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 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, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

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; 2021, № 1) 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 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, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных.

1. Угрозы безопасности, актуальные при сборе и обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – информации о степени соответствия) в информационных системах организаций финансового рынка, установленных частью 10 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) (далее – организации финансового рынка) 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) или без подтверждения волеизъявления клиента, совершения действий без личного присутствия клиента, а также операций (сделок) не уполномоченным лицом, в целях единственного фактора аутентификации при:

идентификации и (или) аутентификации физического клиента, в соответствии с пунктом 18.17 статьи 14.1 Федерального закона № 149-ФЗ;

аутентификации физического лица, в соответствии с пунктом 18.24 статьи 14.1 Федерального закона № 149-ФЗ:

1.1. при сборе и 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, при проведении действий, указанных в абзацах 2 – 3 пункта 1 настоящего Указания, 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 - приказ ФСБ России № 378);

1.2. при сборе и обработке биометрических персональных данных в организациях финансового рынка, при проведении действий, указанных в абзацах 2 – 3 пункта 1 настоящего Указания:

1.2.1. при сборе биометрических персональных данных в филиалах или внутренних структурных организаций финансового рынка 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 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;

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 приложения к приказу ФСБ России № 378;

1.2.2. при сборе биометрических персональных данных работниками организаций финансового рынка с использованием мобильных (переносных) устройств вычислительной техники (планшетов), и передаче собранных биометрических персональных данных между переносным средством вычислительной техники и структурными подразделениями организации 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 приложения к приказу ФСБ России № 378;

1.2.3. при сборе биометрических персональных данных организациями финансового рынка с использованием платежных терминалов, и передаче собранных биометрических персональных данных между платежным терминалом и структурными подразделениями организации 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 приложения к приказу ФСБ России;

1.3. при обработке биометрических персональных данных и информации о степени соответствия, при проведении действий, указанных в абзацах 2 – 3 пункта 1 настоящего Указания, в информационной системе организации финансового

рынка:

1.3.1. угроза нарушения целостности (подмены, удаления) 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;

1.3.2. 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 1.3.1 пункта 1.3 настоящего Указания, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 приложения к приказу ФСБ России № 378;

1.4. при передаче биометрических персональных данных при взаимодействии организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка:

1.4.1. 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;

1.4.2. 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;

1.4.3. 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.

2. Угрозы безопасности, актуальные при сборе и обработке биометрических персональных данных в информационных системах организаций финансового рынка для проведения или создания условий для совершения операций (сделок) без согласия клиента или без подтверждения волеизъявления клиента, совершения действий без личного присутствия клиента, а также операций (сделок) не уполномоченным лицом, в целях дополнительного фактора аутентификации при:

идентификации и (или) аутентификации клиента, в соответствии с пунктом 18.17 статьи 14.1 Федерального закона № 149-ФЗ,

аутентификации физического лица, в соответствии с пунктом 18.24 статьи 14.1 Федерального закона № 149-ФЗ:

2.1. при сборе и обработке биометрических персональных данных 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, при проведении действий, указанных в абзацах 2 – 3 пункта 2 настоящего Указания;

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

2.2.1. при сборе биометрических персональных данных в филиалах или внутренних структурных организаций финансового рынка 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 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;

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 приложения к приказу ФСБ России № 378;

2.2.2. при сборе биометрических персональных данных работниками организаций финансового рынка с использованием переносных средств вычислительной техники (планшетов), и передаче собранных биометрических персональных данных между переносным средством вычислительной техники и структурными подразделениями организации 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 приложения к приказу ФСБ России № 378;

2.2.3. при сборе биометрических персональных данных организациями финансового рынка с использованием платежных терминалов, и передаче собранных биометрических персональных данных между платежным терминалом и структурными подразделениями организации 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 приложения к приказу ФСБ России № 378;

2.2.4. при обработке биометрических персональных данных и информации о степени соответствия в информационной системе организации 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), нарушения целостности (подмены, удаления) и конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378;

2.3. при передаче биометрических персональных данных при взаимодействии организаций финансового рынка, иных организаций, индивидуальных предпринимателей с информационными системами 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), нарушения целостности (подмены, удаления) и конфиденциальности (компрометации) информации о степени соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 приложения к приказу ФСБ России № 378.

3. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от «__» _____ 2021 года № ПСД-___) вступает в силу с 01 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.