Меры информационной безопасности ЦБ России

А. Р. Гарданова*, З. Ф. Мухамадеева, Л. Н. Пономарева

Башкирский государственный университет, Институт экономики финансов и бизнеса
Россия, Республика Башкортостан, 450076 г. Уфа, улица Карла Маркса, 3/4.

**Email: alinagardanova@mail.ru*

В статье рассматривается уровень вреда экономике от кибер-атак и мошенничеств в финансовой сфере, проводится анализ мер, предпринимаемых Банком России по регулированию и обеспечению информационной безопасности финансовых операций.

Ключевые слова: кибер-атаки, хакерские атаки, Big Data, транзакция.

Согласно Указу Президента РФ от 13 мая 2017 г. №208В в «Стратегии экономической безопасности Российской Федерации на период до 2030 года» отмечаются определенные цели и задачи государственной политики в сфере обеспечения экономической безопасности страны. В связи с этим Банк России, принимая во внимание вышеупомянутый документ, предпринял ряд мер по повышению уровня информационной безопасности проведения финансовых операций. Данные инициативы ЦБ РФ изложены в Указе Банка России от 7 мая 2018 г. №4793-У «О внесении изменений в положение Банка России от 9 июня 2012 года №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

В соответствии с вышеназванным Указом ЦБ РФ в обеспечении безопасности проведения финансовых транзакций были приняты следующие действия: во первых, с 1 июля 2018 года банки и операторы по переводу денежных средств будут обязаны информировать ЦБ РФ о хакерских атаках. В Указе обозначены требования к обеспечению защиты информации при осуществлении переводов денежных средств. Также, операторы денежных средств и операторы услуг платежной инфраструктуры должны использовать только сертифицированное программное обеспечение и проводить его ежегодное тестирование на проникновение информационной безопасности. Банк России обязывает финансовые организации проходить аудит сторонних компаний для проведения оценки уровня защищенности транзакций.

Регулятор также расширяет перечень требований и к самим Операторам по переводу денежных средств. Например, в число параметров, указываемых Оператором при проведении операций, в обязательном порядке необходимо будет вносить следующие данные:

- максимальное значение суммы денежного перевода;
- список получателей;
- время осуществления транзакции;
- местоположение устройства, использованного для проведения операции.

Оператор также будет отвечать за защиту данных с помощью технологических мер, обеспечивающих:

- идентификацию клиента;
- аутентификацию сообщений;
- возможность контролирования реквизитов.

Данные меры призваны усилить контроль над операциями при осуществлении денежных переводов.

Второе действие, которое было установлено в целях обеспечения безопасности проведения финансовых транзакций, это тот факт, что ЦБ РФ обязал банки раскрывать финансовый ущерб от кибератак. Согласно статистике, в 2017 году российский банковский сектор столкнулся с волной кибератак. За год число подобных атак на финансовый сектор выросло почти в полтора раза. По словам Литвинова Д. А. общий объем хищений в России в результате хакерских атак составляет 1.5–2.0 млрд. рублей. Это официальные данные ЦБ РФ.

Как известно, основными объектами кибератак становятся системы межбанковских переводов, процессинговые системы, платежные шлюзы, дистанционный банкинг и инфраструктура управления банкоматами, доступ к которым может принести злоумышленникам значительно больший доход, чем даже массовый обман клиентов банка. В своей работе «Тенденции развития угроз информационной безопасности» Комиссаров Е. А. отмечает, что кибератака на цифровое устройство становится кибератакой и на систему, что может привести к потерям несравнимо большим, чем взлом отдельно взятого устройства.

С 1 июля 2018 года Банк России изменил форму отчетности о событиях, связанных с нарушением защиты информации. Теперь в отчетности будут указываться экономические последствия для операторов и их клиентов. Это позволит повысить достоверность данных о событиях, связанных с нарушением защиты информации, так как, предоставляемая информация позволит более точно оценивать качество систем управления рисками и систем управления капиталом кредитных организаций.

В третьих, Центральным Банком был предложен стандарт по информационной безопасности. С 1 июля 2018 года Банк России ввел стандарт оказания услуг в сфере информационной безопасности для финансовых организаций – банков, некредитных

финансовых организаций, субъектов национальной платежной системы и др. Использование такого стандарта поможет поддерживать систему обеспечения информационной безопасности малым и средним организациям, которым, как правило, зачастую не хватает финансовых ресурсов.

Четвертым фактом в обеспечении безопасности проведения финансовых транзакций является то, что ЦБ разработал «киберГОСТ» для банков. Банк России разработал проект стандарта с категоризацией кибер-инцидентов, о которых банки и некредитные финансовые компании в обязательном порядке должны будут информировать ЦБ, и на его основе создается ГОСТ. Информирование будет осуществляться через запущенную 1 июля новую систему по предотвращению кибер-угроз в финансовой сфере. В список входят несанкционированные переводы денежных средств, финансовые и банковские операции, а также инциденты, связанные с нарушением бесперебойности оказания финансовых услуг. Банкам в обязательном порядке необходимо сообщать в ЦБ обо всех событиях, связанных с хищением средств клиентов, в частности, о взломах личных смартфонов граждан или компьютерных систем компаний.

Несомненно, что к контролю и совершенствованию процесса защиты данных финансовых операций необходимо подходить комплексно. Поэтому данный документ описывает требования к организации всех основных процессов защиты информации, в том числе по защите от атак с использованием вредоносного программного обеспечения. Таким образом, будут сертифицироваться и системные разработки, и программные обеспечения (ПО).

Итак, основное требование нового ГОСТа по безопасности финансовых (банковских) операций следующее: все технические меры защиты информации должны иметь сертификат соответствия стандартам Федеральной службы по техническому и экспортному контролю (ФСТЭК).

И в пятых, Банк России с помощью Big Data вправе вычислять «черных кредиторов». Возможности Big Data будут использованы для защиты россиян в интернете от «черных кредиторов». ЦБ РФ разрабатывает проект, позволяющий применить новую модель надзора, а именно различать сайты компаний, имеющих и не имеющих право выдавать займы потребителям, для принятия соответствующих мер по их устранению. Это будет распространяться на все сайты, принимающие оплату, включая благотворительные организации. Разумеется машина гораздо быстрее человека проанализирует огромный объем информацию в сети и спасет тысячи доверчивых граждан от будущих финансовых потерь.

Таким образом, исходя из всего вышесказанного, можно сделать вывод, что уязвимость банковской системы является угрозой безопасности не только финансового сектора, но и всего государства. Описанные выше инициативы и меры ЦБ РФ по регули-

рованию и обеспечению информационной безопасности финансовых операций значительно повысят эффективность борьбы с киберпреступностью в данной сфере, а также снизят уязвимость финансового сектора и его инфраструктуры, позволяющих преступникам выводить из страны сотни миллиардов рублей.

Литература

1. Литвинов Д. А. Киберпреступность в банковской сфере России: характер, масштабы, последствия // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж, 2017. №1. С. 38.
2. Комиссаров Е. А. Тенденции развития угроз информационной безопасности // Образование и наука без границ: социально-гуманитарные науки, 2016. №3. С. 209.
3. Новости информационной безопасности [Электронный ресурс]. – URL: https://www.anti-malware.ru/news.
4. Портал газеты «Известия» [Электронный ресурс]. – URL: https://iz.ru/634134/tcentr-kompetentcii-po-informbezopasnosti-sozdadut-pri-sberbanke.

Статья рекомендована к печати кафедрой финансов и налогообложения ИНЭФБ Башкирского Государственного университета (канд. соц. наук, доцент. З. Ф. Мухамадеева)

Measures of the central bank of Russia on information protection in the financial sector

A. R. Gardanova*, Z. F. Mukhamadeeva, L. N. Ponomareva

Bashkir State University, Institute of Economics, Finance and Business
3/4 Karl Marx Street, 450076 Ufa, Republic of Bashkortostan, Russia.

**Email: alinagardanova@mail.ru*

The article discusses the level of damage to the economy from cyberattacks and fraud in the financial sector, analyzes the measures taken by the Bank of Russia to regulate and ensure information security of financial transactions.

Keywords: cyber-attacks, hacker attacks, Big Data, transaction.