Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

« » _____ 2021 г. №_____-У

г. Москва

О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

На основании части 14 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2019, № 18, ст. 2214) настоящее Указание определяет перечень угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных.

1. Угрозы безопасности, актуальные при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – информации о степени соответствия), при взаимодействии организаций финансового рынка, указанных в пунктах 5.6, 5.8 статьи 7 Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма») (Собрание законодательства Российской Федерации, 2001, № 33, ст. 3418; 2021, № 1) (далее – Федеральный закон № 115-ФЗ) с единой биометрической системой для проведения или создания условий для совершения операций (сделок) без согласия клиента – физического лица, представителя клиента – юридического лица, имеющего право без доверенности действовать от имени юридического лица и являющегося физическим лицом (далее – клиент), совершения действий без личного присутствия клиента, а также операций (сделок) не уполномоченным лицом, в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма при:

размещении или обновлении биометрических персональных данных, в единой биометрической системе, банками с универсальной лицензией, банками с базовой лицензией, соответствующими критериям, установленным абзацами вторым – четвертым пункта 5.7 статьи 7 Федерального закона № 115-ФЗ (далее – банки с универсальной лицензией, банки с базовой лицензией);

идентификации клиентов с использованием единой биометрической системы, при приеме на обслуживание клиентов для совершения операций (сделок) организациями финансового рынка, указанными в пункте 5.8 статьи 7 Федерального закона № 115-ФЗ;

проверке соответствия биометрических персональных данных лица, содержащихся в единой биометрической системе, в случае возникновения подозрения у организаций финансового рынка, указанных в пункте 5.8 статьи 7 Федерального закона № 115-ФЗ;

открытии и ведении счета (вклада) клиентов и выдача кредита клиентам, банками с универсальной лицензией:

1.1. при размещении или обновлении биометрических персональных данных в банках с универсальной лицензией, банках с базовой лицензией, при проведении действия, указанного в абзаце 2 пункта 1 настоящего Указания:

1.1.1. при сборе биометрических персональных данных в филиалах или внутренних структурных подразделениях банков с универсальной лицензией, банков с базовой лицензией, с использованием стационарных средств вычислительной техники, и передаче собранных биометрических персональных данных между структурными подразделениями организаций финансового рынка, – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378, зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620 (далее - приказ ФСБ России № 378) (в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации не ниже четвертого класса) и в пункте 12 приложения к приказу ФСБ России № 378 (в случае неприменения средств (систем) защиты информации от

несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации не ниже четвертого класса);

1.1.2. при сборе биометрических персональных данных работниками банков с универсальной лицензией, банков с базовой лицензией, с использованием мобильных (переносных) устройств вычислительной техники (планшетов), и передаче собранных биометрических персональных данных между переносным средством вычислительной техники и информационной инфраструктурой структурных подразделений банков с универсальной лицензией, банков с базовой лицензией, – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378 (в случае применения мер защиты информации определенных в разделе 7.9 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 7580.1-2017) и в пункте 11 приложения к приказу ФСБ России № 378 (в случае неприменения мер защиты информации определенных в разделе 7.9 ГОСТ Р 57580.1-2017);

1.2. при передаче собранных биометрических персональных данных между банками с универсальной лицензией, банками с базовой лицензией и единой биометрической системой, при проведении действия, указанного в абзаце 2 пункта 1 настоящего Указания:

1.2.1. угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378;

1.2.2. угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

1.3. при обработке биометрических персональных данных и информации о степени соответствия, на устройстве клиента, при проведении действий, указанных в абзацах 3 – 5 пункта 1 настоящего Указания – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения целостности (подмены, удаления) информации о степени соответствия, и передаче информации о степени соответствия в организации финансового рынка, установленными пунктом 5.8-1 статьи 7 Федерального закона года № 115-ФЗ, при проведении действий, указанных в абзацах 3 – 5 пункта 1 настоящего Указания, или в единой биометрической системе, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378;

1.4. при обработке информации о степени соответствия, в организациях финансового рынка, указанных в пунктах 5.6, 5.8 статьи 7 Федерального закона № 115-ФЗ, при проведении действий, указанных в абзацах 2 – 5 пункта 1 настоящего Указания:

1.4.1. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, в организациях финансового рынка, указанных в пунктах 5.6, 5.8 статьи 7 Федерального закона № 115-ФЗ, реализующих усиленный и стандартный уровни защиты информации в соответствии с нормативными актами

Банка России, устанавливающими обязательные требования по защите информации для кредитных и некредитных финансовых организаций, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378;

1.4.2. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, в организациях финансового рынка, не подпадающих под критерии, установленные для организаций финансового рынка, указанных в подпункте 1.4.1 пункта 1.4 настоящего Указания, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

1.5. при передаче информации о степени соответствия между организациями финансового рынка, указанных в пунктах 5.6, 5.8 статьи 7 Федерального закона № 115-ФЗ и единой биометрической системой:

1.5.1. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, при передаче указанной информации между организациями финансового рынка, указанными в подпункте 1.4.1 пункта 1.4 настоящего Указания, и единой биометрической системой, том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378;

1.5.2. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, при передаче указанной информации между организациями финансового рынка, указанными в подпункте 1.5.1 пункта 1.5 настоящего Указания, и единой биометрической системой, том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

1.5.3. угроза нарушения конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378.

2. Угрозы безопасности, актуальные при обработке биометрических персональных данных и передаче информации о степени соответствия, при взаимодействии организаций финансового рынка, с единой биометрической системой для проведения или создания условий для совершения операций (сделок) без согласия клиента или без подтверждения волеизъявления, совершения действий без личного присутствия клиента, а также операций (сделок) не уполномоченным лицом, при:

идентификации физического лица, в соответствии с пунктом 18 статьи 14.1 Федерального закона № 149-ФЗ;

аутентификации физического лица, в соответствии с пунктом 18.2 статьи 14.1 Федерального закона № 149-ФЗ:

2.1. при обработке биометрических персональных данных и информации о степени соответствия, на устройстве клиента – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения целостности (подмены, удаления) информации о степени соответствия, и передаче информации о степени соответствия в организации финансового рынка, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378;

2.2. при обработке биометрических персональных данных и информации о степени соответствия, в организациях финансового рынка, при проведении действий, указанных в абзацах 2 – 3 пункта 2 настоящего Указания:

2.2.1. угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, в организациях финансового рынка, реализующих усиленный и стандартный уровни защиты информации в соответствии с нормативными актами Банка России, устанавливающими обязательные требования по защите информации для кредитных и некредитных финансовых организаций, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте

13 приложения к приказу ФСБ России № 378;

2.2.2. угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, в организациях финансового рынка, не подпадающих под критерии, установленные для организаций финансового рынка, указанных в подпункте 1.4.1 пункта 1.4 настоящего Указания, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

2.3. при передаче информации о степени соответствия между организациями финансового рынка, указанных в пунктах 5.6, 5.8 статьи 7 Федерального закона № 115-ФЗ и единой биометрической системой:

2.3.1. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, при передаче указанной информации между организациями финансового рынка, указанными в подпункте 1.4.1 пункта 1.4 настоящего Указания, и единой биометрической системой, том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378;

2.3.2. угроза нарушения целостности (подмены, удаления) информации о степени соответствия, при передаче указанной информации между организациями финансового рынка, указанными в подпункте 1.4.1 пункта 1.4 настоящего Указания, и единой биометрической системой, том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

2.3.3. угроза нарушения конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378.

3. Настоящее Указание в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от «___»

_____2021 года № ПСД-____) вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлен иной срок вступления их в силу.

Абзац 5 пункта 1, пункты 1.1.2, 1.3, 2 настоящего Указания вступают в силу с 1 января 2022 года.

Со дня вступления в силу настоящего Указания признать утратившим силу Указание Банка России от 9 июля 2018 года № 4859-У «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе», зарегистрированное Министерством юстиции Российской Федерации 30 июля 2016 года № 51735.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации
_____ А.В. Бортников
_____ 2021 г.

Директор
Федеральной службы по техническому
и экспортному контролю
_____ В.В. Селин
_____ 2021 г.

Министр цифрового развития, связи и
массовых коммуникаций Российской
Федерации
_____М.И. Шадаев
_____2021 г.

Президент ПАО «Ростелеком»
_____ М.Э. Осеевский
_____ 2021 г.