НЕКОММЕРЧЕСКОЕ ПАРТНЕРСТВО
НАЦИОНАЛЬНЫЙ СОВЕТ ФИНАНСОВОГО РЫНКА

101000, г. Москва , ул. Мясницкая, дом 42, стр. 3
телефон/факс : (499) 678 28 20

исх. НСФР-02/1-438
от 17.10.2016

Первому Заместителю
Председателя Центрального банка
Российской Федерации
Лунтовскому Г.И.

На исх. № 02-23-5/7393 от 15.09.2016

О предложениях по совершенствованию отчетности по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Уважаемый Георгий Иванович!

Национальный совет финансового рынка благодарит Банк России за предоставленную возможность принять участие в обсуждении мероприятий по совершенствованию отчетности в целях создания единой системы противодействия информационным угрозам в кредитно-финансовой сфере Российской Федерации.

I. Предложения Банка России, направленные на совершенствование отчетности по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Форма 0403203) поддерживаются участниками финансового рынка.

Вместе с тем, представляется возможным дополнительно доработать указанную форму отчетности с учетом следующих предложений участников финансового рынка.

1. Исключение вопросов технической реализации инцидентов защиты информации из формы 0403203 поддерживается участниками рынка, так как информационный обмен через Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (FinCERT) по техническим способам реализации инцидентов позволит более оперативно реагировать на выявленные инциденты, а также разрабатывать дополнительные алгоритмы защиты на основе анализа поступающей от банков информации.

Важным также представляется повышение интенсивности информационного обмена FinCERT с финансовыми организациями путем регулярного и максимально оперативного доведения до них результатов анализа как наиболее распространенных, так и новых моделей инцидентов.

2. Пункт 2 Предложений предлагает закрепить в обновленной отчетности по Форме 0403203 только данные по экономическим показателям.

Вместе с тем, Приложение 1 к Указанию Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств» устанавливает, что отчетность по Форме 0403203 содержит сведения об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

В то же время, с учетом закрепления в новой отчетности для FinCERT исключительно технических аспектов инцидентов, представляется важным сохранить в какой-либо из форм также юридические, организационные и географические показатели, отражаемые в настоящее время в Форме 0403202. Представляется, что сохранение только экономических показателей в обновленной форме отчетности по Форме 0403203 может снизить для Банка России эффективность анализа и обработки отчетности, а также может затруднить разработку нормативных актов и рекомендаций по защите информации.

3. Пункт 3 Предложений предусматривает повышение достоверности предоставляемой отчетности в том числе путем сбора перекрестной отчетности операторов по переводу денежных средств и операторов платежных систем, а также на основе анализа изменений по счетам бухгалтерского учета.

С учетом уже существующего единого формата отчетности (Форме 0403202), обеспечивающего сопоставимость информации, получаемой от различных субъектов подачи Формы 0403203, основной задачей здесь видится выработка специальных подходов для возможности осуществления перекрестного анализа получаемой информации, а также повышение глубины контроля за счет анализа изменений по счетам бухгалтерского учета, что потребует использования иных форм отчетности, представляемых финансовыми организациями в Банк России.

4. При формировании требований по предоставлению данных о суммах несанкционированных операций в форме 0403203 необходимо учитывать, что для несанкционированных операций, совершенных с использованием платежных карт, Банком России уже предусмотрена отчетность по форме 0409258.

В связи с этим предлагается исключить возможное дублирование данных отчетных форм 0403203 и 0409258.

При этом представляется целесообразным внести изменения в форму 0409258 путем добавления в нее информации о суммах денежных средств, возвращенных оператором по переводу денежных средств клиентам в рамках реализации обязанности, установленной в статье 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

5. В связи с тем, что у кредитных организаций, обслуживающих получателей денежных средств, несанкционированно списанных со счета плательщика, в большинстве случаев отсутствует достоверная информация о незаконности осуществленного перевода, включение в отчетность данных о таких инцидентах предлагается возложить исключительно на оператора по переводу денежных средств, обслуживающего плательщика.

6. В формах отчетности, затрагивающих экономические параметры совершаемых операций предлагается исключить использование термина «безопасность» в любых сочетаниях, поскольку его использование в целом ряде кредитных организаций приводит к необходимости по формальному признаку привлечения к подготовке указанных форм непрофильных специалистов, отвечающих за вопросы безопасности.

7. При составлении форм отчетности предлагается исходить из следующего перечня юридически значимых и фиксируемых событий в рамках выявляемых инцидентов:

1) выявление признака возможного совершения перевода денежных средств без согласия клиента;

2) отмена операции по переводу денежных средств клиентом;

3) получение от клиента информации об оспаривании совершенной операции;

4) возврат клиенту списанных без его согласия денежных средств;

5) отказ кредитной организации от возврата клиенту списанных денежных средств;

6) возврат денежных средств, списанных без согласия клиента, кредитной организацией, обслуживающей получателя;

7) получение возмещения от международной платежной системы в случае подтверждения факта списания денежных средств без согласия клиента.

При этом большинство кредитных организаций предлагает указывать в формах отчетности только две ключевые даты, порядок определения и фиксация которых могут быть четко унифицированы: дату выявления инцидента и дату принятия кредитной организацией решения по результатам рассмотрения инцидента.

Любые иные события в рамках инцидента (например, дата совершения хищения или дата его выявления) допускают множественность толкования и с трудом поддаются унификации, в связи с чем необходимость их указания неизбежно приведет к снижению уровня репрезентативности отчетности.

8. Предлагается отражать в формах отчетности как общий количественный и суммарный объем обращений клиентов за возмещением денежных средств, так и сумму реального возмещения, производимого кредитными организациями по различным основаниям.

9. В целях сбора только статистически значимых данных, а также снижения затрат кредитных организаций на анализ и учет незначительных инцидентов, предлагается установить минимальный суммовой размер инцидента, подлежащий отражению в отчетности.

10. В целях повышения информативности отчетности предлагается отразить в ней градацию инцидентов по субъекту, в отношении которого он произошел (юридическое лицо, физическое лицо или кредитная организация), а также установить суммовые диапазоны инцидентов для облегчения группировки данных.

Также предлагается повысить детализацию отчетности по каналам и/или инструментам, использованным при совершении хищений. Например: а) ДБО, б) мобильные телефоны, в) платежные карты и г) иное.

11. Кредитные организации отмечают, что оценка влияния той или иной категории инцидентов на бизнес кредитных организаций представляет объективную сложность в связи с множеством факторов, влияющих на успешность или неуспешность использования определенного метода хищения – своевременность выявления и типологизации, скорость доведения информации об этом методе до кредитных организаций и т.д.

В этой связи представляется наиболее целесообразным сконцентрировать усилия на совершенствовании процедур выявления признаков совершения операций без согласия клиента, а также информационно–методического обеспечения кредитных организаций со стороны FinCERT.

Наличие такой системы позволит как своевременно выявлять любые новые способы совершения хищений, так и максимально оперативно доводить необходимую информацию до всех кредитных организаций, тем самым предотвращая возможность последовательного использования идентичного метода хищения в различных кредитных организациях.

12. В связи с очевидной сложностью типизации инцидентов по видам методов их совершения (сложность установления конкретного метода хищения, возможное использование нескольких методов одновременно) предлагается внедрить практику, аналогичную применяемой в сфере ПОД/ФТ практике составления по сложным инцидентам SAR (suspicious activity report, сообщение о подозрительной активности), в рамках свободной формы которого кредитная организация может указать любые значимые факторы, характеризующие как отдельный инцидент, так и группу сходных инцидентов.

В рамках таких сводных сообщений у кредитных организаций будет возможность отразить (тогда, когда это возможно установить) в том числе метод свершения хищения (хищение карты, социальная инженерия, использование вирусной программы и т.п.).

Содержательный анализ такой информации представляется особо ценным для выработки рекомендаций со стороны FinCERT по типологиям многофакторных инцидентов в целях их системного предотвращения.

II. Наряду с предложениями по Форме 0403203 от кредитных организаций также поступил ряд предложений по совершенствованию работы FinCERT:

1. С учетом того, что большинство инцидентов происходят с использованием модулей идентификации абонента сотовой связи (sim-карт), крайне важно обеспечить оперативную агрегацию информации о задействованных при хищениях модулях (номерах мобильных телефонов) совместно кредитными организациями и операторами услуг подвижной радиотелефонной связи (далее – операторы связи).

Указанная информация может использоваться:

– кредитными организациями при анализе информации об используемых клиентами sim-картах;

– операторами связи в целях своевременной блокировки sim-карт, используемых в целях хищения денежных средств;

– правоохранительными органами в целях проведения оперативно-розыскных мероприятий в целях изобличения виновных в хищении лиц.

Одновременно представляется необходимым реализовать комплекс мер по созданию Единой информационной системы для автоматизированной проверки принадлежности модуля подвижной радиотелефонной связи конкретному лицу (далее – ЕИС) на основании данных, передаваемых кредитными и иными финансовыми организациями, определяемыми Правительством Российской Федерации.

В этой связи предлагается инициировать внесение в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» следующих изменений:

1) предусмотреть создание ЕИС, позволяющей на основании запросов заинтересованных организаций получать от операторов связи предусмотренную законом информацию (без создания единой информационной базы);

2) установить, что функционирование ЕИС обеспечивается организацией, определяемой федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере связи (далее – уполномоченная организация);

3) предусмотреть оперативное получение кредитными и иными организациями, заключившими договоры с уполномоченной организацией, на основании запросов следующей информации:

– о подтверждении соответствия абонентского номера сети подвижной радиотелефонной связи и фамилии, имени, отчества (при наличии) абонента, предоставленных физическим лицом – абонентом в кредитную (или иную) организацию;

– при условии указания в запросе сведений о фамилии, имени, отчестве (при наличии) абонента, номера документа, удостоверяющего личность абонента, и абонентского номера сети подвижной радиотелефонной связи, соответствующих сведениям об абоненте, имеющимся у оператора подвижной радиотелефонной связи, получение следующих сведений: а) о дате заключения действующего договора об оказании услуг подвижной радиотелефонной связи; б) о дате выдачи абоненту модуля идентификации абонента; в) о дате последней замены (выдачи дубликата) модуля идентификации абонента абоненту подвижной радиотелефонной связи.

4) установить обязанность операторов связи направлять указанную информацию посредством ЕИС без получения согласия абонента как не относящуюся к персональным данным абонентов,

5) предоставить право на основании запросов получать информацию из ЕИС кредитным и иным организациям, определяемым Правительством Российской Федерации, заключившим с уполномоченной организацией соответствующие договоры.

2. С учетом роста объемов информации, поступающей в FinCERT, а также повышения оперативности его работы, предлагается внедрить систему регулярных рассылок информации о выявленных инцидентах информационной безопасности по всем кредитным организациям – участникам информационного обмена с FinCERT с использованием защищенных каналов в целях предотвращения миграции мошеннических схем между кредитными организациями и повышения уровня превентивного реагирования на новые виды угроз.

3. Предлагается усовершенствовать формат экспорта данных из Клико в ЕСОД.

Национальный совет финансового рынка выражает готовность к активному дальнейшему взаимодействию с Банком России по вопросам совершенствования системы противодействия информационным угрозам в кредитно-финансовой сфере.

С уважением,

Председатель **А.В.Емелин**

Исп.: Бондаренко Д.Д., (499) 678-2820