ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

Департамент информационной безопасности

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (495) 771-91-00

Президенту Ассоциации банков России (Ассоциация «Россия»)

Г.И. Лунтовскому

119180, Москва, ул. Большая Якиманка, д. 23

от 08.02.2019 № 56-3-3/53

на № 02-05/53 от 24.01.2019

О направлении ответов на вопросы

Уважаемый Георгий Иванович!

Департамент информационной безопасности направляет ответы на вопросы, относящиеся к его компетенции, по итогам встречи руководителей Банка России с руководителями коммерческих банков, состоявшейся 1 февраля 2019 года в ОПК «БОР».

Приложение: на 7 л.

Директор Департамента информационной безопасности В.А. Уваров

Ассоциация банков России
Вх. № 02-04/213
«18» февраля 2019 г.

Т.О. Рубцова
(495) 771-99-99

Приложение

Темы и вопросы, находящиеся в компетенции Департамента информационной безопасности Банка России

1. Планируется ли на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (далее – ФинЦЕРТ) организовать площадку по онлайн-обмену информацией о мошеннических переводах физических лиц между банками? На текущий момент обмен через ФинЦЕРТ идет медленно, в результате чего существует параллельный обмен между банками напрямую.

С учетом текущей ситуации ожидать ли и в какие сроки требований в отношении кредитных организаций об обязательном переходе на отечественное программное обеспечение, в частности, об обязательном использовании отечественных систем защиты информации?

1а. С учетом того, что АСОИ ФинЦЕРТ работает в автоматическом режиме, сведения об операциях могут направляться и корректно маршрутизироваться вне зависимости от дня недели в режиме, приближенном к режиму реального времени. В настоящий момент с учетом объемов данных выгрузка обработанных сведений происходит раз в сутки. При наличии потребности со стороны рынка Банк России готов доработать систему и перевести выгрузку в удобный и эффективный для банков с точки зрения выявления мошеннических операций режим.

Внесение данных в базу получателей денежных средств по операциям без согласия клиента осуществляется Банком России после проверки полученных данных по критериям, установленными внутренними документами Банка России. Проверка выполнения критериев требует определенного времени и необходима для снижения вероятности ложноположительного признания операции по переводу денежных средств операцией без согласия клиента, в то время как данные, которыми обмениваются банки напрямую, не проверяются на соответствие установленным критериям.

Стоит отметить, что информация о получателях из базы данных Банка России обязательна к применению банками при осуществлении проверки операции по переводу денежных средств на предмет ее соответствия признакам операций без согласия. Соответствующие признаки установлены приказом Банка России от 27.09.2018 № ОД-2525.

Справочно: В случае если клиент подает в соответствии с формой, установленной договором, обращение о выявлении им операции без согласия, оператор по переводу денежных средств, получивший такое уведомление должен в срок, не превышающий одного рабочего дня с даты получения обращения, уведомить Банк России о факте операции. Для подобного уведомления в Банке России на базе автоматизированной системы обработки инцидентов ФинЦЕРТ (АСОИ ФинЦЕРТ) развернут прототип автоматизированной системы «Фид-

Антифрод». Функционал системы позволяет участникам (участники – поднадзорные Банку России организации, что обеспечивает доверие в рамках информационного обмена), в том числе операторам по переводу денежных средств, направлять уведомления с использованием как веб-интерфейса в ручном и полуавтоматическом режиме, так и интерфейса автоматической загрузки. В настоящее время соответствующий интерфейс проходит испытания и доступен для тестирования участниками. Формат передаваемых данных установлен стандартом Банка России СТО БР БФБО-1.5-2018, при этом описание интерфейса автоматической загрузки размещено на портале АСОИ ФинЦЕРТ.

При получении Банком России уведомления оператора по переводу денежных средств в автоматическом режиме происходит определение оператора по переводу денежных средств, обслуживающего получателя, после чего в адрес соответствующей организации в автоматизированной системе формируется уведомление о получении ее клиентом денежных средств в рамках операции без согласия. При получении такого уведомления оператор по переводу денежных средств, в случае если отправителем выступает юридическое лицо, в соответствии с требованиями законодательства должен приостановить зачисление денежных средств на расчетный счет получателя и запросить документы, подтверждающие обоснованность платежа. Если денежные средства уже зачислены, то банк получателя направляет в Банк России информацию о невозможности приостановления зачисления денежных средств. Вне зависимости от типа заявителя по каждому запросу Банка России по операции без согласия оператор по переводу денежных средств – получатель обязан (в соответствии с нормативным документом Банка России) направить с использованием АСОИ ФинЦЕРТ сведения о получателе (например, хэш паспорта).

1б. Принимая во внимание, что риски зависимости от иностранного программного обеспечения были и остаются актуальными для всех отраслей, Банк России планирует проводить мероприятия и прорабатывать вопросы использования преимущественно отечественного программного обеспечения финансовыми организациями, в том числе в рамках мероприятий программы «Цифровая экономика», совместно с уполномоченными органами государственной власти, устанавливающими требования к сертификации систем защиты информации и оценке соответствия программного обеспечения требованиям безопасности.

<u>Справочно:</u> Стандарт ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» устанавливает требования по применению финансовыми организациями сертифицированных по требованиям безопасности информации средств защиты информации, средств криптографической защиты информации, их классам, а также по применению прикладного ПО АС, сертифицированного на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации, или в отношении которого проведен

анализ уязвимостей по требованиям к оценочному уровню доверия не ниже ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013.

Указанные требования к сертификации устанавливаются уполномоченными органами государственной власти.

В рамках Программы «Цифровая экономика» предусмотрен целый ряд мероприятий по направлению использования преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями (например: развитие отечественных организаций, обеспечивающих потребности отраслей экономики в электронной компонентной базе и комплектующих, развитие Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий (мероприятия из подпункта 05.03).

2. В соответствии с новой редакцией Положения № 382-П[1] организации, осуществляющие переводы денежных средств, обязаны проводить оценку выполнения операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств с привлечением сторонних организаций, имеющих соответствующую лицензию.

Просим Банк России рассмотреть возможность проведения самооценки соответствия для банков с базовой лицензией, так как привлечение сторонних организаций не гарантирует достоверность и качество проведенной оценки и, кроме того, требует существенных материальных затрат (не менее 1500 тыс. руб.).

Практика контрольно-надзорной деятельности Банка России показала, что зачастую кредитные организации формально подходили к проведению самостоятельной оценки соответствия и отражали в отчетности недостоверные показатели о выполнении требований по информационной безопасности, в том числе существенно завышая их.

Так, например, ряд кредитных организаций, выставляя себе максимальные показатели, имели большое количество инцидентов информационной безопасности.

Ужесточение требований Банка России направлено, в первую очередь, на защиту финансовой устойчивости кредитных организаций.

Так, обеспечение бесперебойности функционирования национальной платежной системы, сохранности денежных средств клиентов должно являться одним из основных приоритетов в деятельности любой кредитной организации.

Проведение внешнего аудита на соответствие кредитной организации требованиям по информационной безопасности специализированной организацией позволяет достичь высокого уровня достоверности результатов такой оценки по следующим причинам:

---

[1] Положение Банка России от 09.06.2012 № 382-П «Положение 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».

- профессионализм сотрудников таких организаций ввиду их узкой специализации, а также необходимости соблюдения лицензионных требований;

- беспристрастность при проведении оценки;

- невозможность давления на лиц, проводящих оценку, со стороны руководства кредитных организаций.

Мероприятия, связанные с внешним аудитом, позволят обеспечить надлежащий уровень финансовой устойчивости кредитных организаций и, как следствие, защиту интересов потребителей финансовых услуг.

3. В целях реализации Департаментом информационной безопасности Банка России мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» по разработке профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере» какие изменения планируются в отношении квалификационных требований к образованию должностных лиц Службы информационной безопасности?

Основная цель разработки данного профессионального стандарта – определение трудовых функций и трудовых действий, которые выполняются специалистами по информационной безопасности в кредитно-финансовой сфере в процессе повседневной деятельности. Проектом профессионального стандарта предусмотрена необходимость наличия у данных специалистов высшего образования по программам бакалавриата, специалитета или магистратуры.

4. В целях повышения безопасности отечественного программного обеспечения, выпускаемого на рынок и предназначенного для осуществления финансовых (банковских) операций, считает ли Банк России целесообразным стандартизировать требования для производителей программного обеспечения к процедурам разработки автоматизированных систем и приложений, используемых для переводов денежных средств?

Действительно, Положением Банка России № 382-П закреплено требование по использованию для осуществления переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных ФСТЭК России на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013.

Также рекомендации Банка России по обеспечению информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем устанавливают отдельные положения по составу, содержанию и порядку проведения работ по контролю исходного кода программного обеспечения АБС,

оценке защищенности АБС и по контролю параметров настроек технических защитных мер.

Банком России планируется проведение ряда мероприятий для определения необходимых требований и рекомендаций к такому программному обеспечению (ПО). Вопрос формирования соответствующего профиля защиты для такого ПО прорабатывается совместно с компетентными организациями.

5. Пункт 2.5.8 Положения № 382-П определяет требование к распространению изменений в программном обеспечении, используемом для переводов денежных средств, направленных на устранение ставших известными оператору по переводу денежных средств уязвимостей указанного программного обеспечения. При этом, в случае если указанное программное обеспечение разрабатывалось сторонней организацией (производителем или поставщиком ПО), у оператора по переводу денежных средств отсутствуют возможности контроля сроков и порядка устранения уязвимостей. В связи с отсутствием норм, регулирующих порядок и сроки устранения уязвимостей в программном обеспечении производителями и/или поставщиками, считает ли Банк России целесообразным регламентировать порядок устранения угроз и уязвимостей поставщиками и производителями ПО?

Банк России не обладает полномочиями по регулированию деятельности поставщиков и производителей ПО, поэтому требования устанавливаются для кредитных организаций. Вопросы взаимодействия кредитных организаций с производителями ПО, в том числе определения порядка устранения угроз и уязвимостей ПО, находятся в рамках их договорных отношений.

6. В связи с введением ГОСТ Р 57580.1-2017 («Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер») обязана ли кредитная организация, ранее присоединившаяся к комплексу документов СТО БР ИББС (Стандарты Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»), отправлять в Банк России отчеты о проведенном аудите/самооценке по СТО БР ИББС, или достаточно будет проведения внешнего аудита по ГОСТ Р 57580.1-2017?

Обязанность кредитной организации проводить внешний аудит по ГОСТ Р 57580.1-2017 и оправлять в Банк России отчеты о его проведении будет установлена нормативным актом Банка России с 1 января 2021 года (проект находится на согласовании во ФСТЭК и ФСБ России). До этого срока кредитные организации, присоединившиеся к комплексу документов СТО БР ИББС, должны проводить аудит/самооценку по СТО БР ИББС 1.0 и отправлять в Банк России отчеты об их проведении.

7. Статья 27 Федерального закона № 161-ФЗ дополнена частью 5 «*В целях обеспечения защиты информации при осуществлении переводов денежных средств Банк России осуществляет формирование и ведение базы данных о случаях и*

попытках осуществления переводов денежных средств без согласия клиента.». В ходе использования указанной базы данных информация будет накапливаться о всех случаях и попытках осуществления переводов денежных средств без согласия клиента. Планируется ли процедура удаления сведений из указанной базы данных?

На основании частей 5 и 6 статьи 27 Федерального закона № 161-ФЗ в целях обеспечения защиты информации при осуществлении переводов денежных средств Банк России осуществляет формирование и ведение базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента (далее – база данных). Участники информационного обмена (операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры) обязаны направлять в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента по форме и в порядке, которые установлены Банком России. Таким образом, сведения о случаях и попытках осуществления переводов денежных средств без согласия клиента включаются в базу данных на основании информации, направленной участниками информационного обмена. Порядок ведения базы данных Банком России, в том числе включения, исключения, распространения информации, регулируется внутренним документами Банка России.

Соответствующие правила не являются догмой и подлежат изменению с учетом изменяющихся потребностей рынка. Мы на постоянной основе имеем обратную связь от банков в рамках экспертного совета и инициируем разработку соответствующих изменений.

8. В рамках раздела 4 «Работа с фидами» Прототипа АС «Фид-Антифрод»[2] возникают следующие вопросы. Планируется ли выгрузка фидов, содержащихся в базе данных о случаях и попытках осуществления перевода денежных средств без согласия клиента, чаще, чем на ежедневной основе? А также более подробное описание возможных данных, например, с указанием наименований всех платежных систем?

Работы по развитию АСОИ ФинЦЕРТ и АС «Фид-Антифрод», реализованной на ее программной платформе, предусматривают внесение изменений в функционал, в том числе и в механизм выгрузки фидов, содержащихся в базе данных о случаях и попытках осуществления перевода денежных средств без согласия клиента, чаще, чем на ежедневной основе. Информация о соответствующих изменениях будет отдельно доведена до участников информационного обмена с использованием портала АСОИ ФинЦЕРТ.

9. Вправе ли кредитная организация, являющаяся оператором по переводу денежных средств, у которой средний за полгода объем обязательств перед

[2] Прототип централизованной базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента (Прототип АС «Фид-Антифрод»). Руководство Участника по работе с прототипом АС «Фид-Антифрод» БКМД.62.01.12.553.И3.01.

клиентами по переводу денежных средств без открытия банковских счетов в течение месяца не превышает 2 млрд руб., отправлять (в соответствии с Указанием № 2831-У[3]) отчетность по форме 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств» с периодичностью один раз в полгода? Если да, то будет ли дорабатываться соответствующим образом программное обеспечение, с использованием которого подготавливается данная форма отчетности (KLIKO)?

Возможность представления отчетности по форме 0403203 раз в полгода в соответствии со статьей 62.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» имеют только небанковские кредитные организации, имеющие право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций, у которых средний за полгода объем обязательств перед клиентами по переводам денежных средств без открытия банковских счетов в течение месяца не превышает 2 миллиардов рублей.

[3] Указание 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».