МЕРЫ ЦЕНТРАЛЬНОГО БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ФИНАНСОВОЙ СФЕРЕ

Василенко О.А. Email: Vasilenko1149@scientifictext.ru

Василенко Ольга Андриановна – кандидат экономических наук, доцент ВАК, научная специальность: финансы, денежное обращение и кредит, г. Москва

Аннотация: *кибер-атаки и мошенничество в финансовой сфере приносят огромный ущерб не только банковскому сектору, но и всей экономике России. В статье проводится анализ мер, предпринимаемых Банком России по регулированию и обеспечению информационной безопасности финансовых операций. Автор излагает свою авторскую позицию в отношении инициатив ЦБ РФ, которые должны повысить эффективность борьбы с киберпреступностью в данной сфере и снизить уязвимость финансового сектора и его инфраструктуры, позволяющих преступникам выводить из страны сотни миллиардов рублей.*

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

MEASURES OF THE CENTRAL BANK OF RUSSIA ON INFORMATION PROTECTION IN THE FINANCIAL SECTOR

Vasilenko O.A.

Vasilenko Olga Andrianovna - PhD in Economics, Associate Professor of VAK, SCIENTIFIC SPECIALTY: FINANCE, MONEY CIRCULATION AND CREDIT, MOSCOW

Abstract: *cyber-attacks and fraud in the financial sector bring huge damage not only to the banking sector of Russia, but also to the entire economy. The article analyzes the measures taken by the Bank of Russia to regulate and ensure information protection of financial transactions. The author states her author's position on the initiatives taken by the Central Bank of Russia, which should improve the effectiveness of the fight against cybercrime in this area and reduce the vulnerability of the financial sector and its infrastructure, allowing criminals to withdraw from the country hundreds of billions of rubles.*

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

УДК 336.717

В «Стратегии экономической безопасности Российской Федерации на период до 2030 года», утвержденной Указом Президента РФ от 13 мая 2017 г. № 208, намечены цели и задачи государственной политики в сфере обеспечения экономической безопасности страны. Банк России, принимая во внимание вышеупомянутый документ, принял ряд мер для повышения уровня информационной безопасности проведения финансовых операций. Эти 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».

Что меняется после выхода вышеназванного Указа ЦБ РФ в обеспечении безопасности проведения финансовых транзакций?

1. Банки и операторы по переводу денежных средств с 1 июля 2018 года будут обязаны информировать ЦБ РФ о хакерских атаках. В Указе скорректированы 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. Так, в число параметров, указываемых Оператором при проведении операций, будут входить следующие данные:

а) максимальное значение суммы денежного перевода;

б) список получателей;

в) время осуществления транзакции;

г) местоположение устройства, использованного для проведения операции.

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

а) идентификацию клиента;

б) аутентификацию сообщений;

в) возможность контролирования реквизитов.

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

2. ЦБ РФ обязал банки раскрывать финансовый ущерб от кибератак. В минувшем году российский банковский сектор столкнулся с волной кибератак; за год число подобных атак на финансовый сектор выросло почти в полтора раза. Литвинов Д.А. пишет: «Согласно официальным данным ЦБ РФ, общий объем хищений в России в результате хакерских атак составляет 1,5-2,0 млрд рублей» [1, с. 38].

Основными объектами кибератак становятся системы межбанковских переводов, процессинговые системы, платёжные шлюзы, дистанционный банкинг и инфраструктура управления банкоматами, доступ к которым может принести злоумышленникам значительно больший доход, чем даже массовый обман клиентов банка. «Кибератака на цифровое устройство становится кибератакой и на систему, что может привести к потерям несравнимо большим, чем взлом отдельно взятого устройства» [2, с. 45].

С 1 июля 2018 года Банк России изменил форму отчетности о событиях, связанных с нарушением защиты информации. 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.

3. ЦБ предложил 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. На мой взгляд, использование такого стандарта поможет поддерживать систему обеспечения информационной безопасности малым и средним организациям, которым обычно не хватает финансовых ресурсов.

4. 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 будет создан ГОСТ. Информирование будет осуществляться через запущенную 1 июля новую систему по предотвращению кибер-угроз в финансовой сфере. В список войдут несанкционированные переводы денежных средств, финансовые и банковские операции, а также инциденты, связанные с нарушением бесперебойности оказания финансовых услуг. Банки в обязательном порядке должны будут сообщать в ЦБ и о 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).

5. Банк России вычислит «черных кредиторов» с помощью Big Data. Возможности Big Data будут использованы для защиты россиян в интернете от «черных кредиторов». ЦБ РФ разрабатывает проект, который позволит применить новую модель надзора: 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. Машина гораздо быстрее человека проанализирует огромный объем информацию в сети и спасет тысячи доверчивых граждан от будущих финансовых потерь.

В заключении хочется подчеркнуть, что уязвимость банковской системы, является угрозой безопасности не только финансового сектора, но и всего государства. Описанные выше инициативы и меры ЦБ РФ по регулированию и обеспечению информационной безопасности финансовых операций повысят эффективность борьбы с киберпреступностью в данной сфере, снизят уязвимость финансового сектора и его инфраструктуры, позволяющих преступникам выводить из страны сотни миллиардов рублей.

Список литературы / *References*

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.