ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

«16» декабря 2021 г. № 6018-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 66716
от "30" декабря 2021 г.

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 в информационных системах организаций финансового рынка, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами

Настоящее Указание на основании части 14^1 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; 2018, № 1, ст. 66; 2021, № 1, ст. 18) 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 в информационных системах организаций финансового рынка, указанных в части 10 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; 2018, № 1, ст. 66; 2021, № 1, ст. 18) и осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (единой биометрической системы), а также актуальных при взаимодействии организаций финансового рынка, указанных в части 10 статьи 14^1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иных организаций, индивидуальных предпринимателей с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и вида аккредитации организации из числа организаций, указанных в частях 18^{28} и 18^{31} 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; 2018, № 1, ст. 66; 2021, № 1, ст. 18).

1. Угрозы нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных при автоматизированной обработке биометрических персональных данных на устройстве клиента – физического лица в целях идентификации и (или) аутентификации физического лица в случае выполнения условий, установленных в частях 18^{18} и 18^{20} 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; 2018, № 1, ст. 66; 2021, № 1, ст. 18) (далее – Федеральный закон № 149-ФЗ), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 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 – Состав и содержание организационных и технических мер).

2. Угрозы безопасности, актуальные при сборе биометрических персональных данных, их передаче в осуществляющие идентификацию и

(или) аутентификацию с использованием биометрических персональных данных физических лиц информационные системы (далее – информационные системы) организаций финансового рынка, указанных в части 10 статьи 14^1 Федерального закона № 149-ФЗ (далее – организации финансового рынка), в целях идентификации и (или) аутентификации физического лица в случае выполнения условий, установленных в частях 18^{18} и 18^{20} статьи 14^1 Федерального закона № 149-ФЗ:

2.1 в головном офисе, филиалах или внутренних структурных подразделениях организаций финансового рынка с использованием стационарных средств вычислительной техники и при передаче собранных биометрических персональных данных между головным офисом, филиалами или внутренними структурными подразделениями организаций финансового рынка:

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 11 Состава и содержания организационных и технических мер (в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4 уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными

приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76, зарегистрированным Министерством юстиции Российской Федерации 11 сентября 2020 года № 59772 (далее – Требования по безопасности информации, устанавливающие уровни доверия), и в пункте 12 Состава и содержания организационных и технических мер (в случае неприменения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4 уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия);

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер;

2.2. работниками организаций финансового рынка с использованием мобильных (переносных) устройств вычислительной техники (планшетов) и при передаче собранных биометрических персональных данных между мобильными (переносными) средствами вычислительной техники и информационной инфраструктурой структурных подразделений 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 10 Состава и содержания организационных и технических мер (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 Состава и содержания организационных и технических мер (в случае неприменения программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации);

2.3. работниками организаций финансового рынка с использованием платежных терминалов, банкоматов и при передаче собранных биометрических персональных данных между платежными терминалами, банкоматами и информационной инфраструктурой структурных подразделений 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.

3. Угрозы безопасности, актуальные при обработке (за исключением сбора), в том числе хранении, биометрических персональных данных и

информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – информация о степени соответствия) в информационной системе организации финансового рынка в целях аутентификации физического лица в случае выполнения условий, установленных частью 18^{18} статьи 14^{1} Федерального закона № 149-ФЗ:

угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер;

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

4. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, нарушения конфиденциальности (компрометации) биометрических персональных данных при обработке (за исключением сбора), в том числе хранении, биометрических персональных данных и информации о степени соответствия в информационной системе организации финансового рынка в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем реализации целенаправленных действий с

использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

5. Угрозы безопасности, актуальные при передаче биометрических персональных данных и информации о степени их соответствия в информационную систему организации финансового рынка в целях аутентификации и (или) идентификации физического лица в случае выполнения условий, установленных частями 18^{18} и 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ:

5.1. с использованием стационарных средств вычислительной техники, принадлежащих организации финансового рынка:

угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, 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 (в случае применения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4 уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия), и в пункте 12 Состава и содержания организационных и технических мер (в случае неприменения средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации не ниже 4 уровня доверия в соответствии с

Требованиями по безопасности информации, устанавливающими уровни доверия);

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер;

5.2. с использованием мобильных (переносных) устройств вычислительной техники (планшетов), принадлежащих организации финансового рынка, – 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 Состава и содержания организационных и технических мер (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 Состава и содержания организационных и технических мер (в случае неприменения программных средств (систем) защиты информации, реализующих доверенную загрузку, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации);

5.3. с использованием платежных терминалов, банкоматов, принадлежащих организации финансового рынка, – 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 11 Состава и содержания организационных и технических мер.

6. Угроза безопасности, актуальная при взаимодействии организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка в целях аутентификации физического лица в соответствии с частью 18^{24} статьи 14^{1} Федерального закона № 149-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2018, № 1, ст. 66; 2021, № 1, ст. 18), – угроза нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

7. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол

заседания Совета директоров Банка России от 11 июня 2021 года № ПСД-12) вступает в силу с 1 января 2022 года.

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.