



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

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

От 28.06.2023 № 46-4-3/2368

на от

Об использовании алгоритмов шифрования

Личный кабинет

Участникам информационного
взаимодействия

(по списку рассылки)

Департамент управления данными сообщает о ведущейся работе по замене алгоритмов шифрования, используемых в средствах криптографической защиты информации (далее – СКЗИ), применяемых в информационных системах Банка России, на алгоритмы, утвержденные национальными стандартами ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» (далее – ГОСТ Р 34.12-2015) и ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (далее – ГОСТ Р 34.13-2015).

Документы (сведения) в электронной форме, направляемые в адрес Банка России в зашифрованном виде посредством Личного кабинета участника информационного обмена (далее – УИО), при наличии технической возможности должны быть зашифрованы с применением сертифицированных СКЗИ с использованием блочных шифров соответствующих ГОСТ Р 34.12-2015 («Кузнечик» и «Магма»). В то же время, до 01.06.2024 допустимо использование для шифрования указанных документов межгосударственного стандарта СНГ ГОСТ 28147-89 «Системы обработки информации. Защита

криптографическая. Алгоритм криптографического преобразования» (далее – ГОСТ 28147-89).

Документы (сведения) Банка России, направляемые УИО в зашифрованном виде, будут продолжать зашифровываться с использованием ГОСТ 28147-89 до перевода УИО на использование СКЗИ с шифрованием ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Перевод УИО на использование СКЗИ с шифрованием ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 необходимо завершить не позднее 01.06.2024.

С учетом вышеизложенного, а также принимая во внимание извещение Федеральной службы безопасности Российской Федерации от 01.07.2019 о порядке использования алгоритма блочного шифрования ГОСТ 28147-89, УИО необходимо провести проверку используемых СКЗИ и автоматизированных систем УИО (далее – АС) в части возможности их работы с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. В случае отсутствия указанного функционала в используемых СКЗИ или (и) АС, следует приобрести данные СКЗИ или (и) доработать данные АС самостоятельно.

О переходе на использование шифрования по ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 в процессе электронного взаимодействия будет заблаговременно сообщено дополнительными информационными сообщениями.

Первый заместитель директора
Департамента управления данными

А.В. Ахраменов