

**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 при:

размещении или обновлении биометрических персональных данных в единой биометрической системе (далее – сбор биометрических персональных данных) банками с универсальной лицензией, банками с базовой лицензией, указанными в пункте 5.6 статьи 7 Федерального закона № 115-ФЗ (далее – банки);

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.

1.1. При сборе биометрических персональных данных в банках:

1.1.1. при сборе биометрических персональных данных в филиалах или внутренних структурных подразделениях банков с использованием стационарных средств вычислительной техники и передаче собранных биометрических персональных данных между структурными подразделениями банков – 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 использованием мобильных (переносных) устройств вычислительной техники (планшетов) и передаче собранных биометрических персональных данных между переносным средством вычислительной техники и информационной инфраструктурой структурных подразделений банков – 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 программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации) и в пункте 11 приложения к приказу ФСБ России № 378 (в случае неприменения программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации);

1.1.3. при сборе биометрических персональных данных банками с использованием платежных терминалов, банкоматов и передаче собранных биометрических персональных данных между платежным терминалом, банкоматом и информационной инфраструктурой структурных подразделений банков – 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 программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации) и в пункте 11 приложения к приказу ФСБ России № 378 (в случае неприменения программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации).

1.2. При передаче собранных биометрических персональных данных между банками и единой биометрической системой:

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, полученных с устройства клиента - физического лица при проведении действий, указанных в абзацах третьем и четвертом пункта 1 настоящего Указания – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, 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 пункте 5.8 статьи 7 Федерального закона № 115-ФЗ, при проведении действий, указанных в абзацах третьем и четвертом пункта 1 настоящего Указания – угроза нарушения целостности (подмены, удаления) информации о степени соответствия в организациях финансового рынка, указанных в пункте 5.8 статьи 7 Федерального закона № 115-ФЗ, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378.

1.5. При передаче информации о степени соответствия между организациями финансового рынка, указанными в пункте 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 и единой биометрической системой, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 приложения к приказу ФСБ России № 378;

1.5.2. 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 в соответствии с пунктами первым и вторым части 18.6 статьи 14.1 Федерального закона № 149-ФЗ:

2.1. при обработке биометрических персональных данных, полученных с устройства клиента - физического лица – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378;

2.2. при обработке информации о степени соответствия в организациях финансового рынка – угроза нарушения целостности (подмены, удаления) информации о степени соответствия в организациях финансового рынка, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

2.3. при обработке биометрических персональных данных и информации о степени соответствия организациями финансового рынка с использованием мобильных (переносных) устройств вычислительной техники (планшетов), платежных терминалов, банкоматов – угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, 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 программных средств (систем) защиты информации, реализующих

доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации) и в пункте 11 приложения к приказу ФСБ России № 378 (в случае неприменения программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации).

2.4. При передаче информации о степени соответствия между организациями финансового рынка и единой биометрической системой – угроза нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия при ее передаче между организациями финансового рынка и единой биометрической системой, том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378.

3. Настоящее Указание вступает в силу со дня вступления в силу нормативного правового акта федерального органа исполнительной власти, осуществляющего регулирование в сфере идентификации физических лиц на основе биометрических персональных данных, устанавливающего перечень угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с единой биометрической системой, устанавливаемого на основании пункта 4 части 13 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Со дня вступления в силу нормативного правового акта, указанного в абзаце первом настоящего пункта, 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.