МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

ПРИКАЗ

05.05.2023 № 446

Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 73487
от "26" мая 2023 г.

Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

В соответствии с пунктом 6 части 2 статьи 6 Федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», подпунктом 5.2.67 пункта 5 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418,

ПРИКАЗЫВАЮ:

1. Утвердить по согласованию с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и акционерным обществом «Центр Биометрических Технологий» перечень угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных.

2. Признать утратившим силу приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 1 сентября 2021 г. № 902 «Об утверждении перечня 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, 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, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и учетом 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» (зарегистрирован Министерством юстиции Российской Федерации 3 ноября 2021 г., регистрационный № 65692).

3. Настоящий приказ вступает в силу по истечении десяти дней со дня его официального опубликования и действует до 1 июня 2029 г.

Врио Министра Д.М. Ким

УТВЕРЖДЕН
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 05. 05 .2023 № 446

ПЕРЕЧЕНЬ
угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

1. Угрозы безопасности, актуальные при обработке и передаче биометрических персональных данных в целях аутентификации физического лица:

1.1. При автоматизированной обработке биометрических персональных данных на устройстве 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 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 г. № 378 (зарегистрирован Министерством юстиции Российской Федерации 18 августа 2014 г., регистрационный № 33620) (далее – Состав и содержание организационных и технических мер).

1.2. При обработке государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными

предпринимателями, нотариусами с использованием мобильных (переносных) устройств вычислительной техники (за исключением планшетов) – 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.

1.3. При обработке государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами с использованием планшетов – 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 средств (систем) защиты информации от несанкционированного доступа, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации не ниже четвертого уровня доверия в соответствии с Требованиями, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 г. № 76 (зарегистрирован Министерством юстиции Российской Федерации 11 сентября 2020 г., регистрационный № 59772), или с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер.

1.4. При обработке государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами с использованием оконечных устройств информационных систем, обеспечивающих функционирование контрольно-пропускных пунктов, – 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.

1.5. При обработке государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами с использованием стационарных средств вычислительной техники – 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. Угроза нарушения целостности (подмены, удаления), угроза нарушения конфиденциальности (компрометации) при приеме векторов единой биометрической системы, угроза нарушения целостности (подмены, удаления) при хранении векторов единой биометрической системы в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

3. Угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации) биометрических персональных данных, информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица (далее – информация о степени соответствия) при передаче и обработке в информационной системе организации, осуществляющей аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, в целях аутентификации физического лица, 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, в том числе хранении, предоставленных в соответствии с пунктом 3 части 1 статьи 15 Федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» биометрических персональных данных в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка:

4.1. 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 12 Состава и содержания организационных и технических мер.

4.2. Угроза несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным, в том числе при установке, настройке программных и программно-аппаратных средств.

5. Угрозы нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия при обработке и передаче информации о степени соответствия при взаимодействии государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с информационными системами организаций, осуществляющих аутентификацию на

основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, в целях аутентификации физического лица, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

6. Угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации) персональных данных при предоставлении государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами в федеральную государственную информационную систему «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» сведений о физических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов соответственно, включая идентификаторы таких сведений, перед использованием информационной системы организации, осуществляющей аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, для аутентификации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.