СТАНДАРТ ПЛАТФОРМЫ ЦИФРОВОГО РУБЛЯ

«Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований»

Настоящий стандарт платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований» (далее – Порядок), созданный на основании приказа ФСБ России от 09.02.2005 № (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (далее – Положение ПКЗ-2005), устанавливает процедуры выполнения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России (далее – ПМ БР), на выполнение предъявленных к входящему в его состав средству криптографической защиты информации (далее – СКЗИ) требований.

Настоящий Порядок предназначен для использования финансовыми организациями – участниками платформы цифрового рубля (далее – участники ПлЦР)[1], которые разрабатывают программное обеспечение для мобильных устройств – мобильное приложение (далее – МП), осуществляют встраивание программного модуля Банка России в МП, в том числе с привлечением внешнего подрядчика, и имеют в соответствии с постановлением Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств,

[1] Указанный порядок распространяется только на финансовые организации – участников ПлЦР и не распространяется на Банк России.

выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» лицензию по п. 2 приложения к Положению о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденному постановлением Правительства Российской Федерации от 16.04.2012 № 313[2].

Общие положения

Под программными средствами сети (системы) конфиденциальной связи подразумеваются программные средства, предоставляемые участником

[2] В случае привлечения подрядчика для выполнения работ в полном объеме подрядчик должен иметь указанную лицензию, а участник ПлЦР, при условии, что все работы, подлежащие лицензированию, делает подрядчик, может ее не иметь.

ПлЦР пользователю платформы цифрового рубля (далее – пользователь ПлЦР).

Объектом настоящего Порядка является программное средство – МП, которое использует встроенный ПМ БР, содержащий в своем составе сертифицированное СКЗИ[3].

ПМ БР встраивается в МП и применяется пользователем платформы цифрового рубля для обеспечения конфиденциальности, целостности и установления авторства электронных сообщений, в частности для:

генерации и хранения криптографических ключей;

создания запросов на сертификаты;

хранения сертификатов и списка аннулированных сертификатов;

подписания исходящих электронных сообщений;

шифрования исходящих электронных сообщений;

проверки подписи входящих электронных сообщений;

расшифрования входящих электронных сообщений;

установки канала(ов) связи, защищенного(ых) с использованием протокола TLS в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)» или с Рекомендациями по стандартизации Р 1323565.1.030-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)».

Предметом настоящего Порядка являются отношения между участником ПлЦР, 8 Центром ФСБ России и специализированной организацией (далее − лаборатория), которой 8 Центром ФСБ России предоставлено право проводить исследования по оценке влияния

[3] В том числе, ПМ БР может сам являться СКЗИ.

программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований. При этом в рамках данного порядка может быть задействована только та лаборатория, которая проводила работы по первичной оценке влияния МП на входящие в их состав СКЗИ или ПМ БР с СКЗИ по техническому заданию, согласованному с 8 Центром ФСБ России. В случае необходимости смены лаборатории, проводившей работы по первичной оценке влияния, и возможности применения данного Порядка совместно с такой лабораторий, необходимо провести работы по оценке влияния по техническому заданию, согласованному с 8 Центром ФСБ России.

Настоящий Порядок применим только к таким МП, для которых в выписке из заключения по оценке влияния на входящие в его состав ПМ БР с СКЗИ есть разрешения применения данного Порядка. В случае отсутствия в выписке из заключения по оценке влияния на входящие в их состав ПМ БР с СКЗИ разрешения применения данного Порядка или невозможности применения данного порядка оценка влияния производится в соответствии с п. 35 Положения ПКЗ-2005.

В случае внесения изменений в МП, на которое проведена первичная оценка влияния, отношения в соответствии с данным Порядком не могут превышать 3 лет с момента проведения оценки влияния МП на входящее в его состав ПМ БР с СКЗИ по техническому заданию, согласованному с 8 Центром ФСБ России.

Обязанности участника ПлЦР при использовании настоящего Порядка

В организационной структуре участника ПлЦР должна быть введена отдельная служба безопасности и контроля, осуществляющая функции контроля эксплуатации МП и ПМ БР в составе МП и подчиняющаяся непосредственно руководителю (заместителю руководителя) организации, курирующему блок (подразделение) информационной безопасности (в

соответствии с указом Президента Российской Федерации от 1 мая 2022 г. №250) (далее – руководство участника ПлЦР).

Сотрудниками службы безопасности и контроля должны быть специалисты, которые имеют высшее профессиональное образование по направлению подготовки (специальности) в области информационной безопасности или «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей и (или) переподготовку по одной из специальностей этого направления (нормативный срок – свыше 360 аудиторных часов), обладают высокой осведомленностью в вопросах обеспечения информационной безопасности, имеют достаточные, по заключению руководства участника ПлЦР, компетенции в области безопасности прикладного программного обеспечения и принципов безопасной разработки. Общий стаж работы в области информационной безопасности у одного из специалистов службы безопасности и контроля должен быть не менее 3 лет.

В обязанности специалистов службы безопасности и контроля должны входить[4]:

-контроль за процессом безопасной разработки МП, использующего ПМ БР;

-проведение мероприятий по контролю целостности распространяемого МП и предоставление соответствующих сведений в лабораторию;

-контроль за хранением актуальной версии МП, на которую получены положительные выводы от лаборатории или в отношении которой проведена оценка влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение

[4] В частности, в обязательном порядке проверяется отсутствие в МП:
- средств разработки;
- средств мониторинга использования криптографических ключей;
- опасных конструкций кода, которые могут привести к уязвимостям.

предъявленных к входящему в его состав СКЗИ требований (далее − эталонный образец).

Обязанности, которые определены в настоящем Порядке, должны являться приоритетными для специалистов службы безопасности и контроля.

В случае привлечения внешнего подрядчика для разработки программного обеспечения порядок ознакомления сотрудника службы безопасности и контроля с исходным кодом определяется договором между участником ПлЦР и внешним подрядчиком, имеющим необходимую лицензию ФСБ России.

Порядок контроля за выводами специалистов службы безопасности и контроля должен входить в состав условий договора между лабораторией и участником ПлЦР.

Первичное проведение оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований

Участник ПлЦР после выбора и получения в пользование ПМ БР, включая полный комплект необходимой документации, выполняет работы по его встраиванию в МП.

Участник ПлЦР заключает договор с лабораторией о проведении работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований в соответствии с Положением ПКЗ-2005 и дальнейшего сопровождения процесса изменений МП.

До начала проведения работ участником ПлЦР заключается согласие об обеспечении информационной безопасности МП со встроенным ПМ БР

(приложение 1 «Согласие финансовой организации об обеспечении информационной безопасности мобильного приложения со встроенным ПМ БР»). После утверждения руководством финансовой организации – участника ПлЦР указанного согласия экземпляр направляется в Банк России, и в лабораторию (лаборатория по запросу может предоставить согласие в ФСБ России).

Лаборатория совместно с участником ПлЦР на основании нормативных документов, эксплуатационной документации и исходного кода МП проводит необходимые работы по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав требований.

В эксплуатационной документации на МП должны быть определены условия, неизменность которых будет являться достаточной для подтверждения безопасности МП в части влияния на входящий в его состав ПМ БР, включая неизменность трасс вызовов[5] и порядка вызовов ПМ БР в составе МП, а также неизменность реализации функционала отображения[6] подписываемого содержимого электронного сообщения. Трассы вызовов и порядок вызовов ПМ БР разрабатываются (согласовываются) совместно с лабораторией, проводящей первичную процедуру оценки влияния.

Неотъемлемой частью эксплуатационной документации на МП также должны являться зафиксированные контрольные суммы на исполняемый код МП и ПМ БР в составе МП. Порядок ознакомления лаборатории с исходным кодом определяется договором между участником ПлЦР и лабораторией.

Комплект эксплуатационной документации на МП согласовывается с

[5] Под трассами вызовов понимается, к примеру, последовательность инструкций, которые выполняются при вызове функций ПМ. Взаимодействие должно осуществляться по стандартизированным инструкциям (последовательностям вызовов), которые должны быть неизменны.

[6] Под неизменностью подразумевается отображение электронного сообщения без его модификации по структуре или полям: к примеру, шрифты, дизайн окна визуализации электронного сообщения и т.п. не влияют на данный пункт требования.

лабораторией и утверждается руководством финансовой организации – участником ПлЦР.

При положительных результатах проведенных работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав СКЗИ требований лаборатория направляет результаты данных исследований и комплект необходимой эксплуатационной и технической документации на МП в 8 Центр ФСБ России.

По итогам рассмотрения 8 Центром ФСБ России результатов исследований заказчик работ (участник ПлЦР) получает выписку из заключения 8 Центра ФСБ России об оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав СКЗИ требований, содержащую условия соблюдения требований по информационной безопасности при процессе изменения МП.

Распространению пользователям ПлЦР через официальный канал передачи подлежит только МП, на которое участником ПлЦР получена выписка о положительном заключении 8 Центра ФСБ России об оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР с СКЗИ, на выполнение предъявленных к входящему в его состав СКЗИ требований.

Дальнейший порядок действий в случае отсутствия необходимости модификации МП

При отсутствии необходимости модификации МП специалист службы безопасности и контроля на регулярной основе (не реже 1 раза в месяц) осуществляет сравнение контрольных сумм МП и ПМ БР с СКЗИ в составе

МП с контрольными суммами, указанными в эксплуатационной документации на МП.

В случае отсутствия изменений контрольных сумм МП и ПМ БР сотрудник службы безопасности и контроля составляет отчет о результатах проведенного контроля и передает его в лабораторию. Лаборатория принимает отчет и 1 раз в 6 месяцев сообщает аккумулированную информацию в 8 Центр ФСБ России. В случае изменения контрольных сумм МП и ПМ БР в составе МП специалист службы безопасности и контроля обязан проинформировать:

руководство участника ПлЦР для принятия решения о блокировке использования МП;

лабораторию, которая не позднее 1 рабочего дня направляет письмо об инциденте в 8 Центр ФСБ России;

Банк России в рамках информирования об инцидентах информационной безопасности.

По решению руководства участника ПлЦР после информирования об инциденте специалист службы безопасности и контроля передает ответственному по эксплуатации МП подразделению участника ПлЦР копию эталонного образца МП для восстановления и распространения.

Распространение МП без предварительной сверки контрольных сумм, а также при неуспешной сверке контрольных сумм недопустимо.

Дальнейший порядок действий в случае необходимости модификации МП

При необходимости модификации МП сотрудник службы безопасности и контроля до введения модифицированного МП в эксплуатацию исследует изменения кода МП. Дополнительно сотрудник службы безопасности и контроля проводит контроль целостности путем сравнения контрольных сумм исполняемого кода ПМ БР в составе МП, а также проверяет другие условия обеспечения информационной безопасности, указанные в эксплуатационной и технической документации.

В случае изменения контрольных сумм исполняемого кода ПМ БР в составе МП, удаления, нарушения либо появления новых трасс вызовов ПМ БР в составе МП, а также нарушения других условий обеспечения информационной безопасности сотрудник службы безопасности и контроля сообщает об этом в лабораторию.

При наступлении таких событий участник ПлЦР должен инициировать работы по проведению оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований в соответствии с Положением ПКЗ-2005.

Ввод в эксплуатацию такого МП возможен только после получения участником ПлЦР положительного заключения от лаборатории и выписки о положительном заключении 8 Центра ФСБ России об оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав СКЗИ требований и достаточности мер по обеспечению безопасности МП.

В случае отсутствия изменений контрольных сумм исполняемого кода ПМ БР в составе МП, отсутствия нарушения либо появления новых трасс вызовов ПМ БР в составе МП, а также отсутствия нарушений других условий обеспечения информационной безопасности сотрудник службы безопасности и контроля составляет отчет об изменениях МП, в котором делает обоснованный вывод об отсутствии влияния изменений МП на функционирование ПМ БР в составе МП, фиксирует новую контрольную сумму МП и до ввода его в эксплуатацию передает в лабораторию отчет об изменениях МП, исходный код МП и новые контрольные суммы МП.

Требования к составу предоставляемых в лабораторию сведений определяется в договоре между участников ПлЦР и лабораторией.

Лаборатория обязана регулярно принимать отчеты об изменениях МП и новые контрольные суммы МП, проверять выводы специалиста службы безопасности и контроля, осуществлять расчет контрольных сумм и передавать свои выводы участнику ПлЦР в соответствии со сроками, указанными в договоре. Ввод в эксплуатацию МП возможен только после получения положительных выводов по исследованиям от лаборатории[7].

Лаборатория обязана 1 раз в 6 месяцев сообщать аккумулированную информацию в 8 Центр ФСБ России, а также делать отметку об изменениях контрольных сумм в листе изменений эксплуатационной документации на МП после получения выводов по результатам анализа изменений.

[7] Сроки предоставления ответа лаборатории фиксируются в договоре между лабораторией и участником ПлЦР. Допускается устанавливать штрафные санкции по отношению к лаборатории в случае непредставления выводов в установленный срок.

Приложение 1
к стандарту платформы цифрового рубля
«Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований»

Согласие финансовой организации об обеспечении информационной безопасности мобильного приложения со встроенным программным модулем Банка России в соответствии со стандартом платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований»

В целях обеспечения информационной безопасности при использовании цифрового рубля, а также обеспечения корректного использования ПМ БР в составе МП _____ – участника ПлЦР
(наименование финансовой организации)
(далее – участник ПлЦР) принимает на себя обязательство:

1. Использовать ПМ БР в строгом соответствии с эксплуатационной документацией.

2. Сформировать в финансовой организации – участнике ПлЦР службу безопасности и контроля с прямым подчинением непосредственно

руководителю организации, курирующему блок (подразделение) информационной безопасности.

3. Обеспечить создание должностных инструкций сотрудников службы безопасности и контроля в соответствии с Порядком проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав СКЗИ требований.

4. Заключить договор с лабораторией на проведение работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование ПМ БР, на выполнение предъявленных к входящему в его состав СКЗИ требований, включающий в себя работы по проведению контроля выводов службы безопасности и контроля, а также предоставление достоверных сведений по указанным работам в 8 Центра ФСБ России в соответствии с Порядком проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований, с _____, являющейся лабораторией в соответствии с настоящим порядком.

5. Наделить службу безопасности и контроля функциями, обеспечивающими выполнение обязанностей, установленных данным Порядком.

6. Не распространять МП в открытом доступе, в том числе в официальных магазинах приложений, в случае несоответствия контрольных сумм и/или при наличии отрицательных выводов от лаборатории или 8 Центра ФСБ России.

7. В случае предоставления в лабораторию недостоверных сведений лаборатория имеет право проинформировать об этом 8 Центр ФСБ России и Банк России. В случае подтверждения факта предоставления недостоверных сведений Департамент информационной безопасности Банка России по согласованию с 8 Центром ФСБ России имеет право признать данное согласие в отношении участника ПлЦР неисполненным. С даты признания согласия неисполненным прекращается применение участником ПлЦР Порядка проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований.

Руководитель
_____– участника
(наименование финансовой организации)
ПлЦР, курирующий блок
(подразделение) информационной
безопасности _____/_____
(Подпись) (ФИО)

«____»_____ 20__ г.