СТАНДАРТ ПЛАТФОРМЫ ЦИФРОВОГО РУБЛЯ

УТВЕРЖДАЮ

Заместитель руководителя
Научно-технической службы –
начальник 8 Центра ФСБ России

_____О.В. Скрябин

«07» 05 2026 г.

Порядок проведения работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований

СОГЛАСОВАНО

Директор Департамента
информационной безопасности
Банка России

_____ В.А. Уваров

«07» 05 2026 г.

Настоящий стандарт платформы цифрового рубля «Порядок проведения работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований» (далее – Порядок), созданный на основании приказа ФСБ России от 09.02.2005 № 66 (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 средств криптографической защиты информации (далее – СКЗИ), применяемых для реализации функций приложения клиента[1], или программного модуля[2] в составе приложения клиента, отвечающего требованиям Стандарта платформы цифрового рубля «Спецификация на программный модуль» (далее при совместном упоминании – криптографические средства), на выполнение предъявленных к СКЗИ требований (далее – Оценка влияния).

Настоящий Порядок предназначен для использования финансовыми организациями – участниками платформы цифрового рубля (далее – участники ПлЦР)[3], которые разрабатывают приложение клиента, в том числе с привлечением внешнего подрядчика участника ПлЦР, 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

[1] Термин «приложение клиента» используется в Порядке в значении, определенном Положением Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля».

[2] Программный модуль содержит в своем составе СКЗИ или сам является СКЗИ.

[3] Указанный порядок распространяется на участников ПлЦР, внешних подрядчиков участников ПлЦР и не распространяется на Банк России.

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)» лицензию, включающую перечень работ согласно 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[4].

Общие положения

[4] В случае привлечения внешнего подрядчика участника ПлЦР для выполнения работ в полном объеме он должен иметь лицензию по пункту 2 Приложения к Постановлению Правительства Российской Федерации от 16.04.2012 № 313, а участник ПлЦР, при условии, что все работы, подлежащие лицензированию, делает внешний подрядчик участника ПлЦР, такую лицензию может не иметь.

Криптографические средства применяются для обеспечения конфиденциальности, целостности и установления авторства электронных сообщений при осуществлении операций с цифровым рублем и иных операций. Они в частности могут применяться 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 и внешним подрядчиком участника ПлЦР (в случае его наличия), 8 Центром ФСБ России и специализированной организацией (далее – лаборатория), которой 8 Центром ФСБ России предоставлено право проводить исследования по оценке влияния программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований с целью проведения работ по первичной Оценке влияния и

дальнейшему сопровождению изменений приложений клиента на этапе его эксплуатации.

При этом в рамках настоящего Порядка может быть задействована только та лаборатория, которая проводила работы по первичной Оценке влияния по техническому заданию, согласованному с 8 Центром ФСБ России. В случае необходимости смены лаборатории, проводившей работы по первичной Оценке влияния, и возможности применения настоящего Порядка совместно с такой лабораторией, ей необходимо провести работы по Оценке влияния на основании технического задания, согласованного с 8 Центром ФСБ России.

Настоящий Порядок применим только к таким приложениям клиента, для которых в выписке из заключения по результатам первичной Оценке влияния есть разрешения применения настоящего Порядка. В случае отсутствия в выписке из заключения по результатам первичной Оценке влияния разрешения применения настоящего Порядка или невозможности его применения Оценка влияния производится в соответствии с п. 35 Положения ПКЗ-2005.

В случае внесения изменений в приложение клиента, на которое проведена первичная Оценка влияния, отношения в соответствии с настоящим Порядком не могут превышать 3 лет с момента получения положительного заключения по результатам экспертизы отчетных материалов о проведении Оценки влияния приложения клиента 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 приложения клиента и криптографических средств 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 сотрудников службы безопасности и контроля должен быть не менее 3 лет.

В обязанности сотрудников службы безопасности и контроля должны входить:

- контроль за процессом безопасной разработки приложения клиента[5];
- проведение мероприятий по контролю целостности распространяемого приложения клиента и предоставление соответствующих сведений в лабораторию;
- контроль за хранением актуальной версии приложения клиента, на которую получены положительные выводы от лаборатории или в отношении которой проведена Оценка влияния (далее – эталонный образец).

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

---

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

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

Порядок контроля за выводами службы безопасности и контроля должен входить в состав условий договора между лабораторией и участником ПлЦР. В случае, если договор на первичную Оценку влияния заключен между лабораторией и внешним подрядчиком участника ПлЦР, то порядок контроля за выводами службы безопасности и контроля должен входить как в состав условий договора между лабораторией и внешним подрядчиком участника ПлЦР, так и в состав условий договора между внешним подрядчиком участника ПлЦР и участником ПлЦР.

Проведение первичной Оценки влияния

Участник ПлЦР (или внешний подрядчик участника ПлЦР) после выбора и получения в пользование криптографических средств, включая полный комплект необходимой документации, выполняет работы по их встраиванию в приложение клиента с учетом эксплуатационной документации на криптографическое средство.

Участник ПлЦР (или внешний подрядчик участника ПлЦР) заключает договор с лабораторией о проведении работ по Оценке влияния в соответствии с Положением ПКЗ-2005 и дальнейшем сопровождении процесса изменений приложения клиента.

До начала проведения работ участником ПлЦР утверждается согласие об обеспечении информационной безопасности приложения клиента (приложение 1 «Согласие финансовой организации об обеспечении информационной безопасности приложения клиента в соответствии со стандартом платформы цифрового рубля «Порядок проведения работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение

предъявленных к ним требований»). После утверждения руководством участника ПлЦР указанного согласия экземпляр направляется в Департамент информационной безопасности Банка России и в лабораторию.

Лаборатория совместно с участником ПлЦР (или внешним подрядчиком участника ПлЦР) на основании нормативных документов, эксплуатационной и технической документации и исходного кода приложения клиента проводит необходимые работы по первичной Оценке влияния.

В эксплуатационной и технической документации на приложение клиента должны быть определены условия, являющиеся достаточными для подтверждения безопасности приложения клиента. Данные условия должны включать в себя перечень критических событий, реализация любого из которых потребует проведения участником ПлЦР (или внешним подрядчиком участника ПлЦР) повторных работ по Оценке влияния в соответствии с Положением ПКЗ-2005. К критическим событиям включая, но не ограничиваясь, относятся:

- изменение контрольных сумм исполняемого кода криптографических средств;
- изменение системы сбора аналитики (логирования) работы СКЗИ;
- изменение факторов аутентификации, используемых при доступе к ключевой информации (исключая случаи добавления новых при сохранении существующих факторов аутентификации).

Полный перечень критических событий, а также окружение криптографических средств разрабатывается (согласовывается) участником ПлЦР (или внешним подрядчиком участника ПлЦР) совместно с лабораторией, проводящей работы по первичной Оценке влияния, и фиксируется в эксплуатационной и технической документации на приложение клиента.

Неотъемлемой частью эксплуатационной и технической документации на приложение клиента также должны являться зафиксированные

контрольные суммы на исполняемый код[6] приложения клиента и криптографических средств. Порядок передачи в лабораторию исходных кодов определяется договором между участником ПлЦР (или внешним подрядчиком участника ПлЦР) и лабораторией.

Комплект эксплуатационной и технической документации на приложение клиента согласовывается с лабораторией и утверждается руководством участника ПлЦР.

При положительных результатах проведенных работ по Оценке влияния лаборатория направляет в 8 Центр ФСБ России результаты данных исследований, комплект необходимой эксплуатационной и технической документации на приложение клиента, а также следующую информацию от участника ПлЦР (включая, но не ограничиваясь):

- информацию о создании службы безопасности и контроля, а также об обязанностях и полномочиях службы безопасности и контроля;
- перечень и описание назначения программно-технических средств, применяемых службой безопасности и контроля;
- методические документы по организации контроля за эксплуатацией приложения клиента;
- регламентные документы о порядке взаимодействия службы безопасности и контроля участника ПлЦР с лабораторией.

По итогам рассмотрения 8 Центром ФСБ России результатов исследований лаборатория получает выписку из заключения 8 Центра ФСБ России, содержащую условия соблюдения требований по информационной безопасности при процессе изменения приложения клиента и предоставляет ее заказчику работ – участнику ПлЦР (или внешнему подрядчику участника ПлЦР).

Внесение изменений в эксплуатационную и техническую

[6] В случае планируемой модификации приложения клиента рекомендуется обеспечить раздельную фиксацию контрольных сумм файлов, в которых указана версия приложения клиента, и контрольных сумм других файлов, входящих в состав приложения клиента.

документацию на приложение клиента осуществляется в соответствии с установленными в Российской Федерации правилами внесения изменений в конструкторские и технологические документы.

Дальнейший порядок действий в случае отсутствия необходимости модификации приложения клиента

При отсутствии необходимости модификации приложения клиента служба безопасности и контроля на регулярной основе (не реже 1 раза в месяц) осуществляет сравнение контрольных сумм приложения клиента и криптографических средств с контрольными суммами, указанными в эксплуатационной документации на приложение клиента или зафиксированными лабораторией в соответствии с настоящим Порядком.

В случае отсутствия изменений контрольных сумм приложения клиента и криптографических средств служба безопасности и контроля составляет отчет о результатах проведенного контроля и передает его в лабораторию. В случае изменения контрольных сумм приложения клиента и/или криптографических средств служба безопасности и контроля обязана проинформировать:

- руководство участника ПлЦР для принятия решения о блокировке использования приложения клиента;
- лабораторию, которая не позднее 1 рабочего дня направляет письмо об инциденте в 8 Центр ФСБ России;
- Департамент информационной безопасности Банка России в рамках информирования об инцидентах информационной безопасности.

По решению руководства участника ПлЦР после информирования об инциденте служба безопасности и контроля передает ответственному за эксплуатацию (распространение) приложения клиента подразделению участника ПлЦР копию эталонного образца приложения клиента для дальнейшего распространения.

Распространение (эксплуатация) приложения клиента без предварительной сверки контрольных сумм, а также при неуспешной сверке контрольных сумм, недопустимо.

Дальнейший порядок действий в случае необходимости модификации приложения клиента

При необходимости модификации приложения клиента служба безопасности и контроля до введения модифицированного приложения клиента в эксплуатацию исследует изменения кода приложения клиента. Дополнительно служба безопасности и контроля проводит контроль целостности путем сравнения контрольных сумм исполняемого кода криптографических средств, а также проверяет другие условия обеспечения информационной безопасности, указанные в эксплуатационной и технической документации на приложение клиента.

В случае выявления критических событий, перечень которых зафиксирован в эксплуатационной и технической документации на приложение клиента, служба безопасности и контроля должна сообщить об этом в лабораторию, а участник ПлЦР (или внешний подрядчик участника ПлЦР) должен инициировать работы по проведению Оценки влияния в соответствии с Положением ПКЗ-2005.

В случае отсутствия критических событий, указанных в эксплуатационной и технической документации на приложение клиента, служба безопасности и контроля составляет отчет об изменениях приложения клиента, в котором делает обоснованный вывод об отсутствии влияния изменений приложения клиента на функционирование криптографических средств, фиксирует новые контрольные суммы приложения клиента и до ввода его в эксплуатацию передает в лабораторию отчет об изменениях приложения клиента, исходный код приложения клиента и новые контрольные суммы приложения клиента.

Требования к составу предоставляемых в лабораторию сведений определяется в договоре между участником ПлЦР (или внешним подрядчиком участника ПлЦР) и лабораторией.

Лаборатория обязана регулярно принимать отчеты об изменениях приложения клиента и новые контрольные суммы приложения клиента, проверять выводы службы безопасности и контроля, осуществлять расчет контрольных сумм и передавать свои выводы участнику ПлЦР (или внешнему подрядчику участника ПлЦР) в соответствии со сроками, указанными в договоре.

Эксплуатация приложения клиента возможна после передачи службой безопасности и контроля в лабораторию отчета об изменениях приложения клиента, исходного кода приложения клиента и новых контрольных сумм приложения клиента.

В случае выявления лабораторией несоответствий приложения клиента условиям, определенным настоящим Порядком или эксплуатационной и технической документацией на приложение клиента, она уведомляет участника ПлЦР (или внешнего подрядчика участника ПлЦР), 8 Центр ФСБ России и Департамент информационной безопасности Банка России о выявленном несоответствии.

При получении такого уведомления участник ПлЦР (или внешний подрядчик участника ПлЦР) должен обеспечить использование той версии приложения клиента, на исходные коды которой есть отчетный документ лаборатории о соответствии приложения клиента условиям, определенным в настоящем Порядке. При необходимости допускается обновление номера версии приложения клиента с изменением контрольных сумм файлов, в которых она указана, при неизменности контрольных сумм остального исходного кода приложения клиента. При этом исходный код измененных файлов приложения клиента, а также контрольные суммы этих файлов должны быть переданы в лабораторию.

В случае получения участником ПлЦР (или внешним подрядчиком участника ПлЦР) требования 8 Центра ФСБ России о необходимости выполнения работ по Оценке влияния в соответствии с Положением ПКЗ-2005 участник ПлЦР (или внешний подрядчик участника ПлЦР) должен инициировать выполнение таких работ.

Лаборатория обязана 1 раз в 6 месяцев сообщать аккумулированную информацию в 8 Центр ФСБ России в виде отчетов, содержащих в том числе отметки об изменениях контрольных сумм приложения клиента и/или криптографических средств, а также окружения криптографических средств, зафиксированных в листе изменений эксплуатационной и технической документации.

Приложение 1
к стандарту платформы цифрового рубля
«Порядок проведения работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований»

Согласие финансовой организации об обеспечении информационной безопасности приложения клиента в соответствии со стандартом платформы цифрового рубля «Порядок проведения работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований»

В целях обеспечения информационной безопасности при использовании цифрового рубля, а также обеспечения корректного использования приложения клиента и криптографических средств _____ – участник ПлЦР (далее – участник ПлЦР) принимает
(наименование финансовой организации)
на себя обязательство:

1. Использовать криптографические средства в строгом соответствии с эксплуатационной и технической 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 приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований (далее – Порядок).

4. Заключить договор на проведение работ по оценке влияния приложения клиента, совместно с которым предполагается штатное функционирование криптографических средств, на выполнение предъявленных к ним требований, включающий в себя работы по проведению контроля выводов службы безопасности и контроля, а также предоставление достоверных сведений по указанным работам в 8 Центр ФСБ России в соответствии с настоящим Порядком, с _____, являющейся
(наименование организации)
лабораторией в соответствии с настоящим Порядком.

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

6. Не распространять приложение клиента 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 Департамент информационной безопасности Банка 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 настоящего Порядка.

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

_____/_____
(Подпись) (ФИО)

«____»_____ 20__ г.