Цифровая биометрия в управлении организацией

Digital biometrics in organizational management

УДК 005.93
Получено: 20.04.2026 Одобрено: 22.05.2026 Опубликовано: 25.06.2026

Бурлака С.Н.
Старший преподаватель кафедры предпринимательского права, ФГБОУ ВО «Уральский государственный экономический университет», г. Екатеринбург
e-mail: snburlaka@mail.ru

Burlaka S.N.
Senior Lecturer Department of Business Law, Ural State University of Economics, Yekaterinburg
e-mail: snburlaka@mail.ru

Бельдина О.Г.
Старший преподаватель кафедры гражданского права, ФГБОУ ВО «Уральский государственный экономический университет», г. Екатеринбург
e-mail: bfog@mail.ru

Beldina O.G.
Senior Lecturer Department of Civil Law, Ural State University of Economics, Yekaterinburg
e-mail: bfog@mail.ru

Аннотация
Цифровая биометрия сегодня – это инструмент, кардинально изменяющей способы идентификации личности, возможности получения доступа к множеству услуг, в том числе государственных. Использование цифровой биометрии – один из ключевых факторов глобальной цифровизации всех сфер общественной жизни. В отличие от обычных персональных данных, биометрические персональные данные относятся к категории сведений повышенной чувствительности, поскольку позволяют идентифицировать человека на основе уникальных, неизменяемых, присущих только ему характеристик. В силу этого законодательное регулирование применения биометрии в организациях носит более жесткий характер, предусматривает более строгие требования к обработке, хранению и защите. Параллельно в настоящий момент идет планомерное усиление надзорной практики со стороны отраслевых регуляторов. В статье рассматриваются проблемы адаптации организаций к новым правилам регламентирования, а также устанавливаются алгоритмы законного внедрения систем, работающих с биометрическими персональными данными. В статье впервые комплексно рассматриваются правовые, технологические и финансовые аспекты использования биометрических персональных данных в управлении организацией. Проанализированы затраты на создание защищённой инфраструктуры, экономические выгоды от автоматизации, риски утечек и штрафов, а также показатели окупаемости. Предложен алгоритм экономически обоснованного и законного внедрения биометрии.
Ключевые слова: цифровая биометрия, цифровые технологии, цифровизация, Единая биометрическая система, персональные данные, управление организацией, экономическая эффективность, затраты на биометрию.

Abstract
Digital biometrics today is a tool that is fundamentally changing the methods of personal identification and access to a variety of services, including government services. The use of digital biometrics is a key factor in the global digitalization of all spheres of public life. Unlike regular personal data, biometric personal data is classified as highly sensitive information, as it allows for the identification of an individual based on unique, immutable, and inherent characteristics. Therefore, legislative regulation of the use of biometrics in organizations is more stringent, imposing stricter requirements for processing, storage, and protection. At the same time, industry regulators are systematically strengthening their oversight practices. The article comprehensively examines, for the first time, the legal, technological and financial aspects of using biometric personal data in organizational management. It analyzes the costs of creating a secure infrastructure, the economic benefits of automation, the risks of data leaks and fines, as well as payback indicators. An algorithm for economically justified and lawful implementation of biometrics is proposed.
Keywords: digital biometrics, digital technologies, digitalization, Unified Biometric System, personal data, organization management, subject of biometric personal data, economic efficiency, biometric costs.

Введение

В условиях глобальной цифровизации институционной среды в нашей стране активно развивается применение цифровой биометрии, кардинально изменяющей способы идентификации личности. Цифровая биометрия сегодня – это инструмент получения доступа к множеству услуг, в том числе государственных. В России в соответствии с Федеральным законом от 29.12.2022 N 572-ФЗ действует Единая биометрическая система (ЕБС). Единая биометрическая система является государственной платформой, позволяющей идентифицировать гражданина удаленно по его биометрическим данным. Основными задачами ЕБС являются подтверждение личности без предъявления паспорта; удаленное оформление услуг; усиление цифровой безопасности и т.д. Внедрение новых технологий получило широкое распространение при открытии счета или оформления кредита в банке; получения электронной подписи; заселения в гостиницу без паспорта; оплаты проезда в метро; регистрации бизнеса; получения сим-карты и т.д. Биометрические системы превосходят человеческие способности по точности распознавания лиц и голосов. Например, операционисты банков редко замечают различия между близнецами, тогда как специальные алгоритмы делают это почти наверняка.

При этом с 30 мая 2025 г. в России действуют ужесточённые штрафы за нарушения законодательства в сфере использования и обработки биометрических персональных данных. Параллельно в настоящий момент идет планомерное усиление надзорной практики Роскомнадзора и отраслевых регуляторов, что привело к формированию жёсткого правового режима обработки биометрии. У работающих с биометрией организаций стало больше обязанностей по обеспечению правомерности обработки данных, защиты информационных систем и выполнению процедур по взаимодействию с Единой биометрической системой.

При этом необходимо уточнить, что в российской науке применение технологий цифровой биометрии стало изучаться довольно недавно. Можно выделить труды Рудаковой О.С., Юсупова О.Р., Корнева Л.В., Абдуллаев Э.А., Трифонова М.А., Карцана И.Н. и т.д. Экономическая сторона внедрения биометрии – структура затрат, источники экономии, оценка рентабельности, влияние на финансовые результаты - остаётся малоизученной, что создаёт риск неоправданных инвестиций или, напротив, отказа от выгодных технологий.

Цель и методологическая база исследования

Цель исследования - разработать комплексный подход к внедрению цифровой биометрии в управление организацией, объединяющий юридические, технические и экономические требования. В рамках цели поставлены следующие задачи:

– установить принципы законного использования биометрических персональных данных (правовой блок);

– определить архитектуру безопасной обработки биометрии (технический блок);

– оценить экономические эффекты: затраты (CAPEX, OPEX), выгоды (снижение издержек, рост выручки), риски (утечки, штрафы) и показатели окупаемости (экономический блок).

Методологическая база исследования. Методологической основой исследования явились работы российских ученых, занимающихся изучением внедрения цифровых технологий в управление организациями. Использованы методы: сравнительного и логического анализа, статистический, аксиологический – дополненные экономическими методами: расчёт совокупной стоимости владения (TCO), анализ затрат-выгод (CBA), дисконтирование денежных потоков (Payback Period), оценка вероятностных рисков.

Основные результаты исследования

В 2025 г. россияне совершили более 146 млн платежей с использованием биометрии и доля таких платежей неуклонно растет. Использование биометрических персональных данных стало частью глубокой прошивки массовых бизнес процессов. Можно сказать, что они сформировали новые технологические нормы в управлении организациями, в частности, при распознавании лиц в системах контроля доступа, аналитических платформах видеонаблюдения, сервисах идентификации клиентов, таких как опция «оплаты улыбкой», разблокировка с помощью отпечатков пальцев или скан ладони.

В соответствии со ст. 11 Федерального закона № 152-ФЗ «О персональных данных» биометрические персональные данные — это «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных». В отличие от обычных персональных данных, биометрия относится к категории сведений повышенной чувствительности, поскольку позволяет не просто идентифицировать человека, а делает это на основе уникальных, неизменяемых характеристик [1]. В силу этого законодатель выделяет биометрию в отдельную категорию, предусматривающий более строгие требования к обработке, хранению и защите.

К биометрическим данным закон относит: изображение лица, включая фото - и видеоматериалы, применяемые в алгоритмах распознавания; рисунок радужной оболочки и сетчатки глаза; отпечатки пальцев и ладоней; образцы голоса, позволяющие автоматически идентифицировать человека; иные уникальные характеристики, обеспечивающие возможность автоматизированного сравнения. Законодательно определены следующие виды размещения и обработки биометрических персональные данные в единой биометрической системе: изображение лица человека, полученное с помощью фотовидеоустройств; запись голоса человека, полученная с помощью звукозаписывающих устройств.

Не любое изображение, звук или физическая характеристика автоматически относится к цифровой биометрии. Для квалификации данных как биометрических необходимо одновременное соблюдение нескольких критериев [2]. В качестве первого критерия можно указать необходимость применения специальных технологий обработки. Так для отнесения данных к биометрии нужно, чтобы идентификация проводилась с использованием алгоритмов распознавания лиц, систем автоматического сравнения шаблонов (например, отпечатков пальцев), а также программно-аппаратных комплексов анализа голоса или иных параметров. Следующим критерием является соответствие определенным техническим требованиям, то есть данные должны быть пригодными для идентификации. Так, в частности, фотографии, используемые в системах распознавания лиц, должны соответствовать ГОСТ Р ИСО/МЭК 19794-5, а аудиозаписи для голосовой идентификации должны иметь параметры, позволяющие системе корректно выделить биометрический шаблон и т.д. [3]. Таким образом, можно сделать вывод, что не любые характеристики человека являются биометрическими, а только те, которые могут быть использованы системой идентификации в соответствии с заданными стандартами.

Неправильная квалификация относимости персональных данных к биометрическим влечёт не только избыточные процессы в управлении организацией (излишние согласия и меры защиты), так и риски нарушения законодательства [4]. Так в соответствии с разъяснениями Роскомнадзора и судебной практикой к биометрическим данным не относятся:

– фотографии в личных делах сотрудников, если фото используется только в кадровом документообороте и не применяется для автоматизированной идентификации, оно не является биометрией;

– изображение лица вне рамок превращения его в шаблон и применения алгоритмов распознавания;

– видеонаблюдение или факт съемки лица без его биометрической обработки системами распознавания лиц;

– подпись и почерк вне контекста биометрического анализа;

– скан паспорта без анализа лица, сканирование документа ради подтверждения факта его предъявления не превращает автоматически изображение в биометрические данные.

Крайне важно выделить критерии разграничения между обычным видеонаблюдением и системой, работающей с биометрией [5]. Так обычное видеонаблюдение не образует обработки биометрических персональных данных, если: камеры используются для общей безопасности, контроля обстановки, расследования инцидентов; система не распознаёт лица автоматически, не формирует и не хранит биометрические шаблоны; цель обработки не включает идентификацию конкретных лиц. И в таком случае вполне достаточно информационных табличек о видеосъёмке в зоне наблюдения; локального акта о видеонаблюдении, регламентирующего цели, порядок доступа к записям, сроки хранения; факта ознакомления сотрудников с локальным актом под подпись. Но правовой режим в значительной мере трансформируется при получении системой функций аналитики и распознавания лиц. В этом контексте можно выделить следующие наиболее распространённые ошибки организаций: внедрение «умных» камер и модулей видеоаналитики без пересмотра правового режима и локальных нормативных правовых актов (формально компания считает, что у неё «просто видеонаблюдение»); использование видеозаписей для распознавания лиц задним числом без изменения правовой квалификации обработки и без получения согласий субъектов персональных данных.

Использование цифровых биометрических технологий автоматически означает, что организация находится в зоне повышенного внимания со стороны надзорных органов. Можно выделить несколько основных ключевых правил применения цифровой биометрии в управлении юридическими лицами. Необходимость их соблюдения обусловлена спецификой биометрических данных. Для обеспечения соответствия требованиям законодательства важна определенность в последовательности действий, поскольку юридическая, организационная и техническая части процесса тесно связаны между собой. В первую очередь корректная работа с биометрическими персональными данными начинается с квалификации данных [6]. Организация обязана установить, используется ли информация для автоматизированной идентификации. После определения факта обработки биометрии формируются цели. Они должны быть конкретными, измеримыми и отражёнными в локальных нормативных актах: контроль доступа, учёт рабочего времени, дистанционная идентификация клиентов, безопасность объекта. Комплаенс внутренних документов организации обязан содержать описание состава данных, процессы их передачи, роли сотрудников и технические меры защиты.

В качестве следующего этапа механизма работы с биометрическими данными является получение согласия субъектов. В первую очередь, необходимо выделить требование к однозначности воли субъекта. если оператор использует данные для идентификации, то согласие должно отражать именно эту цель. Надзорная практика показывает, что нарушение именно этого блока требований чаще всего приводит к претензиям со стороны регулятора. Исходя из положений Федерального закона № 152-ФЗ системы контроля

и управления доступом с распознаванием лица всегда работают с биометрическими персональными данными. Это означает, что такие системы должны рассматриваться как контуры обработки биометрических персональных данных независимо от числа сотрудников и масштаба объекта. При этом обработка таких данных допускается только при наличии письменного согласия субъекта с чётким указанием вида данных (изображение лица, шаблон, параметры) и целей (доступ на объект, учёт рабочего времени и т. п.). При этом для работников должны быть предусмотрены иные варианты, чтобы отказ от биометрии не приводил к ограничению их трудовых прав. Для посетителей, не согласных на использование биометрии, также требуется альтернативный механизм доступа (карта-пропуск, PIN-код, визуальная проверка документа) [7]. В контексте этих требований можно выделить такие типичные нарушения как: отсутствие отдельного согласия именно на биометрическую обработку (биометрия часто «спрятана» внутри общего согласия на обработку персональных данных); локальное хранение биометрических шаблонов в системах контроля и управления доступом без учёта требований законодательства и без оценки риска утечки биометрических персональных данных; отсутствие альтернативных способов доступа, то есть фактическое принуждение к сдаче биометрии. Хранение биометрических данных должно быть обособленным. Биометрические шаблоны не могут находиться в тех же массивах данных, что и кадровые сведения или общие клиентские базы. Для них выделяется отдельный сегмент с ограниченным доступом, применением сертифицированных средств защиты, контролем целостности и защищёнными каналами связи.

В тех случае если обработка биометрических персональных данных осуществляется частично силами подрядчика, требуется юридически корректно оформленное поручение. В договоре фиксируются перечень операций, требования к защите данных, уровни ответственности, режим уничтожения информации и обязательства по соблюдению законодательства [8]. При обработке биометрии в обязательном порядке необходимо учитывать права субъекта. Человек может возразить против обработки, потребовать исключения биометрических шаблонов, запросить сведения о хранении данных либо потребовать их уничтожения. Информационные системы должны предусматривать возможность выполнения таких операций, а внутренние процедуры содержать чёткий регламент их обработки.

Следующим ключевым элементом архитектуры обращения с биометрией является обязательное раздельное хранение данных [9]. Биометрические шаблоны должны храниться в Единой биометрической системе. Такой механизм не оставляет возможности сохранять шаблоны в локальных корпоративных системах. При этом действия по загрузке биометрии должны фиксироваться и выполняться уполномоченным сотрудником с использованием усиленной квалифицированной электронной подписи. Оператор обязан использовать стандартизированную форму согласия, доступную в электронном виде, и обеспечивать юридическую значимость всех операций, включая отзыв согласия, уведомления и уничтожение данных. Крайне важным здесь является наличие механизма возражения, то есть субъект может заблокировать размещение данных в Единой биометрической системе, а оператор обязан обеспечить такую возможность. Эта процедура влияет на настройки всего жизненного цикла данных, на механизмы удаления и блокирования шаблонов, а также маршрутизацию таких запросов. Для организаций, которые работали с биометрией до вступления закона в силу, предусмотрены два алгоритма поведения: конвертировать и перенести данные в ЕБС либо уничтожить их при невозможности переноса. Это требует ревизии всех источников биометрии внутри юридического лица.

Механизм управления архитектурой цифровых процессов в организации изменяется если юридическое лицо принимает решение отказаться от биометрических технологий или не использовать механизмы взаимодействия с ЕБС. В таком случае необходимо прекращение сбора биометрических данных, то есть отключение функций распознавания, остановка записи шаблонов и отказ от режимов, предполагающих машинную идентификацию. На смену биометрии вводят очные инструменты распознавания, такие как визуальная проверка

документов, пропускные карты, PIN-коды. Далее подлежат уничтожению ранее собранные биометрические данные, если их перенос в ЕБС не планируется и не требуется законом [10]. Уничтожение проводится с обязательным оформлением актов, с фиксацией ответственных лиц и использованием технологии удаления биометрических персональных данных. Федеральный закон № 152-ФЗ «О персональных данных» предусматривает обязанность оператора уведомить Роскомнадзор о прекращении обработки отдельных категорий данных и подтвердить ликвидацию соответствующих массивов.

Следующим важнейшим звеном архитектуры работы с биометрией является техническое сопровождение данного процесса. Как уже указывалось ранее Федеральный закон № 572-ФЗ закрепил модель, в которой биометрические шаблоны и сведения о личности физического лица хранятся раздельно. Шаблоны размещаются в Единой биометрической системе, а идентификационные сведения - в Единой системе идентификации и аутентификации. Такой механизм исключает возможность объединения критически важных данных в одном информационном массиве и снижает риски доступа к полному профилю субъекта. Для раздельного хранения организациям необходима точная маршрутизация данных без смешения информационных потоков. Ошибки в этой части приводят к нарушению требований ФЗ-572 и создают угрозу компрометации данных [11,12]. Поэтому в организации должны предусматриваться отдельные механизмы отправки, шифрования и подтверждения загрузки, а также ведение журналов действий уполномоченного сотрудника.

Передача биометрических данных обязательно должна производиться по защищенным каналам связи. Подключение осуществляется через криптографические шлюзы уровня КС3, обеспечивающие конфиденциальность, аутентичность, целостность и не корректируемость информационных потоков. Такие шлюзы должны быть сертифицированы по требованиям к средствам криптографической защиты и соответствовать установленным алгоритмам. Внутри корпоративной сети передача данных должна осуществляться по выделенным защищенным сегментам. Это позволяет минимизировать риски перехвата, ограничить круг маршрутов, по которым может передаваться биометрический шаблон, и обеспечить контроль над узлами, участвующими в обработке [13]. Таким образом, архитектура технического сопровождения применения цифровой биометрии в организации включает в себя несколько основных правил: разграничение сетевых зон, через которые проходит биометрия; использование шифрования данных не только при передаче, но и при хранении; обеспечение мониторинга каналов связи и регистрация аномалий; исключение маршрутизации биометрии через общие корпоративные тоннели.

Также существуют требованиям к сегментам обработки биометрии. Сегмент обработки биометрии рассматривается как изолированный контур с собственными правилами доступа и уровнем защищённости, который должен соответствовать установленным нормативам [14]. Сегмент должен обеспечивать невозможность прямого доступа к шаблонам из внешних систем, включая внутренние корпоративные сервисы, если такая передача не предусмотрена регламентами. При подключении к Единой биометрической системе организация обязана иметь инструментарий, обеспечивающий:

– *Выделенный контур обработки.* Системы, которые работают с биометрическими шаблонами, изолируются на уровне сети, инфраструктуры и хранилищ. В этот контур не допускается оборудование, не соответствующее требованиям по защите информации, а доступ сотрудников жёстко контролируется. Сегмент не может быть объединён с обычными пользовательскими зонами или общими цифровыми ресурсами.

– *Использование сертифицированных средств защиты.* Требования к Единой биометрической системе предусматривают применение сертифицированных средств защиты информации: межсетевых экранов, систем предотвращения вторжений, средств доверенной загрузки, механизмов контроля целостности и криптографических средств.

– *Минимизация доступа.* Политика управления доступом выстраивается по принципу «минимально необходимого». Внутри контура определяются отдельные роли: администратор инфраструктуры, оператор загрузки данных, специалист по обеспечению безопасности.

Каждая роль получает строго ограниченные полномочия, а все операции фиксируются в журналах аудита, что является обязательным требованием законодательства.

Внедрение систем цифровой биометрии требует от организации не только соблюдения правовых и технических норм, но и тщательной экономической оценки. До настоящего времени в научной литературе преобладал юридический и технологический подход к биометрии, тогда как её финансовые последствия оставались недостаточно изученными. Между тем, любое решение о развёртывании биометрической инфраструктуры должно быть экономически обосновано: необходимо понимать структуру затрат, ожидаемые выгоды, возможные финансовые потери при нарушениях и сроки окупаемости.

Прежде всего, организация сталкивается с капитальными затратами (4,2 млн руб.). Они включают приобретение биометрических считывателей, например, сканеров отпечатков пальцев или трёхмерных камер распознавания лиц, стоимость которых варьируется от 15 до 50 тыс. руб. за единицу в зависимости от производителя и уровня защищённости. Кроме того, требуются выделенные серверы для изолированного контура обработки данных, сертифицированные средства криптографической защиты информации (например, шлюзы уровня КС3), а также лицензии на программное обеспечение распознавания, которые могут стоить от 500 тыс. руб. в год. Неотъемлемой частью CAPEX являются расходы на интеграцию с Единой биометрической системой и Единой системой идентификации и аутентификации; такие работы в среднем оцениваются от 200 тыс. до одного миллиона рублей в зависимости от масштаба организации и сложности внутренних процессов.

Наряду с капитальными затратами возникают операционные расходы (OPEX). К ним относятся ежегодное продление лицензий и сертификатов, которое обычно составляет 20–30 процентов от первоначальных капитальных вложений. Существенную долю OPEX составляет заработная плата администраторов информационной безопасности и операторов загрузки биометрических данных: для средней компании требуется как минимум один специалист с годовым фондом оплаты труда около 1,2 миллиона руб. Дополнительно организация должна предусматривать расходы на регулярное обучение сотрудников правилам работы с биометрией, проведение внутренних и внешних аудитов, а также на страхование киберрисков. Страховой полис, покрывающий ущерб от возможной утечки биометрических персональных данных, может стоить от 100 тыс. руб. в год.

Однако затраты – это лишь одна сторона экономического баланса. Внедрение биометрии приносит организации прямые и косвенные выгоды. Прямая экономия выражается в сокращении издержек на ручную идентификацию и контроль. Например, система контроля и управления доступом с распознаванием лиц позволяет заменить несколько постов охраны: если в компании со штатом в 100–200 сотрудников ранее требовалось три охранника на проходной, то после автоматизации можно оставить одного оператора. Годовая экономия фонда оплаты труда в таком случае может достигать 2,5–3 миллионов руб. В розничной торговле и сфере услуг биометрическая оплата («оплата улыбкой», оплата отпечатком пальца) сокращает время обслуживания одного клиента в два-три раза, что увеличивает пропускную способность и позволяет обслужить больше покупателей без расширения штата кассиров. Для сети магазинов с ежедневным потоком 500 чел. и средним чеком 500 руб., дополнительная выручка за счёт ускорения расчётов может составить около 1,5 миллиона руб. в год.

Кроме того, биометрия снижает потери от мошенничества. В отличие от паролей или пластиковых карт, биометрические характеристики невозможно украсть и использовать повторно. Как показывает практика банковского сектора, внедрение биометрической идентификации клиентов при выдаче кредитов снижает число мошеннических операций на 15–20. Для среднего регионального банка это означает предотвращение убытков в размере 5–10 миллионов рублей ежегодно. Аналогичный эффект наблюдается в гостиничном бизнесе и на транспорте, где подделка документов становится практически невозможной.

Не менее важным экономическим фактором выступает избежание штрафов и компенсаций. С 30 мая 2025 г. в России действуют оборотные штрафы за утечку биометрических персональных данных - до трёх процентов годовой выручки организации, но

не более 15 миллионов руб. по ст. 13.11 Кодекса об административных правонарушениях. Даже единичное нарушение, например хранение биометрических шаблонов в локальной системе без передачи в Единую биометрическую систему или отсутствие письменных согласий сотрудников, грозит штрафом до 500 тыс. руб. на юридическое лицо. Соблюдение законодательства, напротив, позволяет избежать этих выплат, что следует рассматривать как предотвращённый убыток.

Однако экономический анализ был бы неполным без оценки рисков. Наиболее опасным событием является утечка биометрических данных. Поскольку в отличие от пароля отпечаток пальца или изображение лица невозможно сменить, компрометация таких данных создаёт пожизненный риск для субъекта и, соответственно, многомиллионные репутационные и судебные издержки для организации. Помимо административного штрафа, компания может столкнуться с исками от пострадавших граждан (типичная сумма компенсации морального вреда - от 50 до 100 тыс. руб. на одного человека), а также с падением выручки из-за потери доверия клиентов. Опыт последних лет показывает, что утечка биометрии в публичной компании приводит к снижению выручки на 5–10 процентов в течение полугода после инцидента.

Для иллюстрации экономической эффективности рассмотрим типичный кейс. Средняя организация со штатом 200 сотрудников и небольшим розничным направлением принимает решение о внедрении биометрической системы контроля доступа и оплаты по лицу. Экономические показатели можно увидеть в табл. 1.

Таблица 1

Экономические показатели внедрения биометрической системы в организации (на примере компании со штатом 200 сотрудников и розничным направлением)

Показатель	Значение
Капитальные затраты (CAPEX), млн руб.	4,2
Операционные затраты в год (OPEX), млн руб.	1,1
Экономия на охране (сокращение 3 постов), млн руб./год	2,7
Снижение потерь от мошенничества, млн руб./год	0,9
Дополнительная выручка за счёт скорости обслуживания, млн руб./год	1,5
Итого годовой экономический эффект, млн руб./год	5,1
Простой срок окупаемости (Payback Period), лет	0,82 (≈10 месяцев)

Примечание: расчет выполнен для организации, внедряющей биометрическую систему контроля доступа и оплату по лицу при условии полного соблюдения правовых и технических требований.

При этом чувствительность анализа показывает, что увеличение затрат на защиту (например, дополнительные 500 тыс. руб. CAPEX на усиленную криптографию) снижает вероятность утечки и полностью экономически оправдано.

Таким образом, экономическая составляющая внедрения цифровой биометрии не сводится к простому сличению расходов и доходов. Она требует многофакторного анализа, включающего прямые и косвенные выгоды, вероятностные риски и стоимость отказа от автоматизации. На основе проведённого исследования можно сформулировать следующие рекомендации: во-первых, каждому проекту внедрения биометрии должен предшествовать расчёт совокупной стоимости владения и анализ затрат-выгод; во-вторых, в бюджет необходимо закладывать резерв на киберстрахование и усиленную техническую защиту; в-третьих, целесообразно применять поэтапное внедрение с пилотным проектом на ограниченном участке, что позволяет минимизировать финансовые потери при возможных ошибках. Только такой подход обеспечивает экономическую обоснованность биометрических решений наряду с их правомерностью и технической надёжностью.

Выводы

В современных реалиях биометрия вышла из разряда ИТ-проектов, сегодня это новая социальная инфраструктура. Биометрические персональные данные используются для подтверждения личности, но в отличие от обычных идентификаторов, биометрические данные нельзя сменить. Это делает их особенно уязвимыми при утечках. Развитие биометрических технологий сопровождается последовательным ужесточением регулирования, что отражает общую тенденцию повышения требований к обработке данных, способных однозначно идентифицировать человека. В результате организации, внедряющие биометрию, оказываются в зоне повышенного контроля, где отступления от установленного порядка неизбежно создают юридические и технические риски.

Таким образом, для обеспечения соответствия требованиям законодательства важно соблюдать алгоритм последовательности действий, поскольку юридическая, организационная и техническая части процесса тесно связаны между собой. В первую очередь корректная работа с биометрическими персональными данными начинается с квалификации данных. Организация обязана установить используется ли информация для автоматизированной идентификации. Следующим этапом механизма работы с биометрическими данными является получение согласия субъектов. Здесь необходимо выделить требование к однозначности воли субъекта, если оператор использует данные для идентификации, то согласие должно отражать именно эту цель. При этом для работников должны быть предусмотрены альтернативные варианты, чтобы отказ от биометрии не приводил к ограничению их трудовых прав. Следующим ключевым элементом архитектуры обращения с биометрией является обязательное раздельное хранение данных. Биометрические шаблоны должны храниться в Единой биометрической системе. Такой механизм не оставляет возможности сохранять шаблоны в локальных корпоративных системах. Шаблоны размещаются в Единой биометрической системе, а идентификационные сведения - в Единой системе идентификации и аутентификации. Такой механизм исключает возможность объединения критически важных данных в одном информационном массиве и снижает риски доступа к полному профилю субъекта. Проведённый экономический анализ показывает, что внедрение биометрии при соблюдении правовых и технических требований является финансово оправданным. Капитальные затраты окупаются в среднем за 10–12 месяцев за счёт сокращения расходов на охрану, снижения мошенничества и роста выручки от ускорения обслуживания. Однако несоблюдение законодательства (локальное хранение шаблонов, отсутствие согласий) влечёт риски оборотных штрафов до 15 млн руб. и репутационных потерь, которые могут свести на нет любой положительный эффект. Таким образом, экономическая эффективность биометрии достигается только при комплексном учёте юридических, технических и финансовых факторов. Необратимость биометрии определяет её статус как критически важной категории данных и требует от организаций особой точности при проектировании управленческих процессов и выборе технологических решений.

Литература

1. Бершадская Е.Г., Маркин Е.И., Мартышкин А.И. Методы идентификации личности по изображению лица // XXI век: итоги прошлого и проблемы настоящего плюс. - 2020. - Т. 9. - № 1 (49). - С. 49-53.
2. Исраелян А.М., Исраелян Г.М., Климова Д.Н. Нейросетевые методы идентификации человека по изображению лица //Актуальные научные исследования в современном мире. - 2021. - № 11-12 (79). - С. 111-114.
3. Абдуллаев Э.А. Будущее паролей: заменят ли их биометрические технологии // Молодой ученый. - 2025. - № 7 (558). - С. 4-6.
4. Абламейко М.С., Шакель Н.В., Богуш Р.П. Использование систем искусственного интеллекта при обеспечении общественной безопасности в «Умном городе»: юридические аспекты // Вестник Полоцкого государственного университета. - 2021. - № 2021. - С. 84-92.

5. Бутко Г.П., Меньшикова М.А., Панов М.А. Пути совершенствования цифровых инструментов в деятельности предприятий// Цифровые модели и решения - Т.3.- № 1. - 2024. С.39-48.
6. Ткаченко И.Н., Метелева М.А. Структурные элементы и результативность систем управления предпринимательской деятельностью корпораций// Управленец. - Т.15.- № 5. - 2024.- С. 38-55.
7. Рудакова О.С. Перспективы внедрения технологии биометрической идентификации в банковской сфере // Молодой ученый. - 2020. - № 31 (321). - С. 78-82.
8. Воронов А.С., Орлова Л.Н., Шамолин М.В. Кибербезопасность в системе приоритетов национальной безопасности // Journal of New Economy. - Т.26.- № 4.- 2025. - С. 6-24
9. Крылова И.Ю., Рудакова О.С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике// Молодой ученый. - 2018. - № 45 (231). - С. 74-79.
10. Корнев Л.В. Методы биометрии при обеспечении информационной безопасности// Молодой ученый. - 2022. - № 17 (412). - С. 358-361.
11. Бойко Т.А., Бойко А.А. Анализ основных тенденций мирового и российского рынков биометрических технологий // Инновации и инвестиции. 2020. №5. С.72-76.
12. Тебенькова А.И. Биометрические данные: новые возможности и угрозы // Молодой ученый. - 2025. - № 50 (601). - С. 467-470.
13. Карцан И.Н., Жуков А.О. Механизм защиты промышленной сети. // Информационные и телекоммуникационные технологии. - 2021.- 52.-19-26.
14. Карцан И.Н., Гончаренко Ю.Ю. Влияние кибербезопасности на обработку информации в развивающихся новых технологиях. // Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. VII Всероссийская научно-практическая конференция. - 2022.- С.471-479.