**ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)**

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (499) 300-30-00

Личный кабинет

Президенту Ассоциации банков России

Г.И. Лунтовскому

ИНН 7702077663

От 02.09.2020 № 014-56-3/6478

на от

О направлении ответов на вопросы

Уважаемый Георгий Иванович!

В рамках подготовки ко II Съезду «Банки и экономика в условиях глобальной нестабильности», а также ввиду заинтересованности Ассоциации «Россия» в получении ответов на вопросы, представленные к встрече руководителей Банка России с руководителями коммерческих банков 13-14 февраля 2020 года в пансионате «Бор», Банк России направляет ответы на вопросы по тематике информационной безопасности.

Приложение: на 14 листах.

С уважением,

Заместитель Председателя
Банка России Д.Г. Скобелкин

Приложение.

Темы для обсуждения и вопросы для направления
в Департамент информационной безопасности Банка России

1. В соответствии с абзацем 3 подпункта 2.7.5 пункта 2.7 Положения от 09.06.2012 № 382-П[1] в состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации от воздействия вредоносного кода, включаются следующие требования:

«*В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы; оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы*».

В соответствии с вышеуказанным пунктом правильно ли понимать, что область действия его подпунктов распространяется только на сегмент платежной системы, размещенный на стороне оператора по переводу денежных средств, и задействованный в осуществлении переводов денежных средств? Оператор по переводу денежных средств обязан информировать только того оператора платежной системы, на участке (в сегменте) которого произошло обнаружение? Обязан ли оператор по переводу денежных средств информировать оператора платежной системы, на участке (в сегменте) которого произошло обнаружение, не зависимо от того, был ли факт воздействия вредоносного кода?

Ответ:

В соответствии с методологией, разрабатываемой Комитетом по платежам и рыночным инфраструктурам (КПРИ) Банка международных расчетов в рамках Стратегии «Снижение риска мошенничества в крупностоимостных платежах, связанного с безопасностью конечных пользователей», предусматривается организация работы в платежных системах, которую должны реализовывать операторы платежной системы в соответствии с законодательством Российской Федерации.

Указанная работа направлена, среди прочего, на организацию информационного взаимодействия участников платежной системы в случае возникновения инцидентов информационной безопасности с целью предотвращения компьютерных атак, распространения вредоносных кодов и, в конечном итоге, снижения количества несанкционированных переводов денежных средств.

[1] «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» (далее – Положение № 382-П)

В проекте нормативного акта Банка России взамен Положения Банка России № 382-П[2] предусмотрено, что оператор платежной системы должен установить требования к содержанию, форме и периодичности направления операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры оператору платежной системы информации для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств.

В свою очередь, оператор платежной системы должен обеспечить учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры информации:

о выявленных в платежной системе инцидентах защиты информации;

о методиках анализа и реагирования на инциденты защиты информации.

Одним из таких инцидентов является распространение вредоносного программного обеспечения.

Обращаем внимание, что о фактах обнаружения вредоносного кода или факта воздействия вредоносного кода в первую очередь должен быть проинформирован ФинЦЕРТ Банка России.

Таким образом, оператор платежной системы должен организовать информационное взаимодействие между участниками своей платежной системы (внутри своей платежной системы), чтобы обеспечить управление рисками в рамках платежной системы в целях недопущения распространения компьютерных атак, вредоносных кодов, снижения риска несанкционированных переводов денежных средств.

2. В настоящий момент в соответствии с Положением № 382-П организации, осуществляющие переводы денежных средств, обязаны проводить оценку выполнения операторами платежных систем требований к обеспечению защиты информации при осуществлении переводов денежных средств с привлечением сторонних организаций, имеющих соответствующую лицензию. Предлагаем рассмотреть возможность проведения банками с базовой лицензией самостоятельной оценки выполнения операторами платежных систем требований к обеспечению защиты информации при осуществлении переводов денежных средств, так как привлечение сторонних организаций не гарантирует достоверность и качество проведенной оценки и, кроме того, требует существенных материальных затрат (не менее 1500 тыс. руб.).

Ответ:

Вплоть до 01.07.2018 в Положении Банка России № 382-П предусматривалась самостоятельная оценка выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее

[2] Положение Банка России от 09.06.2012 № 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» (далее – Положение Банка России № 382-П)

соответственно – оценка соответствия, самооценка) оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры (подпункт 2.15.1 пункта 2.15).

В связи с последними изменениями в Положение Банка России № 382-П[3] самооценка была отменена. Изменения вызваны следующим. При проведении проверок поднадзорными организациями предоставлялись высокие результаты самооценки. Между тем, несмотря на высокие результаты самооценки, указанные организации сталкивались с серьезными инцидентами информационной безопасности, которые приводили к крупным финансовым потерям.

Считаем, что риск возникновения инцидентов защиты информации, которому подвергается кредитная организация, не зависит от крупности организации. Риск определяется в пределах остатков денежных средств, находящихся на корреспондентском счете. В этой связи у кредитных организаций малых форм (например, у банков с базовой лицензией) риски информационной безопасности не менее существенные, чем у крупных кредитных организаций с точки зрения финансовой устойчивости.

Исходя из этого, Банком России сделан вывод, что самооценка представляет собой недостоверный инструмент определения уровня защиты информации в поднадзорной организации.

Поскольку сложилась негативная практика проведения самооценки, Банком России принято решение установить требование о необходимости проведения поднадзорными организациями оценки соответствия внешней проверяющей организацией (так называемый внешний аудит). Кроме того, по данной тематике в Банке России реализуется соответствующий SupTech проект.

3. Банк России планирует внесение изменений в Положение № 382-П? Когда можно будет ознакомиться с проектом изменений?

Ответ:

Банк России подготовил проект Положения взамен Положения Банка России № 382-П.

Проект положения в установленном порядке размещался на сайте Банка России в информационно-телекоммуникационной сети «Интернет» в целях оценки регулирующего воздействия с 13 декабря 2019 года по 26 декабря 2019 года, а также на официальном сайте www.regulation.gov.ru в информационно-телекоммуникационной сети «Интернет» для проведения антикоррупционной экспертизы в период с 13 декабря 2019 года по 19 декабря 2019 года.

4. Планирует ли Банк России в части идентификационной информации, используемой для адресации устройства при регистрации информации о действиях клиентов, выполняемых с использованием автоматизированных систем и программного обеспечения, привести к однозначному соответствию формулировки

---

[3] Указание Банка России от 07.05.2018 № 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»

Положения № 382-П (пункт 2.6.3 «информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению») и Методических рекомендаций Банка России от 21.07.2017 № 18-МР «О подходах к управлению кредитными организациями риском легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма» (пункт 2 «контроль идентификатора устройства, с которого осуществлен доступ клиенту к автоматизированной системе, программному обеспечению»)?

Ответ:

Конечная цель указанной нормы, устанавливающей требования о необходимости регистрации идентификационной информации, используемой для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств (подпункт 2.6.3 пункта 2.6 Положения Банка России № 382-П) (аналогичная норма также содержится в новом проекте Положения взамен Положения № 382-П) - идентификация (с определенной степенью достоверности) устройства, которое используется для осуществления переводов денежных средств.

Регистрация указанных сведений необходима с точки зрения работ по противодействию переводам денежных средств без согласия клиента (далее - антифрод). Идентификационная информация устройств должна предоставляться Банку России. Обладание такой информацией ФинЦЕРТом и кредитными организациями позволит повысить эффективность системы антифрода.

Указанные требования необходимы и Департамент информационной безопасности будет в дальнейшем развивать данную тематику.

В части Методических рекомендаций Банка России от 21.07.2017 № 18-МР «О подходах к управлению кредитными организациями риском легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма» - данный вопрос относится к компетенции Департамента финансового мониторинга и валютного контроля.

5. В связи с вступлением в силу Национального стандарта РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1-2017) и Национального стандарта РФ ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» у банков появилась необходимость проведения аудита сторонней организацией на соответствие данным стандартам. В то же время присутствует требование проведения аудита сторонней организацией на соответствие Положения Банка России № 382-П. По многих проверяемым направлениям данные для аудита пересекаются. Возможно ли для оптимизации материальных затрат и временных ресурсов проводить исключительно аудит по ГОСТам (как наиболее полный), и упразднить требование о проведении аудита по Положению № 382-П?

Ответ:

Банк России подготовил проект Положения взамен Положения Банка России № 382-П.

Проект Положения предусматривает только оценку соответствия требований по ГОСТ Р 57580.1-2017[4] в соответствии с порядком и по форме, указанным в ГОСТ Р 57580.2-2018[5].

6. В части требований ГОСТ Р 57580.1-2017:

- можно ли рассматривать в качестве средства защиты от вредоносного кода межсетевые экраны нового поколения (NGFW), системы обнаружения вторжений или иные схожие средства защиты информации, в которых есть функционал для борьбы с вредоносным кодом, например, для блокирования возможностей взаимодействия с командными серверами, загрузки обновлений, утечки информации и т.п.?

- в тексте стандарта часто используется термин «межсетевое экранирование». Надо ли его трактовать буквально и для его реализации применять только специализированные межсетевые экраны или возможно применение любых технических средств, которые могут обеспечить разграничение доступа на сетевом уровне?

- можно ли в качестве средства реализации меры СМЭ.2 использовать коммутаторы и маршрутизаторы, которые могут фильтровать трафик на сетевом уровне? Или обязательно использовать только отдельно стоящие межсетевые экраны, что во внутренней коммутируемой сети может быть затруднительно?

Ответ:

Банк России не вмешивается в оперативную деятельность поднадзорных организаций. В этой связи Банк России не устанавливает конкретные требования к техническим средствам, которые должны применяться.

Однако с учетом значимости финансового рынка, а также принимая во внимание позицию уполномоченных регуляторов, таких как ФСТЭК России и ФСБ России, полагаем, что в рамках ключевых элементов и пограничных зон (например, когда речь идет о взаимодействии с недоверенной средой, сетью «Интернет», в рамках которых вероятны компьютерные атаки), критичных информационных систем (например, ЕБС), целесообразно применять оборудование, которое прошло оценку соответствия по требованиям ФСТЭК России соответствующего класса, указанного в ГОСТ Р 57580.1-2017 (в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации).

---

[4] Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст) (далее - ГОСТ Р 57580.1-2017)

[5] Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст (далее - ГОСТ Р 57580.2-2018)

7. В соответствии с подпунктом 4.1 пункта 4 Положения № 683-П[6] для осуществления банковских операций допускается использование прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений, к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее - прикладное программное обеспечение), в отношении которого проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013. В связи с чем, просим пояснить, что будет являться свидетельством проведения указанного анализа в отношении прикладного программного обеспечения, разработанного кредитной организацией самостоятельно, а также какие требования по предоставлению свидетельств указанного анализа следует учитывать кредитной организации при составлении договоров о поставке прикладного программного обеспечения внешних разработчиков?

Ответ:

Согласно подпункту 4.1 пункта 4 Положения Банка России № 683-П[7] кредитная организация должны использовать прикладное программное обеспечение, которое либо сертифицировано в системе сертификации ФСТЭК России, либо в отношении которого проведен анализ уязвимостей.

В части сертификации ФСТЭК России подтверждающим документом является сертификат ФСТЭК России.

В части анализа уязвимостей нормативные требования к форме документа, свидетельствующего факт проведения анализа уязвимостей программного обеспечения, не установлены. Указанными документами могут быть акты приемки работ по договору, иным образом оформленные документы, исходя из которых возможно сделать вывод о факте, результатах проведения анализа уязвимостей программного обеспечения.

8. В соответствии с требованиями Положения № 672-П[8] кредитным организациям также необходимо руководствоваться формуляром на СКЗИ «Сигнатура», который требует применения межсетевого экрана, сертифицированного по требованиям ФСБ России. Таких решений сейчас на рынке практически нет (у части решений сертификаты прекратят действие в ближайшее время, и их производители не планируют их продлять). Как Банк России рекомендует выполнять это требование в условиях отсутствия на рынке соответствующих решений? Возможна ли его замена на межсетевой экран,

---

[6] «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

[7] Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (далее – Положение Банка России №683-П)

[8] «О требованиях к защите информации в платежной системе Банка России»

сертифицированный по требованиям ФСТЭК России, как это указано в руководстве по обеспечению ИБ АРМ КБР-Н?

Ответ:

Банком России совместно с уполномоченным в данной сфере органом власти (ФСБ России) выработана согласованная позиция, в соответствии с которой в указанных случаях возможно применение средств защиты информации, в том числе средств защиты информации от вредоносного кода, сертифицированных в системе сертификации ФСТЭК России соответствующего класса.

9. Означает ли, что для выполнения требований Указания № 4926-У[9]:

- *«выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента»*

- *«осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, при их наличии»*

кредитная организация должна за свой счет установить и обслуживать на рабочем месте клиента программное обеспечение для выявления компьютерных атак, направленных на объекты информационной инфраструктуры клиента и осуществляющих сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры клиента или достаточно организационных мероприятий на стороне кредитной организации (нахождение косвенных признаков атак на инфраструктуру клиента, выявляемых на основании анализа событий антифрод-системы или интервью с клиентом, подвергшимся компьютерной атаке)?

Ответ:

В соответствии со статьей 56 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон № 86-ФЗ) Банк России не вмешивается в оперативную деятельность кредитных организаций.

В этой связи кредитные организации самостоятельно принимают решение относительно реализации обязательных к исполнению требований, в том числе Указания № 4926-У[10]. Иными словами, кредитные организации самостоятельно

---

[9] «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»

[10] «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами

определяют необходимость реализации организационных и (или) технических мер, направленных на реализацию требований.

Т.е. кредитные организации могут выбрать реализацию или организационных, или технических мер (программное обеспечение, обеспечивающее выявление компьютерных атак), либо могут использовать оба вида мер одновременно.

Кроме того, рекомендуем применять Стандарт Банка России СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств», в котором подробно даны рекомендации по сбору и анализу соответствующих технических данных. Указанный стандарт направлен на сбор, анализ и придание юридической значимости полученным техническим данным.

Указанный стандарт был разработан совместно с ФСБ России, Следственным комитетом Российской Федерации и МВД России.

10. Будут ли опубликованы сводные результаты проведенной Департаментом информационных технологий Банка России в октябре 2019 года оценки уровня обеспечения информационной безопасности и киберустойчивости в поднадзорных кредитных организациях (письмо от 08.10.2019 № 56-3-7/611)? Каким образом данные результаты будут использоваться Банком России в дальнейшем? Планирует ли Банк России закрепить в нормативных документах минимальный уровень обеспечения информационной безопасности в кредитных организациях, и как данный показатель будет учитываться в оценке деятельности кредитных организаций? Будут ли законодательно закреплены требования к вендорам по обязательному проведению самостоятельной сертификации в системе сертификации ФСТЭК на соответствие требованиям по безопасности информации поставляемого кредитным организациям программного обеспечения и предоставлению кредитным организациям соответствующих документальных подтверждений?

Ответ:

Подробные результаты (со статистикой) проведенной в октябре 2019 года оценки уровня обеспечения информационной безопасности и киберустойчивости в поднадзорных кредитных организациях будут обнародованы в рамках проведения XII Уральского форума «Информационная безопасность финансовой сферы».

Указанные результаты планируется использовать для формирования риск-профилирования поднадзорных организаций, что, в свою очередь, будет использоваться для оценки фактических рисков поднадзорных организаций.

В части минимального уровня защиты информации.

Согласно подпункту 3.1 пункта 3 Положения Банка России № 683-П кредитные организации должны обеспечить усиленный (системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг) и стандартный

платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»

уровень защиты информации (все остальные кредитные организации) в соответствии с ГОСТ Р 57580.1-2017.

Согласно подпункту 9.2 пункта 9 Положения Банка России № 683-П кредитные организации должны обеспечить уровень соответствия не ниже третьего в соответствии с ГОСТ Р 57580.2-2018 с 1 января 2021 года. и уровень соответствия не ниже четвертого с 1 января 2023 года.

В части требований к разработчикам программного обеспечения (вендорам) по самостоятельной сертификации.

Банк России вправе установить требования по защите информации только в отношении поднадзорых организаций (кредитных организаций и некредитных финансовых организаций) (статьи 57.4, 76.4-1 Федерального закона № 86-ФЗ).

Таким образом, требования к разработчикам программного обеспечения Банк России устанавливать не будет.

Поднадзорные организации должны обеспечить контроль использования сертифицированного программного обеспечения (или в отношении которого проведен анализ уязвимостей). Указанное означает, что поднадзорные организации самостоятельно определяют в договорах с разработчиками программного обеспечения необходимость поставки сертифицированного программного обеспечения (или в отношении которого проведен анализ уязвимостей).

11. Вследствие развития информационных технологий, в том числе дистанционного банковского обслуживания, в деятельности банков возрастает значение киберрисков, которые могут представлять значительную опасность для финансовой стабильности банка или его репутации, особенно в том случае, если персональные данные клиентов появляются в открытом доступе. Каким образом будут развиваться подходы к регулированию в области информационной безопасности, в том числе правовые и технологические требования?

Ответ:

Действительно, влияние кибер-рисков на банковскую деятельность, деятельность в сфере финансовых рынков сложно переоценить.

Департаментом информационной безопасности проводится масштабная работа по установлению правовой и технологической основы по вопросу защиты информации в банковской сфере и сфере финансовых рынков[11].

---

[11] Так, приняты 2 основных нормативных акта:

Положение Банка России № 683-П;

Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее – Положение Банка России №684-П).

А также специальный нормативный акт:

Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России».

Общий подход правового регулирования заключается в установлении в нормативных актах Банка России отсылочных положений на требования национальных стандартов (ГОСТы), в которых содержатся конкретные технические и организационные меры. В результате в нормативных актах Банка России сделан акцент на технологические требования к защите информации (описание технологических участков и соответствующих требований к ним).

Необходимо отметить, что национальные стандарты учитывают международный опыт и возможность самостоятельного выбора кредитной организацией (некредитной финансовой организацией) организационных и технических мер на основе риск-ориентированного подхода, с возможностью замены мер на компенсирующие.

Так, в настоящее время активно разрабатываются национальные стандарты по операционному риску и операционной надежности. Данные стандарты планируется разработать в 2020 году и одобрить на публичных слушаниях в подкомитете №1 Технического комитета №122. В дальнейшем планируется нормативно закрепить обязательность их применения, безусловно, с отложенными сроками вступления в силу.

При этом, в качестве важного подхода следует отметить тенденцию сбора необходимых Банку России данных не сколько из отчетности, предоставляемой поднадзорными организациями, а в большей степени путем автоматической выгрузки поднадзорными организациями сведений посредством направления через АСОИ ФинЦЕРТ (автоматизированную систему обработки инцидентов) (например, данных логирования (протоколирования) сведений).

В настоящее время подходы регулирования направлены на унификацию, гармонизацию актов между собой. В частности, планируется гармонизация требований Положения Банка России № 683-П с Положением Банка России № 382-П (планируется новый акт, взамен Положения Банка России № 382-П) (например, в части единого порядка проведения оценки соответствия в соответствии с ГОСТ Р 57580.1-2017).

12. Планирует ли Банк России выпустить методические рекомендации по информационной безопасности для поднадзорных организаций вообще, и для МФО в частности? Будут ли проводиться обучения (учения) для поднадзорных организаций в части информационной безопасности?

Ответ:

Положение Банка России № 684-П устанавливает единые требования к некредитным финансовым организациям.

Учитывая, что некредитные финансовые организации осуществляют различные виды деятельности в сфере финансовых рынков, имеющие свои особенности, Банком России планируется разработка методических рекомендаций в отношении ряда некредитных финансовых организаций.

Относительно обучения (учения) для поднадзорных организаций в части информационной безопасности. Департаментом информационной безопасности планируется проведение киберучений в поднадзорных организациях как формы

риск ориентированного надзора. Целью киберучений является повышение готовности финансовой организации к выявлению рисков и противодействию угрозам в части обеспечения киберустойчивости. В рамках киберучений осуществляется стресс-тестирование в части процедур реагирования и восстановления, управления риском реализации информационных угроз, а также оценка уровня управления бизнес-функциями, переданными на аутсорсинг. По итогам киберучений формируется актуализированный риск-профиль поднадзорной организации.

13. Планирует ли Банк России внедрять профессиональные стандарты в части информационных технологий и информационной безопасности в поднадзорных организациях в качестве обязательных?

Ответ:

Банком России разработан проект профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере». В настоящее время проект профессионального стандарта проходит процедуру согласования в соответствии с Постановлением Правительства Российской Федерации от 22.01.2013 № 23 «О Правилах разработки и утверждения профессиональных стандартов». По итогам согласования стандарт будет направлен в Минтруд России на утверждение.

Кроме того, в рамках реализации мероприятий федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» Банком России проводятся работы по разработке образовательных стандартов, программ переподготовки, практико-ориентированного обучения.

14. Следует ли микрофинансовым организациям (МФО) проводить мероприятия согласно требованиям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»? Что необходимо выполнить МФО для соблюдения требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»?

Ответ:

В части Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ).

Согласно пункту 8 статьи 2 Федерального закона № 187-ФЗ субъектами критической информационной инфраструктуры являются, в том числе, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети,

автоматизированные системы управления, функционирующие в банковской сфере и иных сферах финансового рынка.

В этой связи микрофинансовые организации, в качестве субъектов критической информационной инфраструктуры, обязаны проводить мероприятия, предусмотренные Федеральным законом № 187-ФЗ.

В частности, должны информировать о компьютерных инцидентах ФСБ России. Однако информирование рекомендуем осуществлять через Банк России (АСОИ ФинЦЕРТ). Указанный порядок предусмотрен протоколом о взаимодействии Банка России с ФСБ России.

Относительно соблюдения микрофинансовыми организациями требований Положения Банка России № 684-П.

Требования в отношении объектов информационной инфраструктуры (требования ГОСТ Р 57580.1-2017), требования в отношении сертификации или проведения анализа уязвимостей прикладного программного обеспечения, требования в части технологии обработки защищаемой информации не распространяются на микрофинансовые организации.

Таким образом, микрофинансовые организации вправе самостоятельно определять реализацию уровней защиты информации в соответствии с ГОСТ Р 57580.1-2017.

15. Каков порядок проверки МФО со стороны Банка России в части информационной безопасности?

Ответ:

В соответствии со статьей 76.5 Федерального закона № 86-ФЗ порядок проведения проверок, в том числе определение обязанностей проверяемых лиц по содействию в проведении проверок, и порядок применения иных мер устанавливаются нормативными актами Банка России.

Таким образом, проверка микрофинансовых организаций проводится в общем порядке. Однако, безусловно, при проведении проверок учитываются особенности деятельности поднадзорных организаций, в пределах компетенции Департамент информационной безопасности разрабатывает методики проверки.

16. Каким образом следует аттестовать места для снятия биометрии в привязке к конкретным помещениям и рабочим местам на предмет соответствия Приказу ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»? В настоящее время при реализации своих полномочий ФСТЭК России признает только один способ контроля соответствия – аттестация объекта информатизации лицензиатом ФСТЭК России с лицензией на ТЗКИ. Аттестация выполняется в привязке к конкретных помещениям и рабочим местам, и если подходить к ней буквально, действительна до первого факта обновления программного обеспечения (например, обновления безопасности операционной системы) или изменения положения рабочего места, а в случае нестационарного рабочего места невозможна в принципе. При этом отсутствие аттестата на объект информатизации, на котором

обрабатываются персональные данные (в том числе биометрические), грозит санкциями для кредитной организации при проверке.

В этой связи кредитные организации предлагают отказаться от аттестации мест для снятия биометрии в привязке к конкретным помещениям и рабочим местам и перейти к аттестации типового программно-аппаратного решения, тиражируемого внутри организации.

Ответ:

Относительно биометрических персональных данных рекомендации к их обработке в ЕБС подробно описаны в Методических рекомендациях по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утв. Банком России 14.02.2019 № 4-МР).

В указанных методических рекомендациях отсутствуют требования к аттестации мест для снятия биометрических персональных данных в привязке к конкретным помещениям и рабочим местам.

С точки зрения обработки персональных данных Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» также не содержит требований к необходимости проверки мест для снятия биометрических персональных данных в привязке к конкретным помещениям и рабочим местам. Предлагаем обратиться к регулятору в данной области – ФСТЭК России.

17. Действующее законодательство в области распространения шифровальных криптографических средств, в частности требование об их поэкземплярном учете, вступают в конфликт с требованиями об использовании сертифицированных средств криптографической защиты информации в мобильном приложении удаленной идентификации лиц в ЕБС. Существующая нормативная база по распространению коммерческих средств криптографической защиты информации создает сложности при удаленной идентификации лиц в ЕБС, использующих мобильное приложение. При осуществлении лицензируемого вида деятельности ФСБ России требует обеспечить поэкземплярный учет СКЗИ, который в случае с мобильным приложением невозможен, так как на момент его установки идентификация субъекта еще не возможна. Предлагается гармонизировать требования законодательства за счет активации функциональности с помощью SMS, считая это способом идентификации абонента через оператора сотовой связи. Так как при скачивании мобильного приложения распространение СКЗИ осуществляется с сайта нерезидента (Google/Apple), то требование о поэкземплярном учете коммерческих СКЗИ фактически делает нелигитимным распространение мобильных приложений с ГОСТовой криптографией через магазины приложений.

Ответ:

Департамент информационной безопасности осведомлен об указанной проблеме. Поэкземплярный учет СКЗИ, действительно, препятствует широкому распространению отечественной гражданской криптографии. Вместе с тем, данный вопрос находится в компетенции ФСБ России.

В этой связи Банк России совместно с ФСБ России прорабатывает решения указанной проблемы.

Так, указанный вопрос поднимался в рамках национальной программы «Цифровая экономика Российской Федерации», в частности по направлению в сфере развития гражданской криптографии. Банк России планирует продолжить работу по данному направлению в рамках национальной программы «Цифровая экономика Российской Федерации».