МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 65692
от "03" ноября 2021 г.

ПРИКАЗ

01.09.2021 № 902

Москва

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»

В соответствии с пунктом 6 части 13 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, № 11, ст. 1708) и пунктом 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 года № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708; 2021, № 35, ст. 6312),

ПРИКАЗЫВАЮ:

1. Утвердить по согласованию с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и публичным акционерным обществом «Ростелеком» 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 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 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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 01.09.2021 г. № 902

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, 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»

1. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных при автоматизированной обработке биометрических персональных данных на пользовательском оборудовании (оконечном оборудовании), имеющем в своем составе идентификационный модуль, клиента – физического лица, – для обработки биометрических персональных данных в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных в частях 18^{18} и 18^{20} 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), 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, регистрационный № 33620 (далее – Состав и содержание организационных и технических мер).

2. Угрозы безопасности, актуальные при сборе биометрических персональных данных в центральном (головном) офисе, филиалах или внутренних структурных подразделениях организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц (далее – организации), с использованием стационарных средств вычислительной техники и при передаче собранных биометрических персональных данных между филиалами или внутренними структурными подразделениями организаций и центральным (головным) офисом для обработки биометрических персональных данных в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных в частях 18^{18} и 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ:

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 11 Состава и содержания 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, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76, зарегистрированным Министерством юстиции Российской Федерации 11 сентября 2020 года, регистрационный № 59772 (далее – Требования), 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);

2.2. угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер;

2.3. угроза несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств;

2.4. угроза нарушения доступности, в том числе отказа в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

3. Угрозы безопасности, актуальные при сборе биометрических персональных данных работниками организаций с использованием мобильных (переносных) устройств вычислительной техники (планшетов) и при передаче собранных биометрических персональных данных между мобильными (переносными) средствами вычислительной техники и информационной инфраструктурой структурных подразделений организаций для обработки биометрических персональных данных в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных в частях 18^{18} и 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ:

3.1. угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных),

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);

3.2. угроза несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств;

3.3. угроза нарушения доступности, в том числе отказа в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

4. Угрозы безопасности, актуальные при обработке (за исключением сбора), в том числе хранении, биометрических персональных данных и информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – информация о степени соответствия) в осуществляющих обработку биометрических персональных данных информационных системах организаций в целях аутентификации физического лица в случае выполнения условий, установленных частью 18^{18} статьи 14^{1} Федерального закона № 149-ФЗ:

4.1. угроза нарушения целостности (подмены, удаления) биометрических персональных данных и 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;

4.2. 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.

5. Угрозы безопасности, актуальные при обработке (за исключением сбора) биометрических персональных данных и информации о степени их соответствия при взаимодействии с собственными информационными системами организаций в целях аутентификации физического лица в случае выполнения условий, установленных частью 18^{18} статьи 14^{1} Федерального закона № 149-ФЗ:

5.1. при обработке биометрических персональных данных и информации о степени соответствия организациями с использованием стационарных средств вычислительной техники:

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 11 Состава и содержания 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), 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);

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер;

5.2. при обработке биометрических персональных данных и информации о степени соответствия организациями 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).

6. Угроза несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным, при обработке (за исключением сбора) биометрических персональных данных и информации о степени соответствия в осуществляющих обработку биометрических персональных данных информационных системах организаций и при взаимодействии с собственными информационными системами в целях аутентификации физического лица в случае выполнения условий, установленных частью 18^{18} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

7. Угроза нарушения доступности, в том числе отказа в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации, при обработке (за исключением сбора) биометрических персональных данных и информации о степени соответствия в осуществляющих обработку биометрических персональных данных информационных системах организаций и при взаимодействии с собственными

информационными системами в целях аутентификации физического лица в случае выполнения условий, установленных частью 18^{18} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

8. Угроза нарушения целостности (подмены, удаления) биометрических персональных данных и информации о степени соответствия, нарушения конфиденциальности (компрометации) биометрических персональных данных при обработке (за исключением сбора), в том числе хранении, биометрических персональных данных и информации о степени соответствия в осуществляющих обработку биометрических персональных данных информационных системах организаций в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 13 Состава и содержания организационных и технических мер.

9. Угрозы безопасности, актуальные при обработке (за исключением сбора) биометрических персональных данных и информации о степени их соответствия при взаимодействии с собственными информационными системами организаций в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ:

9.1. при обработке биометрических персональных данных и информации о степени соответствия организациями с использованием стационарных средств вычислительной техники:

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 11 Состава и содержания 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), 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);

угроза нарушения конфиденциальности (компрометации) биометрических персональных данных, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 11 Состава и содержания организационных и технических мер;

9.2. при обработке биометрических персональных данных и информации о степени соответствия организациями 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).

10. Угроза несанкционированного доступа к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным при обработке (за исключением сбора) биометрических персональных данных и информации о степени соответствия в осуществляющих обработку биометрических персональных данных информационных системах организаций и при взаимодействии с собственными информационными системами в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18^{20} статьи 14^{1} Федерального закона

№ 149-ФЗ, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

11. Угроза нарушения доступности, в том числе отказа в обслуживании компонентов, нарушения функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации при обработке (за исключением сбора) биометрических персональных данных и информации о степени соответствия в осуществляющих обработку биометрических персональных данных информационных системах организаций и при взаимодействии с собственными информационными системами в целях идентификации либо идентификации и аутентификации физического лица в случае выполнения условий, установленных частью 18^{20} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем использования уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей), внедрения вредоносного программного обеспечения, использования недекларированных возможностей программного обеспечения, ошибочных действий в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

12. Угроза нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения конфиденциальности (компрометации) информации о степени соответствия при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с информационными системами организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, в целях аутентификации физического лица в соответствии с частью 18^{24} статьи 14^{1} Федерального закона № 149-ФЗ, в том числе путем реализации целенаправленных действий с использованием возможностей, указанных в пункте 12 Состава и содержания организационных и технических мер.

13. Угрозы безопасности, актуальные при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей,

нотариусов и организаций, за исключением организаций финансового рынка, с информационными системами организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, в целях идентификации либо идентификации и аутентификации физического лица в соответствии с частью 18^{26} статьи 14^{1} Федерального закона № 149-ФЗ:

13.1. угроза нарушения целостности (подмены, удаления) биометрических персональных данных и 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;

13.2. 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.