ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

«16» декабря 2021 г. № 6017-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

Настоящее Указание 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; 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, 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» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2018, № 1, ст. 66; 2021, № 1, ст. 18), с единой информационной системой 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, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных.

1. Угрозы безопасности, актуальные при сборе биометрических персональных данных и их передаче в целях размещения или обновления биометрических персональных данных в единой информационной системе 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, указанной в статье 14^1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее соответственно – единая биометрическая система, информация о степени соответствия, Федеральный закон № 149-ФЗ):

1.1. В головном офисе, филиалах или внутренних структурных подразделениях организаций финансового рынка, указанных в части 10 статьи 14^1 Федерального закона № 149-ФЗ (далее – организации финансового рынка), являющихся банками с универсальной лицензией, банками с базовой лицензией, указанными в пункте 5^6 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; 2018, № 1, ст. 66; 2021, № 1, ст. 18) (далее соответственно – банки, Федеральный закон № 115-ФЗ), с использованием стационарных средств вычислительной техники и

при передаче собранных биометрических персональных данных между головным офисом, филиалами или внутренними 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 – Состав и содержание 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);

1.2. Работниками банков с использованием мобильных (переносных) устройств вычислительной техники (планшетов) и при передаче собранных биометрических персональных данных между мобильными (переносными) средствами вычислительной техники (планшетами) 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 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);

1.3. Работниками банков с использованием платежных терминалов, банкоматов и при передаче собранных биометрических персональных данных между платежными терминалами, банкоматами 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 11 Состава и содержания организационных и технических мер.

2. Угрозы безопасности, актуальные при взаимодействии банков с единой биометрической системой в целях размещения или обновления биометрических персональных данных в единой биометрической системе:

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 Состава и содержания организационных и технических мер;

2.2. 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.

3. Угрозы безопасности, актуальные при обработке (за исключением сбора) биометрических персональных данных, их проверке и передаче информации о степени соответствия, при взаимодействии организаций финансового рынка, являющихся организациями, указанными в пункте 5^8 статьи 7 Федерального закона № 115-ФЗ (Собрание законодательства Российской Федерации, 2001, № 33, ст. 3418; 2018, № 1, ст. 66; 2021, № 27, ст. 5094), с единой биометрической системой в целях идентификации клиента – физического лица, представителя клиента – юридического лица, имеющего право без доверенности действовать от имени юридического лица

и являющегося физическим лицом, с использованием единой биометрической системы, а также в целях проверки соответствия биометрических персональных данных лица, уполномоченного распоряжаться денежными средствами, находящимися на банковском счете клиента – юридического лица, его биометрическим персональным данным, содержащимся в единой биометрической системе, в случае возникновения подозрения у кредитной организации, предусмотренного абзацем десятым пункта 5^8 статьи 7 Федерального закона № 115-ФЗ:

3.1. При автоматизированной обработке биометрических персональных данных на устройстве 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 Состава и содержания организационных и технических мер;

3.2. При обработке информации о степени соответствия в организациях финансового рынка, являющихся организациями, указанными в пункте 5^8 статьи 7 Федерального закона № 115-ФЗ:

угроза нарушения целостности (подмены, удаления) 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) 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;

3.3. При передаче информации о степени соответствия между организациями финансового рынка, являющимися организациями,

указанными в пункте 5^8 статьи 7 Федерального закона № 115-ФЗ, и единой биометрической системой:

угроза нарушения целостности (подмены, удаления) 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) 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.

4. Угрозы безопасности, актуальные при обработке (за исключением сбора) биометрических персональных данных, их проверке и передаче информации о степени соответствия, при взаимодействии организаций финансового рынка с единой биометрической системой в целях аутентификации физического лица в соответствии с частью 18^2 статьи 14^1 Федерального закона № 149-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2018, № 1, ст. 66; 2021, № 1, ст. 18):

4.1. При автоматизированной обработке биометрических персональных данных на устройстве 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 Состава и содержания организационных и технических мер;

4.2. При обработке информации о степени соответствия в организациях финансового рынка – 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;

4.3. При обработке биометрических персональных данных и информации о степени соответствия организациями финансового рынка с использованием мобильных (переносных) устройств вычислительной техники (планшетов) – 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);

4.4. При обработке биометрических персональных данных и информации о степени соответствия организациями финансового рынка с использованием 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 11 Состава и содержания организационных и технических мер;

4.5. 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, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

5. Угроза безопасности, актуальная при взаимодействии организаций финансового рынка с единой биометрической системой при передаче собранных биометрических персональных данных между осуществляющими обработку биометрических персональных данных информационными системами организаций финансового рынка и единой биометрической системой в случае, указанном в части 18^{23} статьи 14^{1} Федерального закона № 149-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2018, № 1, ст. 66; 2021, № 27, ст. 5094), – угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

6. 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.[1]

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.

[1] Но не ранее вступления в силу совместного нормативного акта Банка России и Публичного акционерного общества «Ростелеком» о признании утратившим силу Указания Банка России и Публичного акционерного общества «Ростелеком» от 9 июля 2018 года № 4859-У/01/01/782-18 (протокол заседания Совета директоров Банка России от 20 января 2022 года № ПСД-1).