МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ № _____

Москва

Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

В соответствии с пунктом 3 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) и 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 прилагаемые:

Методику проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с биометрическими персональными данными, содержащимися в указанных информационных системах, одного физического лица;

Методику проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой осуществляется поиск предоставленных биометрических персональных данных одного физического лица по биометрическим персональным данным, содержащимся в указанных информационных системах, более чем одного физического лица.

2. Установить, что в отношении биометрических персональных данных, используемых в соответствии с частями 18 и 18.14 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» для идентификации, степень взаимного соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, достаточная для проведения идентификации физического лица, составляет не менее 0,9999.

3. Положения утверждаемых в соответствии с пунктом 1 настоящего приказа методик в отношении биометрических персональных данных, используемых в соответствии с частями 18.14, 18.17, 18.18 и 18.20 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вступают в силу с 1 января 2022 г.

4. Признать утратившим силу приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21 июня 2018 г. № 307 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся 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 гражданина Российской Федерации, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (зарегистрирован Минюстом России 29.06.2018, регистрационный № 51496).

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

6. Контроль за исполнением настоящего приказа возложить на статс-секретаря – заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации О.Б. Пака.

Министр М.И. Шадаев

УТВЕРЖДЕНА
приказом Министерства цифрового
развития, связи и массовых
коммуникаций
Российской Федерации
от _____2021 г. № _____

МЕТОДИКА
проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с биометрическими персональными данными, содержащимися в указанных информационных системах, одного физического лица

1. Методика проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с биометрическими персональными данными, содержащимися в указанных информационных системах, одного физического лица (далее – Методика), применяется в отношении биометрических персональных данных, используемых в соответствии с частями 18, 18.2, 18.14, 18.17, 18.18 и 18.20 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ), при проверке соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также расчете степени взаимного соответствия указанных биометрических персональных данных.

2. Методика применяется с учетом пунктов 8.2.3 и 8.2.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2007 г. № 403-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2009), пункта 12.2.2 национального стандарта Российской Федерации ГОСТ Р 58624.3-2019 «Информационные технологии (ИТ). Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний», утвержденного приказом Федерального агентства по

техническому регулированию и метрологии от 20 ноября 2019 г. № 1197-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2019).

3. Данные о степени взаимного соответствия биометрических персональных данных в отношении биометрических персональных данных, используемых в соответствии с частями 18 и 18.14 статьи 14.1 Федерального закона № 149-ФЗ, представляются оператором 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, только в случае, если значение степени взаимного соответствия биометрических персональных данных не ниже установленного настоящим приказом.

4. В целях принятия решения о соответствии предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется степень взаимного соответствия указанных данных (P), рассчитываемая как:

$P = 1 - \prod_{i=1}^{n} p_i^{\text{ВЛС}} \times \prod_{j=1}^{m} p_j^{\text{ВОКПА}}$,

где $\prod_{i=1}^{n} p_i^{\text{ВЛС}}$ – произведение $p_i^{\text{ВЛС}}$ для всех i от 1 до n;

$\prod_{j=1}^{m} p_j^{\text{ВОКПА}}$ – произведение $p_j^{\text{ВОКПА}}$ для всех j от 1 до m;

$p_i^{\text{ВЛС}}$– доля предоставленных государственным органом, органом местного самоуправления, организацией финансового рынка, иными организациями, индивидуальным предпринимателем, нотариусом (далее – государственный орган, банк и иная организация, индивидуальный предприниматель, нотариус) биометрических персональных данных каждой из n-модальностей, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, которые ошибочно признаны совпадающими с указанными биометрическими персональными данными другого физического лица, содержащимися в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных;

$p_j^{\text{ВОКПА}}$ – доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных каждой из m-модальностей или для каждого независимого унимодального и (или) мультимодального алгоритмов, используемых для обнаружения атаки на биометрическое предъявление в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при атаке на данную информационную систему, которые ошибочно признаны подлинными биометрическими персональными данными;

n – количество независимых модальностей, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных;

m – количество независимых модальностей или независимых унимодальных и (или) мультимодальных алгоритмов, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, для обнаружения атаки на биометрическое предъявление.

5. Вероятность ложного совпадения ($p_i^{\text{ВЛС}}$) предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных указанным биометрическим персональным данным физического лица, содержащимся в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется как минимальное значение вероятности ложного совпадения, при котором соответствующая ей вероятность ложного несовпадения ($p_i^{\text{ВЛНС}}$) не превышает порогового значения вероятности ложного несовпадения.

Вероятность ошибки классификации предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных при атаке ($p_j^{\text{ВОКПА}}$) на информационную систему, обеспечивающую идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется как минимальное значение вероятности ошибки классификации биометрических персональных данных при атаке, при котором соответствующая ей вероятность ошибки классификации подлинных биометрических персональных данных ($p_i^{\text{ВОКПБП}}$) не превышает порогового значения вероятности ошибки классификации подлинных биометрических персональных данных.

6. Вероятность ложного несовпадения предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных указанным биометрическим персональным данным физического лица, содержащимся в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется как доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных, которые ошибочно признаны несовпадающими с указанными биометрическими персональными данными идентифицируемого или аутентифицируемого физического лица, содержащимися в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных.

Вероятность ошибки классификации предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом подлинных биометрических персональных данных определяется как доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом подлинных биометрических персональных данных, которые ошибочно признаны атаками на информационную систему, обеспечивающую идентификацию и (или) аутентификацию с использованием биометрических персональных данных.

УТВЕРЖДЕНА
приказом Министерства цифрового
развития, связи и массовых
коммуникаций
Российской Федерации
от _____2021 г. № _____

МЕТОДИКА
проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой осуществляется поиск предоставленных биометрических персональных данных одного физического лица по биометрическим персональным данным, содержащимся в указанных информационных системах, более чем одного физического лица

1. Методика проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при которой осуществляется поиск предоставленных биометрических персональных данных одного физического лица по биометрическим персональным данным, содержащимся в указанных информационных системах, более чем одного физического лица (далее – Методика), применяется в отношении биометрических персональных данных, используемых в соответствии с частями 18, 18.2, 18.14, 18.17, 18.18 и 18.20 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ), при проверке соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также расчете степени взаимного соответствия указанных биометрических персональных данных.

2. Методика применяется с учетом пункта 8.4.3 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура.», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2007 г. № 403-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2009), пункта 12.2.2 национального стандарта Российской Федерации ГОСТ Р 58624.3-2019 «Информационные технологии (ИТ). Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний», утвержденного приказом Федерального агентства по

техническому регулированию и метрологии от 20 ноября 2019 г. № 1197-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2019).

3. Данные о степени взаимного соответствия биометрических персональных данных в отношении биометрических персональных данных, используемых в соответствии с частями 18 и 18.14 статьей 14.1 Федерального закона № 149-ФЗ, представляются оператором 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, только в случае, если значение степени взаимного соответствия биометрических персональных данных не ниже установленного настоящим приказом.

4. В целях принятия решения о соответствии предоставленных биометрических персональных данных физического лица биометрическим персональным данным физических лиц, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется степень взаимного соответствия указанных данных (P), рассчитываемая как:

$P = 1 - \prod_{i=1}^{n} p_i^{\text{ВЛПБИ}} \times \prod_{j=1}^{m} p_j^{\text{ВОКПА}}$,

где $\prod_{i=1}^{n} p_i^{\text{ВЛПБИ}}$ – произведение $p_i^{\text{ВЛПБИ}}$ для всех i от 1 до n;

$\prod_{j=1}^{m} p_j^{\text{ВОКПА}}$ – произведение $p_j^{\text{ВОКПА}}$ для всех j от 1 до m;

$p_{\text{i}}^{\text{ВЛПБИ}}$– доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных физических лиц, биометрические персональные данные которых не содержатся в информационной системе, каждой из n-модальностей, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, которые ошибочно признаны совпадающими с указанными биометрическими персональными данными, содержащимися в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных;

$p_j^{\text{ВОКПА}}$ – доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных каждой из m-модальностей или для каждого независимого унимодального и (или) мультимодального алгоритмов, используемых для обнаружения атаки на биометрическое предъявление в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, при атаке на данную информационную систему, которые ошибочно признаны подлинными биометрическими персональными данными;

n – количество независимых модальностей, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных;

m – количество независимых модальностей или независимых унимодальных и (или) мультимодальных алгоритмов, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, для обнаружения атаки на биометрическое предъявление.

5. Вероятность ложноположительной биометрической идентификации ($p_{\text{i}}^{\text{ВЛПБИ}}$) предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных, определяется как минимальное значение вероятности ложноположительной биометрической идентификации, при которой соответствующая ей вероятность ложноотрицательной биометрической идентификации ($p_i^{\text{ВЛОБИ}}$) не превышает порогового значения вероятности ложноотрицательной биометрической идентификации.

Вероятность ошибки классификации ($p_i^{\text{ВОКПА}}$) предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных при атаке на информационную систему, обеспечивающую идентификацию и (или) аутентификацию с использованием биометрических персональных данных, определяется как минимальное значение вероятности ошибки классификации биометрических персональных данных при атаке, при котором соответствующая ей вероятность ошибки классификации подлинных биометрических персональных данных ($p_i^{\text{ВОКПБП}}$) не превышает порогового значения вероятности ошибки классификации подлинных биометрических персональных данных.

6. Вероятность ложноотрицательной биометрической идентификации предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных определяется как доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных физического лица, биометрические персональные данные которого содержатся в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных, которые ошибочно признаны несовпадающими с указанными биометрическими персональными данными идентифицируемого или аутентифицируемого физического лица, содержащимися в информационной системе, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных.

Вероятность ошибки классификации предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом подлинных биометрических персональных данных определяется как доля предоставленных государственным органом, банком и иной организацией, индивидуальным предпринимателем, нотариусом подлинных биометрических персональных данных, которые ошибочно признаны атаками на информационные системы, обеспечивающие идентификацию и (или) аутентификацию с использованием биометрических персональных данных.