

Золотарюк Анатолий Васильевич

канд. техн. наук, доцент

Федотовская Валерия Алексеевна

студентка

Кретова Елизавета Александровна

студентка

ФГОБУ ВО «Финансовый университет

при Правительстве Российской Федерации»

г. Москва

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

Аннотация: в статье отмечается роль банков в реальной экономике, раскрываются проблемы банковской безопасности в современных условиях и актуальность их разрешения. Сравнивается надежность ПО в России и западных странах. Описывается предложение ЦБ РФ по созданию консорциума по реализации технологии блокчейн в банковском секторе. Раскрываются предложения по защите банковских информационных систем от случайных и преднамеренных угроз.

Ключевые слова: банки, информационная безопасность, банковское программное обеспечение, угрозы банковскому сектору, технология блокчейн, консорциум ЦБ РФ, автоматизированная система, обработка информации банка, доступ, банковские информационные системы, глобальная компьютеризация.

Банковский сектор является важным элементом цельной финансовой системы любой страны. Коммерческие банки призваны аккумулировать денежные средства, осуществлять кредитование различных отраслей экономики. С момента своего возникновения, банки неистово вызывали и вызывают интерес, который связан не только с хранением или получением денежных средств, но и с секретной информацией о финансовой деятельности различных субъектов экономики, имеющих соглашения с банками [7; 9].

В век современных технологий значение информационной безопасности банков в связи с глобальной компьютеризацией, распространением использования облачных ресурсов и развитием инструментов внедрения в информационные системы из внешней среды многократно возросло [1; 3; 5].

В нашей стране данная проблема является особенно актуальной, поскольку в отличие от западных банков, где программное обеспечение (ПО) разрабатывается конкретно под каждый банк и устройство автоматизированной системы обработки информации банка (АСОИБ) во многом является коммерческой тайной. В России получили распространение типовые, «стандартные» банковские пакеты, информация о которых известна большому кругу ИТ-сотрудников многочисленных банков, в т.ч. ушедшим из компании кадрам, что облегчает несанкционированный доступ в банковские информационные системы [2; 4].

Причем, во-первых, надежность «стандартного» ПО ниже из-за того, что разработчик нацелен на более широкие условия, в которых этому ПО придется функционировать, а во-вторых, некоторые российские банковские пакеты, прежде всего, их ранние версии, не в полной мере удовлетворяют требованиям безопасности и разграничения доступа к информационным ресурсам. Так, на экономическом форуме в Казани «Finopolis 2016» было объявлено об объеме покушений на хищение денежных средств со счетов российских банков за 9 месяцев 2016 года. Цифра составила 5 млрд рублей. Кражу 3 млрд все-таки удалось предотвратить, но 2 млрд рублей мошенникам удалось похитить. И хотя, по словам начальника главного управления безопасности и защиты информации ЦБ РФ Артема Сычева, «этот сумма совсем несущественна», так как составляет только «десятые доли от всего объема денежного оборота в России» [8], не обращать внимания на угрозы банковскому сектору нельзя. И многое уже делается.

В июле текущего года заместителем председателя Банка России Ольгой Скоробогатовой было объявлено, что в России будет создан так называемый консорциум при участии регулятора (ЦБ РФ) для изучения технологии блокчейна [6].

Идея технологии блокчейн состоит в реализации огромной базы данных общего пользования, которая функционирует без централизованного руководства. Интерес к этой идее в форме консорциума проявили группа QIWI, Accenture, БИНБАНК, МДМ Банк, Банк «Открытие», Тинькофф Банк и совсем недавно – Сбербанк России. Участники консорциума ЦБ РФ будут выявлять проблемы функционирования предлагаемой инновационной системы, предполагающей защиту от отступлений в финансовом законодательстве.

В чем же состоит идея данной технологии? Все привыкли, что операции с деньгами и документами обязательно проходят через посредников. Государственные органы, банки или юристы призваны проверять подлинность каждой из проделанных операций. Но суть блокчейна состоит в том, чтобы каждый из участников системы был ее же регулятором. Таким образом, не подразумевается иметь центральный орган управления.

Но так ли идеальна эта идея в будущем? Конечно, способ снижения затрат бизнеса на услуги посредников достаточно притягателен. Однако в то же время нельзя не упомянуть об угрозах кибератак. Преступность вероятнее всего будет заинтересована в едином центре информации. Следовательно, создаваемому консорциуму, как представляется авторам, необходимо изучить и исследовать на практике все сбои и вероятные проблемы при эксплуатации такого рода технологии в реальной жизни. То есть перед правительством и заинтересовавшимися в блокчейне институтами стоит огромная задача выявления рисков новомодной инновации для безопасности банковского сектора.

К данным условиям неопределенности можно отнести технологические риски, возникновение которых возможно на начальных этапах внедрения. Сбои в настройке системы и ее работе, – действия по устранению данных неполадок необходимо заранее предусмотреть, так как неточная проработка первых шагов внедрения на рынок блокчейна может привести к губительной системе в целом.

Следует добиться исключения или, по крайней мере, существенного снижения воздействия на банковские информационные системы, функционирующих в

современных технологических реалиях, случайных и преднамеренных угроз, как внешних, так и внутренних.

Список литературы

1. Аникеева К.А. Перспективы облачных технологий в банковском деле / К.А. Аникеева, А.В. Золотарюк, А.С. Макова // Валютное регулирование и валютный контроль. – 2014. – №9. – С. 52–56.
2. Банковские информационные системы и технологии. Часть 1. Технология банковского учета / Я.Л. Гобарева, Е.Р. Кочанова, Д.В., Нестерова Т.Н. [и др.]; под ред. Д.В. Чистова. – М.: Финансы и статистика, 2005.
3. Гайдар Е.В. ВІ-технологии предотвращают мошенничество в банковской сфере / Е.В. Гайдар, А.В. Золотарюк, Е.С. Худеньких // Валютное регулирование и валютный контроль. – 2015. – №5. – С. 63–66.
4. Гобарева Я.Л. Автоматизация деятельности кредитной организации на платформе «1С: Предприятие 8» / Я.Л. Гобарева, А.В. Золотарюк, Е.Р. Кочанова [и др.]; под общ. ред. проф. Д.В. Чистова. – М.: 1С- Паблишинг, 2012.
5. Золотарюк А.В. Информационные технологии банковского бизнеса // Валютное регулирование и валютный контроль. – 2014. – №8. – С. 56–57.
6. Информационный портал Banki.ru [Электронный ресурс]. – Режим доступа: <http://www.banki.ru/news/bankpress/?id=9071339> (дата обращения: 23.10.2016).
7. Мельников В.П. Информационная безопасность и защита информации: Учебник / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Академия, 2012.
8. РБК Новости [Электронный ресурс]. – Режим доступа: <http://rt.rbc.ru/tatarstan/freenews/57ff9bba9a794717d71af1a2> (дата обращения: 16.10.2016).
9. Чистов Д.В. Проектирование информационных систем: Учебник и практикум / Д.В. Чистов, П.П. Мельников, А.В. Золотарюк, Н.Б. Ничепорук; под ред. проф. Д.В. Чистова. – М.: Юрайт, 2015.