Ассоциация банков России
(Ассоциация «Россия»)

ПРЕЗИДЕНТ

119180, Москва, ул. Большая Якиманка, д.23
www.asros.ru
asros@asros.ru
т. 8-(495)-785-29-90

от 11.03.2024 № 02-05/238

На №_____от_____

Директору Департамента
информационной безопасности
Банка России

В.А. Уварову

Уважаемый Вадим Александрович!

В Ассоциацию банков России обращаются кредитные организации по вопросам информационной безопасности и соблюдения требований нормативных правовых актов в области обеспечения защиты информации.

В частности, члены Ассоциации просят регулятора высказать позицию относительно перспектив использования аутсорсинга информационной безопасности и страхования киберрисков, а также разъяснить порядок исполнения требований к применению средств криптографической защиты информации (СКЗИ).

Просим Вас рассмотреть поступившие вопросы и предложения кредитных организаций (в приложении) и направить ответы и комментарии к ним в адрес Ассоциации.

Приложение: на 6 л. в 1 экз.

И.о. Президента А.А. Войлуков

Жижанов Г.В., 8-499-678-30-13

Приложение

Вопросы и предложения кредитных организаций по вопросам информационной безопасности

1. В настоящее время в Государственной Думе Федерального Собрания Российской Федерации рассматривается законопроект № 404786-8[1], направленный на возможность применения ИТ-аутсорсинга и облачных сервисов. Кредитные организации просят сообщить:

- Позволит ли принятие законопроекта № 404786-8 реализовать сервисную модель оказания услуг кибербезопасности в целях повышения доступности сервисов информационной безопасности для небольших банков?
- В соответствии с Требованиями к СКЗИ[2], утвержденными ФСБ России по согласованию с Банком России, системное ПО не должно содержать модулей, использующих технологию аппаратной виртуализации физических ресурсов. Это означает, что в отношении такого ПО фактически не может применяться облачная модель оказания услуг. Планирует ли Банк России инициировать пересмотр указанных Требований к СКЗИ, чтобы разрешить применение технологии аппаратной виртуализации и, как следствие, облачной модели оказания услуг в отношении ряда ПО, используемого в финансовых организациях?

---

[1] Законопроект № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» (в части совершенствования правовых основ для аутсорсинга информационных технологий и использования облачных услуг финансовыми организациями).

[2] Требования к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 Положения 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», утверждены ФСБ России 28.02.2020 № ФТ-56-3/32.

2. Положениями № 683-П[3] и № 757-П[4] установлены требования к защите информации (ЗИ) при осуществлении банковской деятельности и деятельности в сфере финансовых рынков соответственно, а также к оценке соответствия уровня ЗИ по методике, определенной положениями ГОСТ Р 57580.2-2018[5].

Оценка уровня соответствия ЗИ проводится на основе сравнения результирующей числовой оценки выполнения требований к организационным и техническим мерам ЗИ, а также к планированию, реализации, контролю и совершенствованию процесса ЗИ финансовой организации с нормативными показателями, указанными в пункте 7.9 ГОСТ Р 57580.2-2018. Например, кредитные организации согласно пункту 9.2 Положения № 683-П с 01.01.2023 обязаны обеспечить уровень соответствия не ниже четвертого, что соответствует числовому показателю не менее 0,85.

В этой связи члены Ассоциации просят уточнить, допустимо ли для финансовой организации выполнение требований Положений № 683-П и № 757-П не в полном объеме в случае, если данный факт не повлияет на достижение нормативно установленного уровня соответствия требованиям к ЗИ?

3. При реализации разработчиком безопасного жизненного цикла, указанного в разделе 7.4 Профиля защиты[6], финансовая организация вправе перейти от выполнения требований к оценочному уровню доверия[7] ПО к соблюдению методологии безопасного жизненного цикла ПО.

---

[3] 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».

[4] Положение Банка России от 20.04.2021 № 757-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».

[5] Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

[6] Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций.

[7] В соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

При этом Профиль защиты построен на базе каскадной модели, в которой процесс разработки ПО выглядит как поток, состоящий из последовательных фаз анализа требований, проектирования, реализации, тестирования, интеграции и поддержки. В настоящее время такой подход практически не используется разработчиками, которые перешли на более гибкую методологию непрерывной разработки (например, CI/CD[8]). Кроме того, Профиль защиты не может применяться в отношении ЗОКИИ. Все это существенно ограничивает его практическую применимость.

В этой связи в целях расширения возможностей кредитных организаций по применению Профиля защиты просим разъяснить следующие вопросы:

- в какие сроки Банк России планирует пересмотреть требования раздела 7.4 Профиля защиты с точки зрения их адаптации и синхронизации с современными методологиям гибкой и непрерывной разработки ПО, а также распространить их действие на ЗОКИИ?
- рассматривает ли Банк России возможность применения раздела 7.4 Профиля защиты для целей признания разработанного согласно требованиям данного раздела ПО, соответствующим критериям импортозамещения, чтобы его можно было использовать наряду с ПО, включенным в реестр[9] Минцифры России?

4. В соответствии с пунктом 5 части 2 статьи 6 Закона № 572-ФЗ[10] Минцифры России распространяет на безвозмездной основе для физических и юридических лиц шифровальное (криптографическое) средство для целей работы с биометрией. Планирует ли Банк России участвовать в создании и распространении среди финансовых организаций таких средств в целях

---

[8] continuous integration/ continuous delivery – непрерывная интеграция и непрерывное развертывание.

[9] Единый реестр российских программ для электронных вычислительных машин и баз данных.

[10] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

обеспечения защиты устройств клиентов, с которых осуществляется фотографирование для целей аутентификации по биометрии?

5. В соответствии с требованиями пункта 5.1 Положения № 683-П кредитные организации должны обеспечить целостность электронных сообщений и подтвердить их составление уполномоченным на это лицом с использованием усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения и имеющих сертификат соответствия требованиям ФСБ России.

Кредитные организации отмечают, что при встраивании такого СКЗИ в мобильные приложения (МП) требуется проведение длительной процедуры оценки влияния[11], которая длится более 7-9 месяцев, а также проведение последующих проверок при внесении любых изменений в МП. При этом, учитывая высокую частоту обновлений МП, реализация данного требования на практике приводит к значительным издержкам и трудозатратам кредитных организаций.

В этой связи предлагается рассмотреть возможность применения для указанных выше целей СКЗИ, не имеющих сертификат соответствия требованиям ФСБ России, что позволит не проводить формальные процедуры оценки влияния и упростит реализацию принципов непрерывной разработки. При этом уровень безопасности фактически не изменится, так как реализация такими СКЗИ функции имитозащиты информации будет по-прежнему обеспечена.

Аналогичный подход предлагается применить также при встраивании программного модуля Платформы цифрового рубля Банка России в МП банков.

---

[11] В соответствии с Приказом ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6. В соответствии с требованиями пункта 1.2 Указания № 6541-У[12] предусмотрена обязанность применения СКЗИ класса КС2 в сценариях использования биометрии для банкоматов и диспенсеров талонов очередей. По мнению ряда кредитных организаций, применение таких требований к указанным устройствам является избыточным и приводит к значительным издержкам на обеспечение установленного уровня безопасности. В целях митигации возможных рисков банками уже применяются организационно-технические меры защиты. В частности, в отношении банкоматов осуществляются дополнительные меры, связанные с контролем вскрытия корпуса и отсутствием внешних интерфейсов подключения, а диспенсеры талонов очередей всегда располагаются в пределах контролируемой зоны и не используются для дальнейших юридически значимых операций.

В этой связи в целях оптимизации нагрузки на кредитные организации, особенно в условиях импортозамещения средств защиты информации, в сценариях использования биометрии для банкоматов и диспенсеров талонов очередей предлагается рассмотреть возможность применения СКЗИ более низкого класса КС1.

7. В соответствии с требованиями Закона № 572-ФЗ и Указания № 6541-У в биометрические POS-терминалы (биоPOS-терминалы) должны быть встроены сертифицированные СКЗИ для проверки электронной подписи и шифрования обрабатываемых биометрических персональных данных (бПДн). В настоящее время по требованиям ФСБ России[13] период действия закрытых ключей СКЗИ POS-терминалов ограничен сроком 1 год и 3 месяца, при этом срок

---

[12] Указание Банка России от 25.09.2023 № 6541-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами».

[13] Функционально-технические требования к техническим средствам и программному обеспечению, реализующим СКЗИ в платежных устройствах с терминальным ядром, утверждены Банком России 28.02.2020 № ФТ-56-3/33.

использования POS-терминалов гораздо больше и в среднем составляет 7-10 лет. По этой причине кредитным организациям за время использования терминала приходится несколько раз получать ключи СКЗИ, что влечет за собой значительные трудовые и финансовые издержки.

В этой связи члены Ассоциации предлагают рассмотреть возможность увеличения срока действия ключей для СКЗИ, применяемых в составе биоPOS-терминалов. Такая мера не приведет к снижению защищенности биоPOS-терминалов, так как их применение производится со строгим соблюдением дополнительных требований по защите обрабатываемой информации в рамках сертификации по требованиям международного стандарта PCI PTS POI[14]. Данный стандарт предусматривает невозможность доступа пользователей и администраторов к настройкам и файловым ресурсам устройств, применение специальных механизмов уничтожения информации, в том числе закрытых ключей СКЗИ, при вскрытии корпуса биоPOS-терминала, а также штатное отключение гарантированным способом функциональности биоPOS-терминалов при сбоях.

Кроме того, в целях совершенствования процедур работы биоPOS-терминалов и снижения излишней административной нагрузки предлагается отменить требование по их обязательной ежедневной перезагрузке.

8. Члены Ассоциации заинтересованы в развитии страхования киберрисков и в этой связи просят Банк России рассмотреть и оценить возможность реализации инициативы об увеличении ответственности операторов персональных данных (ОПДн) перед гражданами за утечки их персональных данных и установлении требования по страхованию киберрисков и/или оформлению банковской гарантии в качестве обязательного условия получения статуса ОПДн. В этом случае страховая компания или банк будут заинтересованы в высоком уровне защиты данных на стороне ОПДн, будут проводить его оценку и давать рекомендации по мероприятиям, направленным на его повышение.

---

[14] Стандарт безопасности Payment Card Industry Security Standards Council (PCI SSC) «PIN Transaction Security. Point of Interaction».