

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 единой биометрической системе, 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 единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

Приказ · № 445 · от 05.05.2023 · Министерство цифрового развития, связи и массовых коммуникаций · Действует без изменений

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

МОСКВА

5 мая 2023 г. № 445

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 единой биометрической системе, 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 единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

Зарегистрирован Минюстом России 26 мая 2023 г.

Регистрационный № 73486

В соответствии с пунктом 4 части 2 статьи 6 и пунктом 2 части 4 статьи 14 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 5.2.66 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, Центральным банком Российской Федерации 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 единой биометрической системе, 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 единой биометрической системой, 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 25 мая 2021 г. № 494 "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 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, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных" (зарегистрирован Министерством юстиции Российской Федерации 15 сентября 2021 г., регистрационный № 65009).

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 5 мая 2023 г. № 445

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 единой биометрической системе, 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 единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных

1. Угрозы безопасности, актуальные при обработке, включая сбор, биометрических персональных данных в многофункциональных центрах предоставления государственных и муниципальных услуг для передачи в единую биометрическую систему в целях размещения биометрических персональных данных в единой биометрической системе:

1.1. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных,

нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных) при обработке, включая сбор, биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состав 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. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных) при передаче собранных биометрических персональных данных между многофункциональными центрами предоставления государственных и муниципальных услуг и единой биометрической системой, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состав и содержания организационных и технических мер.

1.3. Угроза нарушения конфиденциальности (компрометации) биометрических персональных данных при передаче собранных биометрических персональных данных между многофункциональными центрами предоставления государственных и муниципальных услуг и единой биометрической системой, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состав и содержания организационных и технических мер.

2. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных, угроза нарушения конфиденциальности (компрометации) биометрических персональных данных при обработке, включая сбор, биометрических персональных данных на пользовательском оборудовании (оконечном оборудовании), имеющем в своем составе идентификационный модуль, физического лица (далее - пользовательское оборудование физического лица), и передаче биометрических персональных данных с пользовательского оборудования физического лица с использованием мобильного приложения единой биометрической системы в единую биометрическую систему, путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 Состав и содержания организационных и технических мер.

3. Угрозы безопасности, актуальные при обработке и передаче биометрических персональных данных в единую биометрическую систему в целях идентификации и (или) аутентификации, при обработке и передаче биометрических персональных данных в информационные системы аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации в целях аутентификации:

3.1. При обработке с использованием устройства 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 Состав и содержания организационных и технических мер.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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.

4. Угроза нарушения целостности (подмены, удаления) информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица (далее - информация о степени соответствия) при передаче информации о степени соответствия из единой биометрической системы в процессе идентификации и (или) аутентификации физического лица, векторов единой биометрической системы при передаче векторов единой биометрической системы, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

5. Угроза нарушения конфиденциальности (компрометации) информации о степени соответствия при передаче информации о степени соответствия из единой биометрической системы в процессе идентификации и (или) аутентификации физического лица, векторов единой биометрической

системы при передаче векторов единой биометрической системы, 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) информации о степени соответствия при обработке информации о степени соответствия государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

7. 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" ¹ (далее - единая система идентификации и аутентификации) 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 единой биометрической системы для аутентификации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

1 Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

8. 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) информации о степени соответствия, нарушения доступности (блокирования передачи) информации о степени соответствия при обработке, хранении, проверке биометрических персональных данных, передаче и обработке информации о степени соответствия в единой биометрической системе и при взаимодействии единой биометрической системы с единой системой идентификации и аутентификации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

9. Угроза нарушения целостности (подмены, удаления) при обработке в процессе размещения государственными органами, органами местного самоуправления, Центральным банком Российской Федерации, организациями, за исключением организаций финансового рынка, индивидуальными предпринимателями, нотариусами биометрических персональных данных в единой биометрической системе в соответствии с частью 14 статьи 4 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" (далее - импорт биометрических персональных данных, Федеральный закон № 572-ФЗ соответственно), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

10. Угроза нарушения конфиденциальности (компрометации) при обработке в процессе импорта биометрических персональных данных в единую биометрическую систему, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

11. Угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации) биометрических персональных данных при предоставлении в единую биометрическую систему биометрических персональных данных в процессе идентификации и (или) аутентификации, в иных случаях обработки биометрических персональных данных, предусмотренных Федеральным законом № 572-ФЗ, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

12. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных при передаче оператору единой биометрической системы в соответствии с пунктом 9 части 2 статьи 8, частью 11 статьи 14, частью 3 статьи 15 Федерального закона № 572-ФЗ мотивированного запроса о предоставлении информации о результатах проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, основанного на обращении субъекта персональных данных, предполагающего неправомерную обработку его биометрических персональных данных при проведении аутентификации и (или) оспаривающего результаты проведения аутентификации (далее - информация о результате проверки соответствия), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

13. Угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации) информации о результате проверки соответствия при передаче оператором единой биометрической системы в соответствии с пунктом 9 части 2 статьи 8, частью 11 статьи 14, частью 3 статьи 15 Федерального закона № 572-ФЗ информации о результате проверки соответствия, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

14. 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 аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

15. Угроза нарушения целостности (подмены, удаления), нарушения конфиденциальности (компрометации) биометрических персональных данных, информации о степени соответствия при передаче и обработке в информационной системе аккредитованного государственного органа, Центрального банка Российской Федерации в случае прохождения им аккредитации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

16. Угрозы безопасности, актуальные при обработке, в том числе хранении, предоставленных в

соответствии с частью 7 статьи 14 Федерального закона № 572-ФЗ биометрических персональных данных, в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации:

16.1. 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 Состав и содержания организационных и технических мер.

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

17. 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, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с информационными системами аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состав и содержания организационных и технических мер.