Ассоциация банков России
(Ассоциация «Россия»)

ВИЦЕ-ПРЕЗИДЕНТ

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

от 23.10.2023 № 02-05/1150

На №_____от_____

Директору Департамента
информационной безопасности
Банка России

В.А. Уварову

Уважаемый Вадим Александрович!

В Ассоциацию банков России обращаются кредитные организации по вопросам целесообразности совершенствования подходов к периодичности проведения анализа уязвимостей программного обеспечения (ПО) по требованиям к оценочному уровню доверия (далее – ОУД).

Согласно подпункту 4.1 пункта 4 Положения № 683-П[1] и пункту 1.2 Положения № 719-П[2] кредитные организации должны обеспечить использование прикладного ПО автоматизированных систем и приложений, прошедших сертификацию в системе сертификации ФСТЭК России или оценку соответствия по требованиям к ОУД не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013[3].

---

[1] Положение Банка России от 17.04.2013 № 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».

[2] Положение Банка России от 04.06.2020 № 719-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».

[3] Национальный стандарт 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».

Исходя из норм положений указанных нормативных правовых актов, оценка соответствия требованиям по ОУД должна проводиться для каждой конкретной версии ПО и конфигурации информационной системы (ИС) кредитной организации, а обязанность по проведению новой оценки возникает при их обновлении.

По информации кредитных организаций, стоимость услуг по оценке начинается от 1,5 млн рублей, длительность проведения оценки составляет около 10 недель. При этом дополнительно возникает существенная нагрузка на ИТ-подразделения за счет участия в проведении регулярных оценок соответствия и взаимодействия с проверяющей организацией. Отдельными банками отмечается, что для проведения оценки необходим исходный код ПО, который вендоры в ряде случаев отказываются предоставлять, что делает невозможным обращение к независимым оценщикам и проведение оценки банками самостоятельно.

Принимая во внимание, что обновление ПО и ИС происходит на регулярной основе, проведение таких оценок значительно увеличивает трудовые и финансовые затраты кредитных организаций, а также отвлекает сотрудников от исполнения профильных должностных обязанностей по обеспечению информационной безопасности. При этом, несмотря на высокий уровень трудозатрат, документарное сопровождение в соответствии с требованиями регуляторов, по информации ряда кредитных организаций, не оказывает существенного влияния на практическую безопасность ПО, так как требования к документарному сопровождению базируются на устаревших подходах и не учитывают текущие реалии и технологии, используемые в современных производственных процессах. Кроме того, к моменту выхода сертификата соответствия ОУД образец ПО может значительно устареть ввиду применяемых в кредитных организациях гибких методологий разработки и регулярного выпуска релизов.

Вместе с тем кредитные организации вынуждены проводить оценку по ОУД, так как ее отсутствие существенно снижает итоговый результат аудита

кредитной организации по ГОСТ 57580.1-2017[4], что может повлечь за собой применение мер со стороны Банка России.

В целях изучения указанной проблематики и формирования позиции банковского сообщества по данному вопросу Ассоциация провела опрос кредитных организаций. Все участники опроса, в том числе 6 системно значимых кредитных организаций, подтвердили актуальность проблем, связанных с выполнением оценки по ОУД, и необходимость выработки системного решения.

1. 92% участников опроса поддерживают инициативу о переводе проведения оценки по ОУД на **периодическую основу**. 91% из них предлагают установить период проведения оценки по ОУД аналогично периоду проведения оценки соответствия уровню защиты информации по ГОСТ 57580.1-2017, установленный Положением № 683-П – **один раз в два года**, 9% – предлагают период **один раз в год** или предоставить право кредитным организациям устанавливать его самостоятельно. Остальные участники опроса выразили мнение, что даже при переходе на периодическую оценку не будут решены все проблемы, связанные с ее проведением.

2. 54% опрошенных предлагают в качестве дополнительного решения более активно стимулировать применение **процессов и практик безопасного жизненного цикла разработки ПО** с последующим аудитом этих процессов в соответствии с пунктом 7.4 Методического документа Банка России «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» (далее – Профиль защиты). При этом необходимо расширить использование методики Профиля защиты для ПО, применяемого в составе объектов критической информационной инфраструктуры.

Для подтверждения соответствия процесса безопасной разработки требованиям регуляторов, по мнению некоторых кредитных организаций,

---

[4] Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

могут предоставляться следующие подтвержденные, например, лицензиатом ФСТЭК России сведения:

- в организации внедрен процесс безопасной разработки и развертывания ИС;
- принимаются достаточные меры по защите систем, реализующих банковские платежные технологические процессы;
- проводится инструментальный анализ защищенности: сканирование исходного кода, тестирование на проникновение и регулярное (плановое) сканирование уязвимостей;
- по результатам анализа защищенности внедряются компенсационные меры.

Соответствие всем требованиям к процессу безопасной разработки, по мнению кредитных организаций, должно отменять необходимость прохождения оценки по ОУД для ПО.

3. Альтернативно предлагается рассмотреть возможность **комбинации указанных выше предложений**:

- подтверждать на периодической основе (не реже одного раза в два года) соответствия процесса безопасной разработки в организации требованиям Профиля защиты;
- проводить анализ уязвимостей ПО и ИС **только** в случае реализации глобальных («мажорных») обновлений или изменения функций безопасности. При отсутствии таких изменений и обновлений – не реже одного раза в два года.

4. Ряд кредитных организаций предлагает возложить обязанность проведения оценки по ОУД на производителей банковского ПО, так как их компетенции позволят проходить эту оценку более эффективно и в сжатые сроки.

5. Участники опроса также заинтересованы в получении четких методических рекомендаций по проведению оценки по ОУД, содержащие, в частности, условия проведения оценки собственными силами или с

привлечением внешнего подрядчика, сценарии оценки для различных вариантов ИС (коробочные решения вендоров, отдельные модули вендоров, собственная разработка, и любые их сочетания), возможность использования результатов оценки, проведенной вендорами самостоятельно (для системы целиком или отдельных составляющих/модулей) и т.п.

Большинство участников опроса (92%) не видят существенных рисков информационной безопасности при реализации указанных выше предложений, так как многие кредитные организации и банковские вендоры уже успешно внедрили процессы безопасной разработки и имеют опыт производства защищенных продуктов. Кроме того, кредитными организациями реализуется весь комплекс мероприятий по обеспечению информационной безопасности в соответствии с установленными требованиями и стандартами, а также лучшими мировыми практиками анализа защищенности ПО и ИС, которые позволяют обеспечивать высокий уровень защищенности используемых программных решений. Вместе с тем изменение подхода к оценке по ОУД позволит кредитным организациям существенно сократить расходы и нагрузку на ИТ-подразделения.

Просим Вас рассмотреть предложенную кредитными организациями инициативу об изменении порядка проведения оценки по ОУД, а также иные предложения, связанные с выполнением анализа уязвимости ПО и ИС. В случае необходимости выражаем готовность организовать рабочую встречу на площадке Ассоциации с участием Банка России, ФСТЭК России и кредитных организаций для обсуждения указанных предложений.

А.А. Войлуков

Титова О.В., тел. 8-499-678-30-13