



**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПРИКАЗ

№ _____

Москва

Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы и степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации, и о признании утратившим силу приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 6 августа 2021 г. № 816

В соответствии с пунктом 3 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» (Российская газета, 2023, 9 января)

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

Методику проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с векторами единой биометрической системы одного физического лица;

Методику проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой осуществляется поиск предоставленных биометрических персональных

данных одного физического лица по векторам единой биометрической системы более чем одного физического лица.

2. Установить, что в отношении биометрических персональных данных, используемых в соответствии со статьей 9 и частями 1 и 2 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» для идентификации и (или) аутентификации, степень взаимного соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, достаточная для проведения идентификации и (или) аутентификации физического лица, составляет не менее 0,9999.

3. Признать утратившим силу приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 6 августа 2021 г. № 816 «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» (зарегистрирован Минюстом России 08.09.2021, регистрационный № 64922).

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

Министр

М.И. Шадаев

УТВЕРЖДЕНА
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от ____ . ____ .2023 № ____

МЕТОДИКА

проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с векторами единой биометрической системы одного физического лица

1. Методика проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой предоставленные биометрические персональные данные одного физического лица сравнивают с векторами единой биометрической системы одного физического лица, (далее – Методика) применяется в отношении биометрических персональных данных, используемых в соответствии со статьями 5, 9, 10, 14 и 16 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 – Федеральный закон № 572-ФЗ), при проверке соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, а также расчете степени взаимного соответствия биометрических персональных данных, используемых в соответствии со статьей 9 и частями 1 и 2 статьи 14 Федерального закона № 572-ФЗ, и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации.

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., Стандартиформ, 2019).

3. Данные о степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы в отношении биометрических персональных данных, используемых в соответствии со статьей 9 и частями 1 и 2 статьи 14 Федерального закона № 572-ФЗ, представляются оператором государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» только в случае, если значение степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы не ниже установленного настоящим приказом.

4. В целях принятия решения о соответствии предоставленных биометрических персональных данных физического лица векторам единой биометрической системы определяется степень взаимного соответствия указанных данных (P), рассчитываемая как:

$$P = 1 - \prod_{i=1}^n P_i^{\text{ВЛС}} \times L$$

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

$L = \prod_{j=1}^m P_j^{\text{ВОКПА}}$ – произведение $P_j^{\text{ВОКПА}}$ для всех j от 1 до m или 1, если не осуществляется обнаружение атак на биометрическое предъявление;

$P_i^{\text{ВЛС}}$ – доля предоставленных государственным органом, органом местного самоуправления, Центральным банком Российской Федерации, организацией финансового рынка, иными организациями, индивидуальным предпринимателем, нотариусом (далее – государственный орган, Центральный банк Российской Федерации, банк и иная организация, индивидуальный предприниматель, нотариус) биометрических персональных данных каждой из n -модальностей, которые ошибочно признаны совпадающими с векторами единой биометрической системы другого физического лица;

$P_j^{\text{ВОКПА}}$ – доля предоставленных государственным органом, Центральным банком Российской Федерации, 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 на основе 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 на основе биометрических персональных данных;

m – количество независимых модальностей или независимых унимодальных и (или) мультимодальных алгоритмов, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию на основе

биометрических персональных данных, для обнаружения атаки на биометрическое предъявление.

5. Вероятность ложного совпадения ($P_i^{\text{ВЛС}}$) предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных и векторов единой биометрической системы 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, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных при атаке ($P_j^{\text{ВОКПА}}$) на информационную систему, обеспечивающую идентификацию и (или) аутентификацию на основе 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 ($P_j^{\text{ВОКПЫП}}$) не превышает порогового значения вероятности ошибки классификации подлинных биометрических персональных данных.

6. Вероятность ложного несовпадения предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных и векторов единой биометрической системы определяется как доля предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных, которые ошибочно признаны несовпадающими с векторами единой биометрической системы.

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

УТВЕРЖДЕНА
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от ____ . ____ .2023 № ____

МЕТОДИКА

проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой осуществляется поиск предоставленных биометрических персональных данных одного физического лица по векторам единой биометрической системы более чем одного физического лица

1. Методика проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, при которой осуществляется поиск предоставленных биометрических персональных данных одного физического лица по векторам единой биометрической системы более чем одного физического лица, (далее – Методика) применяется в отношении биометрических персональных данных, используемых в соответствии со статьями 5, 9, 10, 14 и 16 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 – Федеральный закон № 572-ФЗ), при проверке соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы, а также расчете степени взаимного соответствия биометрических персональных данных, используемых в соответствии со _____ статьей _____ 9 и частями 1 и 2 статьи 14 Федерального закона № 572-ФЗ, и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации.

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., Стандартиформ, 2019).

3. Данные о степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы в отношении биометрических персональных данных, используемых в соответствии со статьей 9 и частями 1 и 2 статьи 14 Федерального закона № 572-ФЗ, представляются оператором государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» 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 векторам единой биометрической системы определяется степень взаимного соответствия указанных данных (P), рассчитываемая как:

$$P = 1 - \prod_{i=1}^n P_i^{\text{ВЛПБИ}} \times L$$

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

$$L = \prod_{j=1}^m P_j^{\text{ВОКПА}} \quad \text{– произведение } P_j^{\text{ВОКПА}} \text{ для всех } j \text{ от 1 до } m \text{ или 1, если}$$

не осуществляется обнаружение атак на биометрическое предъявление;

$P_i^{\text{ВЛПБИ}}$ – доля предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных физических лиц, в отношении которых отсутствуют соответствующие векторы единой биометрической системы, каждой из n -модальностей, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию на основе биометрических персональных данных, которые ошибочно признаны совпадающими с векторами единой биометрической системы;

$P_j^{\text{ВОКПА}}$ – доля предоставленных государственным органом, Центральным банком Российской Федерации, 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 на основе 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 на основе биометрических персональных данных;

m – количество независимых модальностей или независимых унимодальных и (или) мультимодальных алгоритмов, используемых в информационной системе, обеспечивающей идентификацию и (или) аутентификацию на основе

биометрических персональных данных, для обнаружения атаки на биометрическое предъявление.

5. Вероятность ложноположительной биометрической идентификации ($P_i^{\text{ВЛПБИ}}$) предоставленных государственным органом, Центральным банком Российской Федерации, 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 ($P_j^{\text{ВОКПА}}$) предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных при атаке на информационную систему, обеспечивающую идентификацию и (или) аутентификацию на основе 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, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных определяется как доля предоставленных государственным органом, Центральным банком Российской Федерации, банком и иной организацией, индивидуальным предпринимателем, нотариусом биометрических персональных данных физического лица, в отношении которых имеются соответствующие векторы единой биометрической системы, которые ошибочно признаны несовпадающими с векторами единой биометрической системы.

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