МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

25.05.2021 № 494

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 65009
от "15" сентября 2021 г.

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

В соответствии с пунктом 4 части 13 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2021, № 11, ст. 1708), абзацем шестым пункта 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708; 2021, № 21, ст. 3582),

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый 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 единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение

биометрических персональных данных, их проверку и передачу информации о степени их соответствия представленным 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.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Министр М.И. Шадаев

УТВЕРЖДЕН
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.05 2021 г. № 494

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 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

1. Угрозы безопасности, актуальные при обработке, включая сбор биометрических персональных данных в государственных органах, органах местного самоуправления и организациях, за исключением организаций финансового рынка, для передачи в единую информационную систему персональных данных, обеспечивающую обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – единая биометрическая система):

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 и передаче собранных биометрических персональных данных между структурными подразделениями государственного органа, органа местного самоуправления и организаций, за исключением организаций финансового рынка (далее – обработка и передача биометрических персональных данных между структурными подразделениями), в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 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, приказ ФСБ России № 378);

1.2. 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 и передаче биометрических персональных данных между структурными подразделениями, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378, 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 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 г. № 76 (зарегистрирован Министерством юстиции Российской Федерации 11 сентября 2020 г., регистрационный № 59772);

1.3. 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 государственными органами, органами местного самоуправления, индивидуальными предпринимателями, нотариусами и организациями, за исключением организаций финансового рынка, и единой биометрической системой, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378;

1.4. угроза нарушения конфиденциальности (компрометации) биометрических персональных данных при передаче собранных биометрических персональных данных между государственными органами, органами местного самоуправления, индивидуальными предпринимателями, нотариусами и организациями, за исключением организаций финансового рынка, и единой биометрической системой, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378.

2. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных, угроза нарушения конфиденциальности (компрометации) биометрических персональных данных при обработке биометрических персональных данных, сведений о степени их соответствия предоставленным

биометрическим персональным данным физического лица (далее – степень соответствия) на пользовательском оборудовании (оконечном оборудовании), имеющем в своем составе идентификационный модуль физического лица (далее – устройство физического лица) и передаче биометрических персональных данных с устройства физического лица в единую биометрическую систему, путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 10 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378.

3. Угроза нарушения целостности (подмены, удаления) информации о степени соответствия при передаче информации о степени соответствия, включая персональные данные, между государственными органами, органами местного самоуправления, индивидуальными предпринимателями, нотариусами и организациями, за исключением организаций финансового рынка, и единой биометрической системой (далее – передача информации о степени соответствия) в процессе идентификации физического лица, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378.

4. Угроза нарушения конфиденциальности (компрометации) информации о степени соответствия при передаче информации о степени соответствия в процессе идентификации физического лица, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378.

5. Угроза нарушения целостности (подмены, удаления) информации о степени соответствия при обработке информации о степени соответствия, включая персональные данные, в государственных органах, органах местного самоуправления, индивидуальными предпринимателями, нотариусами и организациями, за исключением организаций финансового рынка, в том числе при передаче информации о степени соответствия государственными органами, органами местного самоуправления, индивидуальными предпринимателями, нотариусами и организациями, за исключением организаций финансового рынка, в единую биометрическую систему в процессе аутентификации физического лица (далее – обработка информации в процессе аутентификации), а также при предоставлении органами, организациями, индивидуальными предпринимателями и 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

---

[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» (Собрание законодательства Российской Федерации, 2011, № 49, ст. 7284; 2021, № 27, ст. 5371).

идентификации и аутентификации) сведений о физических лицах, содержащихся в их информационных системах, 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, утвержденных приказом ФСБ России № 378.

6. Угроза нарушения конфиденциальности (компрометации) информации о степени соответствия при обработке информации в процессе аутентификации, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер, утвержденных приказом ФСБ России № 378.

7. 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, обработке и передаче информации о степени соответствия в единой биометрической системе и при взаимодействии 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, утвержденных приказом ФСБ России № 378.