особенности российского рынка инноваций и его дальнейшее развитие на основе концепции инжиниринга // Наука и искусство управления / Вестн. Ин-та экономики, управления и права Росс. гос. гуманит. ун-та. 2022. № 1. С. 49–62. DOI: 10.28995/2782-2222-2022-1-49-62

Кисова, Холчева 2019 – *Кисова А.Е., Холчева И.А.* Основные подходы к исследованию понятий «экономическая безопасность» и «экономическая безопасность государства» // Дневник науки. 2019. № 5 (29). С. 96.

Наркевич 2022 – *Наркевич Л.В.* Информационно-аналитическая платформа управления обновлением основных средств в условиях цифровой трансформации // Вестн. РГГУ. Сер. «Экономика. Управление. Право». 2022. № 1. С. 22–44. DOI: 10.28995/2073-6304-2022-1-22-44.

Павлова 2021 – *Павлова И.Г.* Методологические аспекты изучения инновационной инфраструктуры // Вестн. РГГУ. Сер. «Экономика. Управление. Право». 2021. № 4. С. 101–110. DOI: 10.28995/2073-6304- 2021-4-101-110.

Пряжникова 2017 – *Пряжникова О.Н.* Экономическая безопасность в контексте личной безопасности // Экономические и социальные проблемы России. 2017. № 1. С. 84–97.

Спильниченко, Соколов, 2021 – *Спильниченко В.К., Соколов А.П.* Источники финансовых угроз информационной безопасности личности // Журн. приклад. исслед. 2021. № 6-6. С. 496–502.

Чистякова, Артемов 2021 – *Чистякова К.А., Артемов О.Ю.* Пути развития корпоративного бизнеса на основе высокотехнологичных проектов в условиях инновационной экономики // Вестн. РГГУ. Сер. «Экономика. Управление. Право». 2021. № 4. С. 22–34. DOI: 10.28995/2073-6304-2021-4-22-34.

References

Burlakov, V.V. and Kempa, V.S. (2022), "Features of the Russian innovation market and its further development based on the engineering concept", *Science and Art of Management / Bulletin of the Institute of Economics, Management and Law of the Russian State University for the Humanities,* no. 1, pp. 49–62, DOI: 10.28995/2782-2222-2022-1-49-62.

Chistyakova, K.A. and Artemov, O.Yu. (2021), "Ways of corporate business development based on high-tech projects in an innovative economy", *RSUH/RGGU Bulletin. "Economics. Management. Law" Series,* no. 4, pp. 22–34, DOI: 10.28995/2073-6304-2021-4-22-34.

Kisova, A.E. and Kholcheva, I.A. (2019), "Main approaches to the study of the concepts 'economic security' and 'economic safety of the state' ", *Dnevnik nauki*, no. 5 (29), 96 p.

Narkevich, L.V. (2022), "Information and analytical platform for managing the renewal of fixed assets in the conditions of digital transformation", *RSUH/RGGU Bulletin. "Economics. Management. Law" Series*, no. 1, pp. 22–44, DOI: 10.28995/2073-6304-2022-1-22-44

Pavlova, I.G. (2021), "Methodological aspects of studying the innovation infrastructure", *RSUH/RGGU Bulletin "Economics. Management. Law" Series*, no. 4, pp. 101–110, DOI: 10.28995/2073-6304-2021-4-101-110

Pryazhnikova, O.N. (2017), "Economic security in the context of personal security", *Economic and social problems of Russia*, no. 1, pp. 84–97.
Spilnichenko, V.K. and Sokolov, A.P. (2021), "Sources of financial threats to personal information security", *Journal of Applied Research*, no. 6-6, pp. 496–502.

Информация об авторе

Владимир К. Спильниченко, доктор экономических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; Spilnvladimir@yandex.ru

Information about the author

Vladimir K. Spilnichenko, Dr. of Sci. (Economics), professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Square, Moscow, Russia, 125047; Spilnvladimir@yandex.ru