

Виталий Г. Иваненко¹, Нина Д. Иванова², Алексей Г. Сабанов³

¹Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия

^{2,3}Российский университет транспорта (МИИТ),
ул. Образцова, 9, стр. 9, Москва, 127994, Россия

¹e-mail: VGIvanenko@mephi.ru, <https://orcid.org/0000-0003-0823-5501>

²e-mail: IvanovaND.Nina@yandex.ru, <https://orcid.org/0000-0001-5942-8050>

³e-mail: Asabanov@mail.ru, <https://orcid.org/0000-0002-2231-0240>

ПОВЫШЕНИЕ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПУТЕМ ВНЕСЕНИЯ ИЗБЫТОЧНОСТИ

DOI: <http://dx.doi.org/10.26583/bit.2022.2.03>

Аннотация. В статье показывается необходимость исследования функциональной надежности систем идентификации и применимости для систем биометрической идентификации методов обеспечения функциональной надежности информационных систем. Рассматриваются методы обеспечения функциональной надежности систем биометрической идентификации путем обеспечения приемлемых показателей надежности средств идентификации и путем внесения избыточности. Исследуется применимость методов для систем биометрической идентификации, оцениваются их достоинства и недостатки. Для программного метода внесения избыточности разработана надежностная схема мажоритарного резервирования «2 из 3» с применением N-версионного программирования. Для реализации системы идентификации с одним дополнительным резервным элементом разработана соответствующая надежностная схема, основанная на принципах дуального программирования. На основе статистических данных NIST по алгоритмам распознавания лиц для разработанных надежностных схем оценены показатели надежности и доказаны их преимущества над системой, состоящей из одного нерезервируемого элемента. Предложенные надежностные схемы согласуются с практикой обеспечения функциональной надежности информационных систем и могут быть интегрированы в системы биометрической идентификации, использующие биометрические характеристики в качестве основного идентификатора доступа.

Ключевые слова: идентификация, функциональная надежность, биометрические алгоритмы идентификации, мажоритарное резервирование, N-версионное программирование, дуальное программирование.

Для цитирования: ИВАНЕНКО, Виталий Г.; ИВАНОВА, Нина Д.; САБАНОВ, Алексей Г. ПОВЫШЕНИЕ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПУТЕМ ВНЕСЕНИЯ ИЗБЫТОЧНОСТИ. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 36–45, 2022. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1416>. DOI: <http://dx.doi.org/10.26583/bit.2022.2.03>.

Vitaliy G. Ivanenko¹, Nina D. Ivanova², Aleksey G. Sabanov³

¹National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia

^{2,3}Russian University of Transport (MIIT),
Obraztsova Str., 9, p. 9, Moscow, 127994, Russia

¹e-mail: VGIvanenko@mephi.ru, <https://orcid.org/0000-0003-0823-5501>

²e-mail: IvanovaND.Nina@yandex.ru, <https://orcid.org/0000-0001-5942-8050>

³e-mail: Asabanov@mail.ru, <https://orcid.org/0000-0002-2231-0240>

Improving functional reliability of biometric identification systems by introducing redundancy

DOI: <http://dx.doi.org/10.26583/bit.2022.2.03>

Abstract. The paper demonstrates a need to study the functional reliability of identification systems and the applicability of methods for ensuring the functional reliability of information systems for biometric identification systems. Methods of ensuring functional reliability of biometric identification systems via providing indicators of reliability of identification devices and introducing redundancy are considered. The applicability of the methods for biometric identification systems is investigated, its advantages and disadvantages are evaluated. Triple modular redundancy scheme has been developed for the program redundancy using N-version programming. An appropriate reliability scheme based on the principles of dual programming has been developed to implement the identification system with one additional redundant element. Based on the NIST statistics of face recognition algorithms for the developed reliability schemes the reliability indicators were evaluated and its advantages over a system consisting of a single non-redundant element have been shown. The proposed reliability schemes are consistent with the practice of ensuring the functional reliability of information systems and can be integrated into biometric identification systems that use biometric data as the main access identifier.

Keywords: *identification, functional reliability, biometric identification algorithms, triple modular redundancy, N-version programming, dual programming.*

For citation: IVANENKO, Vitaliy G.; IVANOVA, Nina D.; SABANOV, Aleksey G. Improving functional reliability of biometric identification systems by introducing redundancy. *IT Security (Russia)*, [S.l.], v. 29, no. 2, p. 36–45, 2022. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1416>. DOI: <http://dx.doi.org/10.26583/bit.2022.2.03>.

Введение

В большинстве информационных систем защита важных для организации информационных активов от доступа неавторизованных пользователей реализуется с применением трех основных процессов контроля доступа: идентификации, аутентификации и авторизации. В данной статье исследуется проблема безопасности процесса идентификации.

В настоящее время существует множество методов, с помощью которых субъект доступа может быть идентифицирован. К основным типам идентификаторов субъектов доступа относятся:

- универсальные идентификаторы (электронный паспорт, ИНН, СНИЛС);
- корпоративные идентификаторы (пропуск на территорию организации);
- личные идентификаторы (биометрические данные человека).

Развитие биометрических технологий идентификации является особенно актуальной и востребованной задачей [1]. Современные платежные системы активно вводят оплату по биометрическим данным в качестве единственного идентификатора доступа без последующего процесса аутентификации (оплата по биометрическим данным проездного билета в метро, покупки в оффлайн-магазинах).

Биометрическая идентификация имеет вероятностную природу, и в соответствии с международными стандартами^{1,2} использование биометрических данных в качестве основного фактора идентификации не является безопасным. Биометрические характеристики не содержат «секрета», вследствие чего, не могут служить фактором аутентификации, а только лишь подтверждением, например, фактора владения аутентифицирующей информацией [2].

Одним из критериев доверия к результатам идентификации является обеспечение достаточного уровня надежности систем биометрической идентификации [3]. В [4–6] на основе тестирования различных устройств биометрической идентификации и имеющихся

¹NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. URL: <https://doi.org/10.6028/NIST.SP.800-63b> (дата обращения: 15.05.2022)

²NIST SP 800-63A. Digital Identity Guidelines: Enrollment and Identity Proofing. URL: <https://doi.org/10.6028/NIST.SP.800-63a> (дата обращения: 15.05.2022)

статистических данных выявлено, что полученные показатели надежности не являются достаточными для информационных систем с большим количеством пользователей.

Несмотря на то, что использование биометрических данных в качестве основного фактора идентификации не рекомендуется международными стандартами, и проблема надежности таких систем идентификации обозначается в научных исследованиях, в платежные системы РФ активно внедряется биометрическая идентификация по причине удобства ее использования со стороны клиента [7]. Вышеизложенное свидетельствует об актуальности исследования безопасности биометрической идентификации, в том числе, функциональной надежности таких систем идентификации.

В рамках настоящего исследования рассматривается процесс вторичной идентификации, задачей которой является распознавание пользователя при повторном запросе доступа в информационную систему. Основными этапами первичной идентификации являются проверка достоверности и верификация предъявляемых кандидатом идентификаторов, надежность выполнения которых в настоящей статье рассматриваться не будет.

1. Методы обеспечения функциональной надежности систем идентификации

Функциональную надежность информационных систем в соответствии с [8] можно определить как общую надежность системы, результатам функционирования которой можно оправданно доверять. Функциональную надежность систем идентификации можно обеспечить двумя различными способами:

- путем обеспечения приемлемых показателей надежности программных и программно-технических средств;
- путем внесения информационной, структурной, временной, программной и других видов избыточности.

Первый способ обеспечения функциональной надежности реализуется путем улучшения и модернизации программно-технических средств идентификации (например, смарт-карт и биометрических устройств), а также программных средств идентификации (например, биометрических алгоритмов). Данному способу посвящены исследования [4–6].

Второй способ обеспечения функциональной надежности ориентирован на повышение функциональной надежности системы идентификации в целом, а не ее отдельных компонентов. Внесение избыточности в систему идентификации реализуется путем внедрения дополнительных программных и программно-технических средств (сверх тех, что могли бы обеспечить ее функционирование) с целью повышения ее функциональной надежности.

Данная статья посвящена исследованию способа повышения функциональной надежности путем внесения избыточности. Применимо к системам биометрической идентификации можно выделить следующие методы внесения избыточности в информационные системы [9]:

- структурная избыточность (ввод в систему идентификации избыточных устройств биометрической идентификации);
- временная избыточность (многократная реализация заданной функции на одном и том же оборудовании и с применением одного и того же биометрического алгоритма с последующим сравнением результатов);
- программная избыточность (параллельное применение различных биометрических алгоритмов к одним и тем же исходным данным с последующим сравнением результатов);

– информационная избыточность (множественная регистрация биометрических образов кандидата на этапе первичной идентификации).

На практике возможности применения избыточности ограничиваются допустимыми значениями стоимости избыточных устройств и алгоритмов биометрической идентификации или времени принятия решения. В связи с этим, при проектировании системы идентификации необходимо решать задачу оптимизации с ограничениями: определение оптимальной вносимой избыточности для достижения максимально возможной функциональной надежности системы идентификации, характеризующейся степенью достоверности выходной информации, с учетом ограничивающих факторов.

Исследование внесения информационной избыточности в систему первичной идентификации представлено в [10], поэтому в рамках настоящей статьи не рассматривается.

Как показано в [11], для анализа функциональной надежности систем идентификации и аутентификации можно применить процессный подход, следовательно, процесс вторичной биометрической идентификации может быть рассмотрен как последовательность следующих этапов:

- сбор информации, поступающей от биометрического считывателя (распознавание кандидата);
- обработка информации (создание биометрического образа, извлечение контролируемых биометрических параметров);
- сравнение биометрического образа с имеющимися в базе данных (проверка существования идентификатора).

Информация, обрабатываемая в системе идентификации, может быть подвергнута искажению на каждом из этапов, следовательно, обуславливается необходимость обеспечения функциональной надежности в течение всего процесса идентификации.

Функциональную надежность на всех трех этапах вторичной идентификации можно обеспечить структурной избыточностью путем введения дополнительного независимого устройства биометрической идентификации, на котором будет реализован весь процесс вторичной идентификации. Данный метод не увеличит время отклика, но потребует больших финансовых вложений по причине высокой стоимости устройств биометрической идентификации. Меньших финансовых вложений потребует введение дополнительного биометрического считывателя, но в этом случае повышение функциональной надежности будет реализовано только для первого этапа вторичной идентификации.

Введение временной избыточности увеличит время принятия решения, но не потребует дополнительных финансовых затрат. Повторный сбор информации с последующей ее обработкой и проверкой существования идентификатора повысит надежность выполнения биометрической идентификации на всех этапах, но может не снизить риски отказа вторичной идентификации.

Компромиссом между дополнительными финансовыми затратами и временными задержками может являться внесение программной избыточности на втором и третьем этапах идентификации. Параллельное применение нескольких биометрических алгоритмов на одном и том же биометрическом устройстве повысит точность идентификации, но не снизит риски отказа вторичной идентификации и повлияет на увеличение времени отклика, так как программная избыточность влечет за собой временную из-за необходимости использования дополнительных ресурсов для поддержки параллельной работы программ.

Повышение функциональной надежности систем биометрической идентификации путем внесения избыточности возможно лишь при увеличении времени отклика и дополнительных финансовых затратах. Следующим вопросом следует рассмотреть построение надежностной схемы для системы идентификации с последующей оценкой параметров надежности.

2. Построение надежностной схемы для системы идентификации

Мажоритарное резервирование является одним из подходов к внесению избыточности и используется с целью повышения достоверности выходной информации [9, 12]. Надежностная схема с мажоритарным резервированием состоит из нечетного количества n параллельно работающих элементов и восстанавливающего органа. Отказ данной системы наступает при отказе $k = \frac{n+1}{2}$ элементов. Как описано в [9], мажоритарное резервирование в информационных системах реализуется с использованием восстанавливающего органа. Восстанавливающий орган, реализованный программным или аппаратным способом, определяет выходную информацию по большинству голосов (мажоритарным методом) [9].

Кратностью резервирования m в соответствии с [13] называется отношение количества резервных элементов к числу основных элементов. В случае мажоритарного резервирования, состоящего из n элементов, параллельно работающих и выполняющих одну и ту же функцию, кратность резервирования равна: $m = \frac{n-1}{1} = n-1$.

В случае системы идентификации с программной избыточностью решение о существовании предъявленного идентификатора в базе данных («да», «нет») будет приниматься на основе голосования n результатов работы нескольких биометрических алгоритмов. Такой метод внесения программной избыточности называется N-версионным программированием [9].

Биометрическая идентификация имеет вероятностную природу, для оценки надежности биометрических алгоритмов используются следующие характеристики [14]:

- ошибка первого рода ($FPIR$ — False Positive Identification Rate) — ошибка ложноположительной идентификации;
- ошибка второго рода ($FNIR$ — False Negative Identification Rate) — ошибка ложноотрицательной идентификации.

Значения $FNIR$ и $FPIR$ алгоритма обычно можно настроить в программном обеспечении устройства биометрической идентификации. При уменьшении значения $FPIR$ до минимально возможного, значение $FNIR$ возрастает³, делая систему идентификации надежной для безопасности организации, но ненадежной для пользователей. Лучший алгоритм выбирается посредством сравнения $FNIR$ при одинаковых значениях $FPIR$.

На рис. 1 представлена надежностная схема с применением N-версионного программирования, реализованного мажоритарным резервированием «2 из 3», для 3-х алгоритмов распознавания лиц: cloudwalk-mt-004, idemia-008, cubox-002. Значения ложноотрицательной идентификации $FNIR$ для данных алгоритмов по данным NIST за

³Study on Face Identification Technology for its Implementation in the Schengen Information System.
URL: https://www.researchgate.net/publication/334762344_Study_on_Face_Identification_Technology_for_its_Implementation_in_the_Schengen_Information_System (дата обращения: 05.01.2022)

2021 г.⁴ при $FPIR = 0.000001$ соответственно равны: $FNIR_1 = 0.0013$, $FNIR_2 = 0.0032$, $FNIR_3 = 0.0041$.

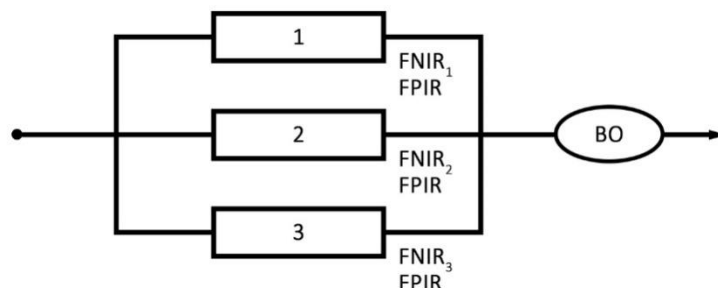


Рис. 1. Система идентификации с применением N-версионного программирования
Fig. 1. Identification system using N-version programming

Оценим вероятность ложноположительной идентификации для надежностной схемы «2 из 3», приняв следующие допущения:

- ошибки алгоритмов независимы;
- вероятность отказа восстанавливающего органа (ВО) принять равной 0 при условии его программной реализации [8].

Отказ данной системы возможен при одновременном отказе двух и более элементов. Следовательно, вероятность ложноположительной идентификации системы «2 из 3» $FPIR_{2из3}$ вычисляется по (1) при условии, что все элементы имеют одинаковое значение $FPIR$.

$$FPIR_{2из3} = \sum_{i=2}^3 C_3^i FPIR^i (1 - FPIR)^{3-i} = 3FPIR^2 - 2FPIR^3. \quad (1)$$

Следовательно, вероятность ложноположительной идентификации системы «2 из 3» равна $FPIR_{2из3} = 3 \times 10^{-12}$ против $FPIR = 1 \times 10^{-6}$ системы идентификации, состоящей из одного нерезервируемого элемента.

Вероятность ложноотрицательной идентификации вычисляется аналогично (1), и для трех алгоритмов с различными $FNIR$ вычисляется как:

$$FNIR_{2из3} = \prod_{i=1}^3 FNIR_i \left(1 + \sum_{j=1}^3 \frac{1 - FNIR_j}{FNIR_j} \right). \quad (2)$$

Вероятность ложноотрицательной идентификации системы «2 из 3» при ранее заданных $FNIR_1 = 0.0013$, $FNIR_2 = 0.0032$, $FNIR_3 = 0.0041$ равна $FNIR_{2из3} = 2 \times 10^{-5}$.

Построенная надежностная схема с применением N-версионного программирования, реализованного мажоритарным резервированием «2 из 3», улучшает показатели надежности идентификации, но требует дополнительных финансовых затрат и увеличивает время отклика. Финансовые затраты необходимы для установки и поддержки дополнительных программ, но они существенно ниже, чем могли быть для системы с внесенной структурной избыточностью. У построенной надежностной схемы снижение скорости выполнения идентификации возникает по причине того, что программная избыточность неизбежно влечет за собой временную, так как параллельное выполнение нескольких независимых программ на одном и том же устройстве требует

⁴NIST. FRVT (Face Recognition Vendor Test) Performance Summary. URL: <https://pages.nist.gov/frvt/html/frvt11.html> (дата обращения: 05.01.2022)

дополнительных ресурсов на поддержку параллельной обработки, что снижает скорость идентификации, реализуемой несколькими программами, по сравнению с идентификацией, выполненной одной нерезервируемой программой.

Дополнительные временные задержки и финансовые затраты можно минимизировать, если снизить количество резервных программ (биометрических алгоритмов), то есть уменьшить кратность резервирования m . Для надежной схемы «2 из 3» (рис. 1) кратность резервирования равна $m_{2из3} = 2$, и это является минимальным значением кратности резервирования для надежных схем с применением N-версионного программирования, так как мажоритарную систему голосования при количестве элементов $n < 3$ реализовать невозможно.

Надежная схема кратности резервирования $m = 1$ (с одним основным алгоритмом идентификации и одним дополнительным резервным) может быть реализована с применением дуального программирования [9]. Для системы идентификации внесение программной избыточности с применением дуального программирования может быть реализовано следующим образом: основным алгоритмом является биометрический алгоритм с установленным высоким значением $FNIR$, дополнительно с ним используется тот же биометрический алгоритм, но с установленным высоким значением $FPIR$.

Основной алгоритм с высоким значением $FNIR$ (и, следовательно, невысоким значением $FPIR$) является надежным для пользователя (так как минимизирует ошибку ложноотрицательной идентификации). Дополнительный алгоритм с высоким значением $FPIR$, напротив, является надежным для безопасности организации, но имеет ошибку ложноотрицательной идентификации большую, чем у основного алгоритма, так как при увеличении значения $FPIR$ значение $FNIR$ уменьшается. Если результаты работы алгоритмов не отличаются на величину большую, чем допустимая погрешность, решение об идентификации принимается по результатам работы основного алгоритма. В противном случае, за верный принимается результат работы алгоритма с высоким значением $FPIR$, как более надежного для безопасности организации. Функцию выбора выполняет решающий орган [9], в который должен быть запрограммирован критерий выбора с установленной допустимой погрешностью результатов работы основного и дополнительного алгоритмов.

На рис. 2 представлена надежная схема для модифицированного дуального программирования с применением алгоритма распознавания лиц 20face-000. В соответствии с данными NIST, характеристики алгоритма 20face-000 имеют следующие значения: при $FPIR_1 = 0.00001$ $FNIR_1 = 0.0723$, при $FPIR_2 = 0.000001$ $FNIR_2 = 0.1828$.

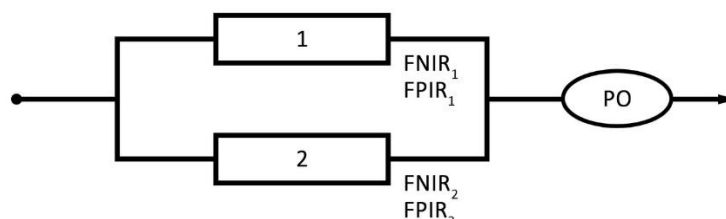


Рис. 2. Система идентификации с применением дуального программирования
Fig. 2. Identification system using dual programming

Считая работу алгоритмов независимой и пренебрегая вероятностью отказа решающего органа (PO), ложноположительная идентификация наступит при отказе

алгоритма с высоким значением $FPIR$. Тогда вероятность ложноположительной идентификации равна $FPIR_{дп} = FPIR_2 = 0.000001$, при условии, что вероятность ложноотрицательной идентификации системы равна $FNIR_{дп} = FNIR_1 = 0.0723$.

Преимуществом надежностной схемы с применением дуального программированием над схемой «2 из 3» является возможность использования одного биометрического алгоритма с различными параметрами $FPIR$, $FNIR$ и меньшая кратность резервирования, влекущая за собой уменьшение времени отклика. Недостатком дуального программирования является необходимость выбора допустимой погрешности, на основе которой принимается решение о допуске/недопуске кандидата и, следовательно, увеличение погрешности результата.

Заключение

В настоящее время биометрические системы идентификации заняли прочные позиции в системах контроля доступа. Несмотря на рекомендации NIST не использовать биометрические характеристики как основной фактор идентификации и невозможность использования биометрических в качестве аутентифицирующих данных, во многих платежных системах биометрическая идентификация является основным идентифицирующим и аутентифицирующим фактором.

Вероятностная природа биометрических систем идентификации обуславливает необходимость исследования как надежности биометрических алгоритмов идентификации, так и функциональной надежности самой системы биометрической идентификации.

В настоящей работе был проведен анализ возможных методов обеспечения функциональной надежности биометрических систем идентификации и обоснована целесообразность применения метода повышения функциональной надежности путем внесения программной избыточности как компромиссной между временными задержками и финансовыми затратами.

Предложенные в работе надежностные схемы для систем биометрической идентификации согласуются с практикой обеспечения функциональной надежности информационных систем. Расчет основных показателей надежности биометрической идентификации по статистическим данным из актуальной базы данных NIST показал целесообразность применения предложенных в настоящей работе надежностных схем для обеспечения функциональной надежности систем идентификации. Предложенные надежностные схемы могут быть интегрированы в существующие системы биометрической идентификации, использующие биометрические характеристики в качестве основного идентификатора доступа.

СПИСОК ЛИТЕРАТУРЫ:

1. Vandana and N. Kaur. A Study of Biometric Identification and Verification System, 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2021, p. 60–64. DOI: <https://doi.org/10.1109/ICACITE51222.2021.9404735>.
2. Конявская С.В. Бесфакторная классификация аутентифицирующих данных: начала построения. Комплексная защита информации: материалы XXIV научно-практической конференции. 2019, с. 194–200. URL: <https://www.okbsapr.ru/library/publications/kzi2019-konyavskaya/> (дата обращения: 06.01.2022).
3. Сабанов А.Г. Критерии доверия к результатам идентификации субъектов доступа. Электросвязь. 2019, № 3, с. 38–44. URL: aladdin-rd.ru/company/pressroom/articles/kriterii-doveria-k-rezultatam-identifikacii-subektov-dostupa (дата обращения: 13.05.2022).

4. Nídllová V., Hart J. Reliability of biometric identification using fingerprints under adverse conditions. *Agronomy Research*. 2015, № 13(3), p. 786–791. URL: https://agronomy.emu.ee/vol133/13_3_17_B5.pdf (дата обращения: 02.01.2022).
5. Сабанов А.Г., Смолина С.Г. Сравнительный анализ биометрических методов идентификации личности. *Труды ИСА РАН*. 2016, № 66, с. 12–21. URL: http://www.isa.ru/proceedings/images/documents/2016-66-3/t-16-3_11-20.pdf (дата обращения: 02.01.2022).
6. Brumník Robert & Balantić Zvone. Reliability and Efficacy of Identification Systems and Supply Chain Management. *Strojniski Vestnik*. 2008, no. 54(11), p. 783–795. URL: https://www.researchgate.net/publication/290780033_Reliability_and_Efficacy_of_Identification_Systems_and_Supply_Chain_Management (дата обращения: 02.01.2022).
7. Бутов А.В., Карякин А.М. Проблемы развития биометрии как основы цифровизации отечественной экономики и пути их решения. *Известия ВУЗов ЭФиУП*. 2020, № 1(43), с. 48–52. URL: <https://elibrary.ru/item.asp?id=42654116> (дата обращения: 15.05.2022).
8. Гаранин А.И. О функциональной надежности информационных систем. *ИТНОУ: информационные технологии в науке, образовании и управлении*. 2018, № 2(6), с. 45–50. URL: <https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem> (дата обращения: 02.01.2022).
9. Шубинский И.Б. Надежные отказоустойчивые информационные системы. М.: «Журнал Надежность», 2016. – 547 с. URL: <https://www.dependability.ru/jour/manager/files/books/%25D0%259A%25D0%25BD%25D0%25B8%25D0%25B3%25D0%25B0I.pdf> (дата обращения: 02.01.2022).
10. Сартасов С.Ю. Оценка надёжности биометрических систем с непрерывной классификацией и множественной регистрацией. *Компьютерные инструменты в образовании*. 2013, № 4, с. 12–20. URL: <https://cyberleninka.ru/article/n/otsenka-nadyozhnosti-biometricheskih-sistem-s-nepreryvnoy-klassifikatsiyey-i-mnozhestvennoy-registratsiyey> (дата обращения: 05.01.2022).
11. Сабанов А.Г. Методы исследования надежности удаленной аутентификации. *Электросвязь*. 2012, № 10, с. 20–24. URL: https://www.aladdin-rd.ru/company/pressroom/articles/metody_issledovania_nadezhnosti_udalenoj_autentifikacii (дата обращения: 02.01.2022).
12. Викторова В.С., Степанянц А.С. Модели и методы расчета надежности технических систем. М.: «ЛЕНАНД», 2016. – 256 с. URL: <https://lib-bkm.ru/13362> (дата обращения: 03.01.2022).
13. Гусев А.В., Романчев И.В. Резервирование – пути повышения надежности систем. *Труды Международного симпозиума «Надежность и качество»*. 2009, № 2, с. 186–187. URL: <https://elibrary.ru/item.asp?id=15601445> (дата обращения: 15.05.2022).
14. Galbally H.J., Ferrara P., Haraksim R., Psyllos A., Beslay, L. Study on Face Identification Technology for its implementation in the Schengen Information System. Luxembourg, Publications Office of the European Union, 2019. DOI: <https://doi.org/10.2760/661464>.

REFERENCES:

- [1] Vandana and N. Kaur. A Study of Biometric Identification and Verification System, 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2021, p. 60–64. DOI: <https://doi.org/10.1109/ICACITE51222.2021.9404735>.
- [2] Konyavskaya S.V. Besfaktornaya klassifikatsiya autentificiruyushchih dannyh: nachala postroeniya. *Kompleksnaya zashchita informacii: materialy HKHIV nauchno-prakticheskoy konferencii*. 2019, s. 194–200. URL: <https://www.okbsapr.ru/library/publications/kzi2019-konyavskaya/> (accessed: 06.01.2022) (in Russian).
- [3] Sabanov A.G. Kriterii doveriya k rezul'tatam identifikacii sub"ektov dostupa. *Elektrosvyaz'*. 2019, № 3, s. 38–44. URL: [aladdin-rd.ru/company/pressroom/articles/kriterii-doveria-k-rezultatam-identifikacii-subektov-dostupa](https://www.aladdin-rd.ru/company/pressroom/articles/kriterii-doveria-k-rezultatam-identifikacii-subektov-dostupa) (accessed: 02.01.2022) (in Russian).
- [4] Nídllová V., Hart J. Reliability of biometric identification using fingerprints under adverse conditions. *Agronomy Research*. 2015, № 13(3), p. 786–791. URL: https://agronomy.emu.ee/vol133/13_3_17_B5.pdf (accessed: 02.01.2022).
- [5] Sabanov A.G., Smolina S.G. Comparative analysis of personal identification biometry methods. *Trudy ISA RAN*. 2016, no. 66, p. 12–21. URL: http://www.isa.ru/proceedings/images/documents/2016-66-3/t-16-3_11-20.pdf (accessed: 02.01.2022) (in Russian).
- [6] Brumník Robert & Balantić Zvone. Reliability and Efficacy of Identification Systems and Supply Chain Management. *Strojniski Vestnik*. 2008, no. 54(11), p. 783–795. URL: https://www.researchgate.net/publication/290780033_Reliability_and_Efficacy_of_Identification_Systems_and_Supply_Chain_Management (accessed: 02.01.2022).

- [7] Butov A.V., Karyakin A.M. Problemy razvitiya biometrii kak osnovy cifrovizatsii otechestvennoj ekonomiki i puti ih resheniya. Izvestiya VUZov EFiUP. 2020, № 1(43), s. 48–52. URL: <https://elibrary.ru/item.asp?id=42654116> (accessed: 15.05.2022) (in Russian).
- [8] Garanin A.I. On the functional reliability of information systems. ITNOU: Informacionnye tehnologii v nauke, obrazovanii i upravlenii. 2018, № 2(6), p. 45–50. URL: <https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem> (accessed: 02.01.2022) (in Russian).
- [9] Shubinsky I.B. Nadezhnye otkazoustojchivye informacionnye sistemy. M.: «Journal Dependability», 2016. – 547 s. URL: <https://www.dependability.ru/jour/manager/files/books/%25D0%259A%25D0%25BD%25D0%25B8%25D0%25B3%25D0%25B0I.pdf> (accessed: 02.01.2022) (in Russian).
- [10] Sartasov S.Yu. Ocenka nadyozhnosti biometricheskikh sistem s nepreryvnoj klassifikaciej i mnozhestvennoj registraciej. Computer Tools in Education. 2013, № 4, s. 12–20. URL: <https://cyberleninka.ru/article/n/otsenka-nadyozhnosti-biometricheskikh-sistem-s-nepreryvnoj-klassifikatsiey-i-mnozhestvennoj-registratsiey> (accessed: 05.01.2022) (in Russian).
- [11] Sabanov A.G. Metody issledovaniya nadezhnosti udalenoj autentifikacii. Elektrosvyaz'. 2012, № 10, s. 20–24. URL: https://www.aladdin-rd.ru/company/pressroom/articles/metody_issledovania_nadezhnosti_udalenoj_autentifikacii (accessed: 02.01.2022) (in Russian).
- [12] Viktorova V.S., Stepanyanc A.S. Modeli i metody rascheta nadezhnosti tekhnicheskikh system. M.: «LENAND», 2016. – 256 s. URL: <https://lib-bkm.ru/13362> (accessed: 03.01.2022) (in Russian).
- [13] Gusev A.V., Romanchev I.V. Rezervirovanie – puti povysheniya nadezhnosti sistem. Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo». 2009, № 2, s. 186–187. URL: <https://elibrary.ru/item.asp?id=15601445> (accessed: 15.05.2022) (in Russian).
- [14] Galbally H.J., Ferrara P., Haraksim R., Psyllos A., Beslay, L. Study on Face Identification Technology for its implementation in the Schengen Information System. Luxembourg, Publications Office of the European Union, 2019. DOI: <https://doi.org/10.2760/661464>.

Поступила в редакцию – 26 февраля 2022 г. Окончательный вариант – 16 мая 2022 г.
Received – February 26, 2022. The final version – May 16, 2022.