**DOI 10.36622/1682-7813.2025.28.1.004**
**УДК 327:004.94**

# БИОМЕТРИЯ ЗАЩИТЫ ОБЪЕКТОВ: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ

**В.А. Минаев, К.М. Бондарь, В.Ю. Федорович**

В статье кратко изложено содержание недавней вышедшей в свет монографической работы коллектива авторов, посвященной развитию биометрической защиты объектов, включая задачи обеспечения информационной безопасности. В числе объектов рассмотрены документы, цифровые следы нарушений и преступлений, биометрические данные лиц в системах идентификации и аутентификации. В монографии обсуждены достижения и методология современных биометрических технологий, традиционной и перспективной защиты документов, создания комплексной биометрической модели распознавания личности, развития биометрических моделей и технологий в криминалистике и судебной экспертологии. Детальной оценке подверглись основы биометрических технологий; возможности маркирования документов в целях обеспечения их требуемой валидности; разработка комплексной биометрической модели распознавания личности, с помощью которой достигнута точностью около 99%; пути развития биометрической защиты объектов; направления и перспективы применения биометрических моделей и технологий в криминалистике и судебной экспертологии. Представленные в монографии научные результаты свидетельствуют о значимом вкладе авторов и перспективности их исследований в отношении биометрических подходов, моделей и технологий защиты объектов, противодействия современным угрозам в сфере противоправных деяний как по линии общеуголовной, так и киберпреступности.

Ключевые слова: биометрическая защита объекта, биометрические характеристики человека, маркирование документа, биометрическая модель распознавания личности, криминалистика, судебная экспертология.

## Введение

В конце 2024 года в издательстве Дальневосточного института МВД России имени И. Ф. Шилова вышла в свет монография «Биометрическая защита объектов» [1], раскрывающая сложившиеся представления и перспективные суждения о современных направлениях научно-практических разработок в области обеспечения безопасности – развитии биометрии защиты объектов (рис. 1).

Обращение к разнообразному перечню статических и динамических биометрических признаков человека обусловлено их объективной, природной уникальностью, относительной доступностью в практическом и технологическом смысле, способностью оперативно (в режиме реального времени) обеспечить идентификацию и аутентификацию личности, в том числе – в значительных людских потоках, например, в метро.

Практический аспект результатов проведенного исследования ориентирован на обеспечение информационной безопасности и ее актуальнейшей сферы – кибербезопасности, правоохранительную деятельность оперативных, следственных, экспертно-криминалистических и других подразделений, решающих задачи предупреждения правонарушений, раскрытия и расследования преступлений.

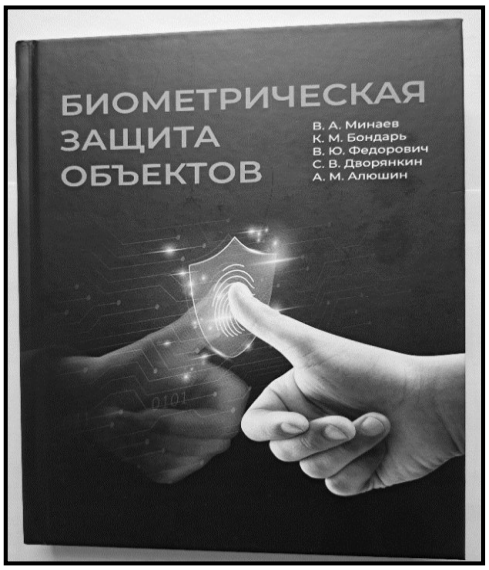


Рис.1. Обложка монографии «Биометрическая защита объектов»

На сегодняшний день имеется значительный по временным рамкам и вариантам практических приложений объем разработок, служащих противодействию деяниям противоправного характера в системах государственной, общественной и личной безопасности.

Приведем положения, определяющие логику развития обозначенной предметной области. Они систематизируют научные подходы, оценки, аналитические обзоры и иные научные формы, отраженные в [2-4] и других работах.

**Система биометрических технологий**

Биометрическое распознавание понимается как *система автоматической идентификации человеческой личности, основанная на оценке специализированными методами физиологических, биологических, биохимических характеристик или поведенческих факторов*, *а также на оценке комплекса этих характеристик.* Основные из них для иллюстрации приведены на рис. 2.

Для индивидуального распознавания человека используются следующие *физические* или *физиологические (статические)* характеристики: отпечатки пальцев, папиллярные узоры; рисунок сетчатки или радужной оболочки глаза; черты лица и их геометрия; голосовые параметры; рисунок вен ладони; запаховые следы; особенности геометрии ладоней.

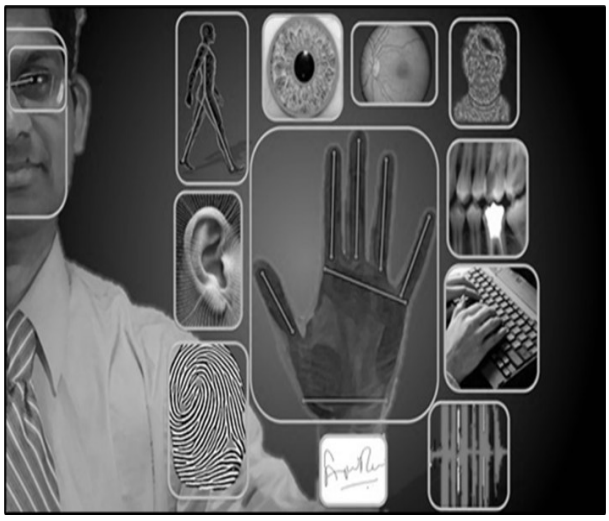

Рис. 2. Основные биометрические характеристики [1]

Перспективными считаются иные подходы, также связанные со статическими человеческими характеристиками: потовые выделения; геометрия ушной раковины; ДНК (в том числе – при анализе волос); особенности формы губ; особенности формы носа; зуб; осанки; термограмма лица.

К *поведенческим* (*динамическим*) характеристикам человека относятся особенности: походки; почерка и динамики подписи; манеры набора компьютерного текста; силы нажатия компьютерных клавиш; сердечного ритма; речевых параметров.

В современных разработках отмечаются и другие перспективные подходы:

- распознавание жестов;
- микровибрация пальцев;
- микродвижения;
- клавиатурный почерк – стилометрия;
- индивидуальные настройки компьютера.

Отмеченные аспекты биометрической идентификации систематизированы в монографии.

Пример комплексного применения ведущих технологий распознавания реализован в системе «Безопасный город», представленной в работе [5].

В указанной системе существует тревожное оповещение в случае обнаружения сходства биометрии лица с данными автоматизированных хранилищ. В ней видеопоток данных поступает с камер города Москвы (к началу 2025 г. их насчитывалось около двухсот тысяч с полным охватом административных единиц города) в Единый центр хранения и обработки данных. В Центре обеспечено надежное хранение видеозаписей и их эффективная аналитическая обработка.

При возникновении криминальной ситуации система видеонаблюдения фиксирует процесс совершения правонарушения, а также индивидов, в него вовлеченных. Это впоследствии становится доказательством по возбужденным уголовным делам, а также материалом для производства таких судебных экспертиз, как портретная, видео- и фототехническая.

Далее в монографии показано развитие процесса агрегирования биометрических сведений. В России это соответствует

созданию с 2010 года государственной единой биометрической системы (ЕБС). Важной особенностью функционирования ЕБС является обеспечение надежной безопасности хранимых данных на основе многоконтурной информационной защиты, распределения исходных биометрических сведений и опосредованного управления ими через портал Госуслуг.

Создание принципиально нового уровня информационной безопасности обусловлено текущими и потенциальными угрозами биометрическим данным. Так, в настоящее время «кража личности» считается одним из самых опасных киберпреступлений.

Дело в том, что в отличие от традиционных паролей, биометрические сведения и характеристики неотъемлемы от своего носителя и, следовательно, похищенный шаблон нельзя заменить новым, нескомпрометированным.

Подводя итог результатам современного развития, скажем, что технологии биометрической идентификации могут стать альтернативой (но не заменой) бумажным документам, карточкам, пропускам и пр.

Основными сферами использования биометрической идентификации являются банковские операции, бизнес, электронная торговля, безопасность (государственные, корпоративные, «умные» системы); аутентификация различных устройств; управление динамическими системами (например, потоками пассажиров в аэропортах).

Расширяются приложения в системах доступа, паспортного и пограничного контроля, в решении задач правоохранительных органов, обеспечении функционирования социальных объектов, образовательных учреждений и многих других.

При этом биометрические данные невозможно забыть или потерять, а сам факт их сбора базируется на условии физического присутствия человека на объекте защиты.

В монографии отмечены следующие перспективные направления.

*Обеспечение правоохранительной деятельности.* Биометрические технологии способны оказать значительную помощь в процессах предупреждения, раскрытия и расследования преступлений. В частности, в работе [6] детально оценены методы, технологии, примеры эффективной эксплуатации аналитических систем, ориентированных на современные и перспективные оперативные, следственные, криминалистические, профилактические задачи.

Данное направление сегодня требует разработки и внедрения методов использования искусственного интеллекта для биометрического анализа полученных сведений в целях дальнейшей постановки на криминалистические и оперативно-розыскные учеты, создания единой базы сведений о *цифровых следах*.

*Биометрическая защита объектов*. В монографии рассматриваются следующие объекты:

– документы разной направленности, содержания и форматов (бумажные и электронные). Особое внимание уделяется документам и информационным объектам в правоохранительной деятельности, фиксации различных видов следов, технологиям, которые поддерживают разведывательные и процессуальные действия;

– все виды следов правонарушений и преступлений, фиксацию статических и поведенческих характеристик лиц, совершивших криминальные деяния и подозреваемых в них;

– биометрические данные, вносимые в ЕБС идентификации и аутентификации, которые становятся все более привлекательными как объекты совершения современных видов киберпреступлений.

*Математическое обеспечение биометрических технологий.*

Подходы, алгоритмы и процедуры биометрической идентификации и аутентификации связаны с аналитической обработкой биометрических данных, их сравнения с идентификаторами пользователей на основе самых современных математических методов и моделей.

В связи с этим выделены следующие основные направления математического обеспечения:

– описание функционирования конкретного прибора или устройства биометрической идентификации;

– подтверждение гипотез при сравнительном исследовании методов биометрической идентификации и определении направлений дальнейшей разработки, организации противодействия попыткам компрометации;

– моделирование биометрической идентификации. Создание и практическое приложение моделей ориентируется на имитационную поддержку принимаемых решений (стратегических, тактических, оперативных).

В каждом из указанных направлений отмечаются элементы развития, совершенствования применяемых методов, изменения алгоритмической составляющей.

**Комплексная биометрическая модель распознавания личности**

Тенденция к интеграции различных биометрических характеристик позволила обозначить авторам монографии такой новый подход, как комплексная биоподпись [3].

В этих целях предлагается передача в составе биоподписи (БП) информации о состоянии сердечно-сосудистой, нервной и дыхательной систем человека. Показано, что указанные биопараметры обеспечивают значительно большую достоверность оценки текущего состояния автора документа по сравнению с другими методами.

Применение предлагаемой технологии биомаркирования позволяет выявлять случаи неадекватного физического, психического и эмоционального состояния автора, а также состояния его принуждения к подписи и утверждения документа.

Для формирования изображений спектрограмм, которые содержат биометрические данные автора документа, применяется быстрое преобразование Фурье.

Проведенное авторами монографии сравнение показало преимущество биоподписи перед электронной и речевой подписями, штрих кодами, другими полиграфическими технологиями.

Авторы монографии акцентируют внимание на:

– интеграции речевых сообщений в технологии биометрической защиты [7];

– использовании фитнес-браслетов для сбора биометрической информации при синтезе биоподписи [2];

– противодействии киберугрозам на основе комплексной биометрической модели удаленной идентификации [4].

*Акустический анализ/синтез при биометрической защите документов* [7]. Здесь акцентируется внимание на авторской технологии, предназначенной для защиты и обработки информации акустического вида. Она связана с образным анализом-синтезом именно речевых сигналов (РС). Особенности указанной технологической платформы позволяют поддерживать разнообразный спектр подходов в области синтезированного создания (генерации), а также аналитического речепреобразования речеподобных сигналов (РПС).

Получаемые при этом РПС могут быть сформированы под систему заданных свойств речевой информации, определяемую спецификой того или иного способа голосового управления, обеспечения бесперебойной связи или организации ее безопасных режимов осуществления. Гибкость и значительный объем настраиваемых параметров отмеченной платформы служат перспективной базой эффективному выявлению фактов и противодействию развивающихся методов фальсификации на основе речевых сигналов.

Основной технологией данного подхода является последовательное преобразование вида «звук-изображение-звук». Оно трансформирует до образа узкополосой спектрограммы исходный звуковой РС. Выполняется данное первичное преобразование методами цифровой обработки. Затем осуществляется переход в волновую форму, но уже с требуемыми характеристиками. Следует подчеркнуть, что в исследуемой области также важно и апробировано обратное преобразование «изображение-звук-изображение».

Можно отметить успешность применения данной технологии в задачах идентификации говорящего, кодирования и компрессии речи, скремблирования, нейтрализации помех и искажений, противодействия атакам клонированным голосом, аудиостеганографии.

Как показывают исследования, современные системы верификации неустойчивы к спуфингу (кибератака, при которой мошенники маскируются под других людей или компании), реализуемому с помощью автоматического синтеза голоса.

Отмеченная возможность имитации относится к методам голосового клонирования. При этом реализуются возможности голосового изменения у конкретного человека до уровня голосового звучания другого человека. Созданный голосовой фрагмент должен отражать признаки голоса человека (натуральные, естественные, индивидуальные), под которого готовится имитация.

Традиционным при этом является обращение к пранкеру или пародисту, который напрямую выступает голосовым имитатором. Но в современном противоправном развитии в речевой обработке широко разворачиваются специализированные программно-технические средства (реального времени, отложенного режима, с операторным или программным управлением).

На фоне известных и применяемых криминалистических подходов выявления голосового подражания человеком, возникает решение сложных задач по обнаружению признаков в клонировании речи нейросетевыми способами. Пути данного глубокого исследования инициированы авторскими разработками, частично приведенными в монографии.

В этих целях в ней подробно исследованы особенности создания угроз интерфейсам голосовой формации от разнообразных атак речевых клонов. Обращено внимание на следующие их разновидности, например: выявление артефактов и особенности экспертизы речевых клонов; следы включения/выключения записи; сохранение постоянства узкополосных гармонических канальных помех по времени; сохранение постоянства мелодии основного тона на длительных участках речевых вокализмов; линейность движения формант; вокодерные признаки в составе искусственной речи; тембральные искажения; мел-кепстральные искажения.

Авторы монографии формируют методику создания уникальных аудиомаркеров для подтверждения подлинности РС. В числе основных биометрических элементов подобного аудиомеркера выступают: отпечаток пальца, рукописная подпись, фото маркируемой личности.

*Биоподпись документов на основе информации от фитнес-браслетов* [2] связана с использованием последних в качестве средства сбора информации о конкретном индивиде. Полученная биометрия может быть внедрена в биоподпись пользователя. Такая возможность открывается на основе специального набора биопараметров, характеризующих состояние автора документа в момент его подписания либо утверждения.

При этом осуществляется анализ всей совокупности биопараметров, а также их сравнение с аналогичными биопараметрами, характерными для нормального состояния автора. Полученные сведения дают возможность выявлять неадекватное поведение, в том числе – получение подписи под принуждением, либо под воздействием наркотических веществ.

Наряду с традиционными биопараметрами (частота сердечных сокращений, артериальное давление, зрачковая реакция), анализировался тремор рук. В этих целях в монографии проанализировано применение фитнес-браслетов (ФБ), в состав которых включены акселерометр и гироскоп, позволяющие с достаточной точностью фиксировать тремор.

Функциональное достоинство предлагаемого подхода состоит в том, что ФБ, как правило, постоянно находится на руке. Это позволяет регистрировать биопараметры автора в момент работы с документом.

Технология биоподписи (БП) является развитием технологии речевой подписи (РП) документа. Суть реализации БП заключается в передаче в составе документа графического фрагмента, содержащего краткую речевую информацию о наиболее значимых аспектах документа. В качестве таких аспектов могут выступать важные даты, объемы

финансирования, перечень юридических и физических лиц, а также многое другое.

На физическом уровне этот способ защиты документов базируется на уникальности голоса его автора, который находится в специализированной базе данных. Технология дает возможность доступа к данной базе сторонних юридических и физических лиц при направлении документа с РП внешним потребителям.

Изображение спектрограммы РС автора при этом, как правило, используется в качестве графического фрагмента РП.

Технология дает возможность тиражировать документ, в который встроена РП. Это реализуется обычным полиграфическим оборудованием. Его функционал просто встраивает РП в форме графического фрагмента в любые элементы копий документов и даже в виде *цифровых водяных знаков*.

*Противодействие киберугрозам на основе комплексной биометрической модели* [4] связано с ее возможностью аутентифицировать человека при удаленном электронном обмене.

Авторами монографии решены задачи обоснования биометрических показателей личности, представления их в графическом формате, графической визуализации комплексной биометрической картины, включая спектральные характеристики сигналов.

Осуществлена разработка алгоритмов реализации комплексной модели в составе программно-аппаратного комплекса, на базе которого достигнуты значительные значения интегральной точности распознавания личности (не менее 99%). Это дает возможность ожидать существенного снижения киберугроз при реализации практических задач удаленного электронного обмена.

*Биометрия в криминалистике и судебной экспертологии.* Изучение биометрических характеристик человека, как важнейших источников значимой информации, осуществлялось на протяжении многих десятилетий.

В монографии выделены примеры применения биометрических технологий при решении задач криминалистической службы, отмечены хронологические вехи их развития.

Сделан вывод об отсутствии пока стройной системы в теоретических подходах и выработке конкретных рекомендаций по повышению эффективности биометрических систем в раскрытии и расследовании преступлений.

В МВД России, наряду с выполнением более полусотни текущих экспертиз (свыше 1,5 млн исследований в 2023 г.), ведется разработка и новых направлений, ориентированных на использование биометрических сведений.

Так, с 2019 г. разрабатывается методический и программно-аппаратный инструментарий по выявлению признаков монтажа видеоизображений, созданных нейронными сетями – дипфейков.

В фоноскопическом направлении эксперты определяют признаки использования специальных программных средств для изменения параметров голоса, создают правила и алгоритмы разграничения речи человека и бота.

В процессе фоноскопических и автороведческих исследований внедряются новые методы выявления синтезированной речи на фонограмме и признаки искусственной генерации текстов. Эксперты научились идентифицировать личность человека по текстовым сообщениям, созданным с помощью мессенджеров.

Развиваются технологии анализа массивов больших данных, распознавания образов, компьютерной экспертизы, видеоаналитики, дополненной и виртуальной реальности. Целями их использования является ускорение и повышение эффективности расследования преступлений, повышение точности осуществляемых судебных экспертиз, увеличение обоснованности и правомерности решений, принимаемых на этой основе.

Подчеркнем перспективность идентификация человека по характеристикам лица (нашли применение около 40 признаков). Она в биометрической сфере считается одним из динамично развивающихся направлений на базе антропологической реконструкции.

Особенностью развития технологии является ее взаимосвязь с функционированием габитоскопических специализированных автоматизированных информационно-поисковых систем, например: «Сова», «Портрет-Поиск», «Кримнет», «Портрет+», «Опознание», «Видеопоток» и иным.

Особый интерес представляют сведения о работе МВД России по формированию Федеральной базы данных геномной информации (ФБДГИ).

В монографии выделены и проанализированы основные направления в области защиты информации и других сферах деятельности, где биометрические технологии могут дать максимальный эффект:

– оперативное дистанционное визуальное распознавание (идентификация) с помощью систем интеллектуального видеонаблюдения;

– автоматизированные системы регистрации биометрических данных, индивидуализирующих человека;

– биометрическое удостоверение личности (например, биометрический паспорт);

– развивающиеся виды судебных экспертиз и исследований (например, судебно-фоноскопическая, ДНК-анализ);

– противодействие нелегальной миграции;

– предупреждение мошенничеств и других злоупотреблений в сфере электронной коммерции и банковской деятельности;

– автоматизированные системы розыска преступников (включая организованные трансграничные экстремистские группы, а также похищающих людей, работорговцев, занимающихся распространением оружия, взрывчатых веществ, наркотических средств).

В работе особое внимание уделяется роли цифровых следов в сфере экспертно-криминалистической деятельности, связанных с биометрической информацией.

Сформулировано понятие цифровых следов – *криминалистически значимая информация о любых действиях в цифровой среде, возникающих в процессе создания, обработки, хранения и передачи данных.*

Опуская криминалистический контекст, отметим, что указанное определение весьма точно характеризует отношения и в сфере информационной безопасности.

Сейчас эта сфера все активнее обогащается технологиями больших данных, их гармоничного сочетания с алгоритмами интеллектуальной обработки информации, все в большей мере применяются поисковые, информационно-аналитические, консультационные и иные системы, в том числе – базирующиеся на обработке биометрических данных.

Отмечается, что применяемые при этом технологии способны поддерживать решения задач поиска в ФБДГИ совпадений «след–лицо»; мониторинга с помощью систем интеллектуального видеонаблюдения траекторий движения лиц, автомобилей, иных объектов, представляющих интерес для правоохранительных органов; поиска повторяющихся последовательностей телефонных звонков (выявление группы связанных между собой лиц); обоснования следственных версий об использовании транспортных средств и разнообразного круга других насущных розыскных действий и аналитических обобщений.

При этом особо подчеркнем, что цифровые следы человека формируются и фиксируются разнообразными видами электронных устройств, в сферу действия которых он попадает. Ими выступают мобильные телефоны; смартфоны с поддержкой современных приложений; ноутбуки, нетбуки, планшеты и иные малогабаритные компьютеры; электронные гаджеты (например, многофункциональные электронные часы, пульсомеры, шагомеры и т.п.); видеокамеры различных систем наблюдения, автомобильные регистраторы, *GPS*-навигаторы и многие другие.

Из сказанного следует, что выявление цифровых следов, по сути, предполагает и мониторинг социальных сетей. Поэтому в монографии подчеркивается необходимость комплексного обращения к мониторинговым системам и технологиям аналитической разведки *OSINT (Open Source INTtelligence)*, способным дополнять разведывательные возможности по выявлению и анализу материалов оперативного интереса.

В организационно функциональном исполнении таких систем и технологий должны быть реализованы принципы:

– сбора данных о максимально возможном количестве реальных акторов;

– сбора данных о сетевой активности многих десятков тысяч аккаунтов;

– хранения данных в собственном огромном надежно защищенном хранилище, а не на компьютере конечного пользователя;

– обработки пользовательских запросов на основе собственных алгоритмов.

Системы данного класса имеют существенные особенности эксплуатации:

– полнота анализируемой информации не ограничивается заранее известными объектами;

– распределенный сбор данных значительно снижает вероятность идентификации мониторинга;

– затруднено определение объектов интереса или их признаков со сторонних структур;

– доступ к опубликованному контенту, который затем удален;

– реализация технологии анализа информации об активности объекта интереса;

– получение информации о связях объектов интереса, у которых профили защищены.

Совокупность отмеченных и иных технологических возможностей создает базу для существенного повышения эффективности выявления и сбора доказательств по нарушениям кибербезопасности за счет гибкого и оперативного получения информации (запросы выполняются в течение нескольких минут).

Очевидно, что системы мониторинга на основе больших данных представляют собой инструмент, который позволяет быстро находить перспективные материалы и более оперативно решать многие задачи анализа, предоставляет принципиально новые возможности по выявлению цифрового портрета нарушителей киберсферы, в том числе – с привлечением биометрических сведений.

Поддержка работы указанной системы должна основываться на применении передовых технологий информационно-аналитического характера (больших данных, моделирования, искусственного интеллекта).

**Заключение**

Таким образом, в статье представлены ключевые положения, изложенные в монографии «Биометрическая защита объектов». В ней рассмотрены результаты многолетней исследовательской работы коллектива авторов по систематизации подходов, внедрению методов использования биометрических сведений в целях повышения эффективности защиты объектов и обеспечения кибербезопасности, раскрытия и расследования преступлений, их профилактики.

Изложены новые методы защиты документов, биометрических следов правонарушений, а также биометрических данных лиц, зафиксированных в системах аутентификации и идентификации.

Детальной оценке подверглись современные составляющие предметной области: основы биометрических технологий; возможности маркирования документов в целях обеспечения их требуемой валидности; разработка комплексной биометрической модели распознавания личности с точностью не менее 99%; пути развития биометрической защиты объектов; направления и перспективы применения биометрических моделей и технологий в криминалистике и судебной экспертологии.

Представленные в монографии научные результаты свидетельствуют о значимом вкладе авторов и перспективности их исследований в отношении биометрических подходов, моделей и технологий защиты объектов, противодействия современным угрозам в сфере противоправных деяний как по линии общеуголовной, так и киберпреступности.

**Список литературы**

1. Минаев В. А., Бондарь К. М., Федорович В. Ю., Дворянкин С. В., Алюшин А. М. Биометрическая защита объектов: Монография / Под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: РИО ДВЮИ МВД России имени И. Ф. Шилова, 2024. – 284 с.

2. Алюшин А. М., Дворянкин С. В. Анализ перспектив использования фитнес-

браслетов в качестве источника биометрической информации при синтезе биоподписи важного документа // Безопасность информационных технологий = IT Security. 2024. Т. 31. № 1. – С. 63–74.

3. Минаев В. А., Дворянкин С. В., Алюшин А. М. Методы биомаркирования защищаемых объектов // Информация и безопасность. 2023. Т. 26. Вып. 3. – С. 321–328.

4. Минаев В. А., Федорович В. Ю., Дворянкин С. В., Алюшин А. М. Удаленная аутентификация на основе комплексной цифровой биометрической модели как метод противодействия киберугрозам // Актуальные проблемы внедрения цифровизации, обеспечения информационной безопасности и противодействия киберпреступности: Материалы Международной научно-практической конференции. 30 ноября 2023 г. Алматы. Алматы: Алматинская академия МВД Республики Казахстан имени Макана Есбулатова, 2023. – С. 56–62.

5. Бондарь К. М., Дунин В. С. Поисковая техника, средства контроля и досмотра: Учебно-практическое пособие (Изд. 2-е, доп., переработанное). Хабаровск: ДВЮИ МВД России, 2022. – 156 с.

6. Минаев В. А., Федорович В. Ю., Бондарь К. М., Поликарпов Е. С., Рабчевский Е. А. Сетевая деструктивная информация: поиск и противодействие: Монография. М.: МосУ МВД России, 2024. – 346 с.

7. Дворянкин С. В. и др. Защита информации, речевая информация, речевой сигнал, речеподобный сигнал, образный анализ-синтез / Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики: Монография / Коллектив авторов. М.: КНОРУС, 2021. – С. 224–259.

Московский университет МВД России им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia named after V.Ya. Kikot

Дальневосточный юридический институт МВД России имени И.Ф. Шилова
Far Eastern Law Institute of the Internal Affairs Ministry of Russia named after I.F. Shilov

Поступила в редакцию 15.01.25

**Информация об авторах**

**Минаев Владимир Александрович** – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, e-mail: m1va@yandex.ru

**Бондарь Константин Михайлович** – канд. техн. наук, доцент, профессор кафедры информационно-технического обеспечения ОВД Дальневосточного юридического института МВД России имени И.Ф. Шилова, e-mail: bondar_km@mail.ru

**Федорович Василий Юрьевич** – канд. юрид. наук, доцент, заместитель начальника по науке, Московский университет МВД РФ им. В.Я. Кикотя, e-mail: fevur@yandex.ru

# OBJECT PROTECTION BIOMETRICS: OPPORTUNITIES AND PROSPECTS

**V.A. Minaev, K.M. Bondar, V.Yu. Fedorovich**

The article summarizes the content of the recent published monographic work by a team of authors devoted to the development of biometric protection of objects, including the tasks of ensuring information security. The objects included documents, digital traces of violations and crimes, and biometric data of individuals in identification and authentication systems. The monograph discusses the achievements and methodology of modern biometric technologies, traditional and prospective document protection, the creation of a comprehensive biometric model for personality recognition, the development of biometric models and technologies in criminology and forensic expertise. The basics of biometric technologies were subjected to a detailed assessment; the possibility of labeling documents in order to ensure their required validity; the development of a comprehensive biometric model of identity recognition, which achieved an accuracy of at least 99%; ways of development of biometric protection of objects; directions and prospects of application of biometric models and technologies in criminalistics and forensic expertise. The scientific results presented in the monograph testify to the significant contribution of the authors and the prospects of their research in relation to biometric approaches, models and technologies for protecting objects, countering modern threats in the field of illegal acts both in the field of ordinary and cybercrime.

Keywords: biometric protection of object, biometric characteristics of a person, labeling of document, biometric model of personality recognition, criminalistics, forensic expertise.

Submitted 15.01.25

**Information about the authors**

**Vladimir A. Minaev** – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, V. Ya. Kikot Moscow University of the Internal Affairs Ministry, e-mail: m1va@yandex.ru

**Konstantin M. Bondar** – Cand. Sc. (Technical), Professor of the Information and Technical Support Department of Internal Affairs Agencies of the Far Eastern Law Institute of the Internal Affairs Ministry of Russia named after I. F. Shilov, e-mail: bondar_km@mail.ru

**Vasily Yu. Fedorovich** – Cand. Sc. (Law), Associate Professor, Deputy Head of Science, Kikot Moscow University of the Ministry of Internal Affairs of the Russian Federation, e-mail: fevur@yandex.ru