



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

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

От 08.07.2020 № ИН-014-56/110
на от

Информационное письмо об анализе
уязвимостей ПО по требованиям к
оценочному уровню доверия (ОУД)

Операторам по переводу денежных
средств

Некредитным финансовым
организациям

Операторам услуг платежной
инфраструктуры

В целях обеспечения единообразной практики применения отдельных положений нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации при осуществлении перевода денежных средств и в целях противодействия осуществлению переводов денежных средств без согласия клиента, а также в целях противодействия осуществлению незаконных финансовых операций, Банк России сообщает следующее.

Кредитные организации обязаны обеспечивать защиту информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента согласно Положению Банка России от 17 апреля 2019 года № 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 № 683-П);

Некредитные финансовые организации обязаны обеспечивать защиту информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций согласно Положению Банка России от 17 апреля 2019 года № 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 № 684-П);

Операторы по переводу денежных средств, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации при осуществлении переводов денежных средств согласно Положению 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» (далее – Положение № 382-П).

В силу подпункта 4.1 пункта 4 Положения № 683-П, пункта 9 Положения № 684-П и подпункта 2.5.5.1 пункта 2.5 Положения № 382-П кредитные организации, некредитные финансовые организации и операторы услуг платежной инфраструктуры должны проводить анализ уязвимостей¹ в отношении указанного в этих нормах прикладного программного обеспечения автоматизированных систем и приложений по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4 (далее – Анализ) в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности.

¹ Положения о проведении анализа уязвимостей по требованиям к оценочному уровню доверия предусмотрены также пунктом 9.5 национального стандарта ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года N 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014).

В целях проведения Анализа рекомендуем применять одобренный подкомитетом № 1 «Безопасность финансовых (банковских) операций» Технического комитета по стандартизации № 122 «Стандарты финансовых операций»² методический документ «Профиль защиты прикладного программного обеспечения и автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций», размещенный на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» в подразделе «Стандарты Банка России» раздела «Информационная безопасность».

Настоящее информационное письмо подлежит размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель Председателя
Банка России

Д.Г. Скобелкин

² Организован в соответствии с приказом Росстандарта от 21.08.2017 № 1759 «Об организации деятельности технического комитета по стандартизации «Стандарты финансовых операций».