Доклад
первого заместителя Председателя Банка России Г.И. Лунтовского на Восьмом уральском форуме «Информационная безопасность финансовой сферы» (16-20 февраля 2016 года, Республика Башкортостан)

«Актуальные вопросы обеспечения информационной безопасности и приоритетные меры по противодействию правонарушениям в кредитно-финансовой сфере»

В настоящее время вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы являются приоритетным направлением регулятивной и надзорной деятельности центральных банков и финансовых регуляторов во всем мире. Указанное внимание финансовых регуляторов вызвано, прежде всего, стремительным внедрением поднадзорными организациями современных ИТ-технологий, что так же привлекает интерес и внимание криминалитета. При этом, с применением ИТ-технологии сегодня осуществляется значительная доля операций, имеющих финансовые последствия, в первую очередь платежных транзакций.

В данном вопросе Российская Федерация не является исключением. Поэтому Банк России уделяет повышенное внимание к вопросам обеспечения информационной безопасности и противодействия киберугрозам.

В 2015 году в структуре Банка России создан Центр мониторинга и предупреждения компьютерных атак, осуществляемых в кредитно-финансовой сфере (FinCERT). Основная цель создания Центра - координации работ по противодействию криминальным элементам, активность которых направлена на личное обогащение с использованием методов несанкционированного доступа к ИТ-инфраструктуре организаций кредитно-финансовой сферы. Также организовано взаимодействие FinCERT с МВД России, ФСБ России и Государственной системой обнаружения,

предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Проведенный FinCERT Банка России совместно с МВД России анализ правонарушений, выявленных в кредитно-финансовой сфере, показал, что в настоящее время основными типами правонарушений являются:

атаки на информационные ресурсы кредитных организаций с целью вывода их финансовых активов;

атаки на ИТ-инфраструктуру некредитных финансовых организаций – участников торгов путем использования неплатежных торговых инструментов (в том числе, торговых терминалов, процессинговых сервисов).

В IV квартале 2015 года результатом выявленных правонарушений по указанным направлениям явилось хищение денежных средств со счетов клиентов кредитно-финансовых организаций в сумме превышающей 1,5 млрд. рублей. Вместе с тем, уже в текущем году, благодаря совместным усилиям Банка России, МВД и банковского сообщества в рамках взаимодействия, организованного FinCERT удалось предотвратить хищений на сумму более 500 млн. рублей.

Основными целями злоумышленников являлись как непосредственное хищение денежных средств, так и сокрытие следов ранее совершённых незаконных финансовых операций. Несмотря на то, что указанные действия носят технический характер и связаны с используемыми ИТ-технологиями, они приводят к появлению значимых финансовых рисков кредитно-финансовых организаций, в том числе к нарушению обязательных нормативов к капиталу.

Статистика Банка России показывает, что невнимательное отношение менеджмента кредитных организаций к вопросам обеспечения ИБ, как правило приводит к значимым финансовым потерям, и свидетельствует о незрелости подходов к управлению рисками. Таким образом, невнимание к вопросам обеспечения информационной безопасности является

дополнительным фактором негативного влияния на устойчивость кредитных организаций. Так, за последний квартал 2015 года лицензии лишились три кредитных организации, ранее подвергшихся атакам.

Банком России рассматриваются следующие основные причины появления рисков атак на организации кредитно-финансовой сферы:

наличие множественных уязвимостей программного и аппаратного обеспечения автоматизированных систем и приложений, отсутствие должной реализации процедур контроля соответствия автоматизированных систем и приложений требованиям информационной безопасности;

низкая эффективности мероприятий, проводимых организациями кредитно-финансовой сферы по внедрению и использованию документов Банка России в области стандартизации обеспечения информационной безопасности;

отсутствие правовой основы по распространению нормативных требований к обеспечению защиты информации, устанавливаемых Банком России, на все процессы деятельности кредитных организаций;

отсутствие должной достоверности контроля выполнения технических требований, как правило реализуемого в форме самооценки.

В составе ключевых направлений деятельности по снижению перечисленных рисков Банком России выделяются следующие:

проработка вопроса о законодательном закрепление права Банка России, совместно с ФСТЭК России и ФСБ России, по нормативному регулированию и контролю всех вопросов, связанных с обеспечением информационной безопасности в организациях кредитно-финансовой сферы, в том числе вопросов защиты информации, отнесенной к категории банковской тайны;

законодательное закрепление основ деятельности по реализации системы противодействия хищениям денежных средств (системы антифрод) и создание такой системы на базе FinCERT Банка России;

обеспечение скорейшей разработки и ввода в действие национальных стандартов, регулирующих технические вопросы обеспечения информационной безопасности в организациях кредитно-финансовой сферы;

реализация совместно с ФСБ России и ФСТЭК России системы подтверждения соответствия обеспечения информационной безопасности кредитно-финансовых организаций требованиям национальных стандартов;

пересмотр технологических требований, связанных с осуществлением переводов денежных средств, внедрение безопасных технологий, в том числе для участников платежной системы Банка России;

пересмотр технологии контроля со стороны Банка России за соблюдением участниками платежной системы Банка России требований к обеспечению информационной безопаснсоти;

реализация системы надзорных мер, учитывающей результаты контроля информационной безопасности в рамках системы подтверждения соответствия национальным стандартам.

Все указанные направления планируется к детальному обсуждению на Форуме. Считаю, что их всестороннее обсуждение будет традиционно способствовать определению оптимальных решений, которые в перспективе позволят преодолеть негативные явления, вызванные деятельностью киберпреступников.

Желаю участником форума плодотворной и успешной работы.