Проект

Утверждена
Указом Президента
Российской Федерации
от _____ № ___

Доктрина развития системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий

I. Основные положения

Доктрина развития системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий (далее соответственно – Доктрина, ИКТ), определяет приоритеты, цели, задачи и основные направления развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, на среднесрочный и долгосрочный период.

В соответствии с Федеральным законом от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации» Доктрина обеспечивает реализацию в Российской Федерации положений:

Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400;

Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646;

Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203;

Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утвержденной распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р;

Основ государственной политики Российской Федерации в области международной информационной безопасности, утвержденных Указом Президента Российской Федерации от 12 апреля 2021 г. № 213.

При разработке Доктрины учтены:

Основы государственной политики в сфере стратегического планирования в Российской Федерации, утвержденные Указом Президента Российской Федерации от 8 ноября 2021 г. № 633;

Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10 октября 2019 г. № 490;

Стратегия развития финансового рынка Российской Федерации до 2030 года, утвержденная распоряжением Правительства Российской Федерации от 29 декабря 2022 г. № 4355-р;

Стратегия развития отрасли связи Российской Федерации на период до 2035 года, утвержденная распоряжением Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р;

иные нормативные правовые акты Российской Федерации, определяющие направления применения ИКТ в Российской Федерации и документы стратегического планирования Российской Федерации.

Период реализации Доктрины разделен на 3 этапа:

на I этапе (2027 – 2028 годы) планируется реализация организационно-подготовительных мероприятий, в том числе разработка и принятие нормативных правовых актов, необходимых для реализации ключевых направлений Доктрины, апробация потенциальными участниками ряда создаваемых технологий противодействия правонарушениям, совершаемым с ИКТ, утверждение методик расчета целевых показателей реализации Доктрины и возможная корректировка сроков, процессов и масштаба реализации отдельных мероприятий с учетом установленных целевых показателей;

на II этапе (2029 – 2030 годы, включительно) планируется создание организационных и технологических основ для реализации задач Доктрины, создание и поэтапное внедрение соответствующих механизмов противодействия правонарушениям, совершаемым с использованием ИКТ;

на III этапе (2031 – 2035 годы, включительно) – развитие созданных механизмов и формирование предложений по дальнейшему их совершенствованию в рамках системы противодействия преступлениям, совершаемым с использованием ИКТ.

Доктрина исходит из необходимости комплексного подхода к предотвращению возможности использования ИКТ в противоправных целях, борьбе со всей совокупностью правонарушений, совершаемых с использованием ИКТ, а не отдельных их видов, приоритета профилактической (предупредительной) деятельности, а также кадрового обеспечения компетентных ведомств, продолжая курс, заложенный в Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утвержденной распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р,

и в плане мероприятий по ее реализации, утвержденном распоряжением Правительства Российской Федерации от 14 августа 2025 г. № 2207-р.

Для целей настоящей Доктрины используются следующие основные термины и понятия:

антифрод-меры – комплекс правовых, технических и организационных мер, направленных на выявление, предупреждение и пресечение правонарушений, совершаемых с использованием ИКТ;

антифрод-система – комплекс программных средств, аналитических методов и процедур, внедряемых организациями и предназначенных для выявления, предупреждения и пресечения в режиме реального времени подозрительных операций, совершаемых с использованием ИКТ, без согласия клиента или с его согласием, полученным под влиянием обмана или при злоупотреблении доверием;

информационно-коммуникационная система – любое устройство или группа соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит сбор, хранение и автоматическую обработку электронных данных;

единый профиль – совокупность уникальных признаков физического или юридического лица, связанных в единой доверенной среде для целей идентификации при совершении юридически значимых действий в цифровой среде;

цифровой след – зафиксированная в электронной (цифровой) форме информация о действиях пользователя, программных и аппаратных средств в информационных системах и сетях связи, в том числе сведения о компьютерном или электронном устройстве, которая может быть использована для выявления, раскрытия и расследования правонарушений, совершаемых с использованием ИКТ;

электронное (цифровое) доказательство – сведения о фактах, имеющих значение для уголовного, административного или иного дела, представленные в электронной (цифровой) форме, получаемые, проверяемые и оцениваемые в порядке, установленном законодательством Российской Федерации, в том числе в дистанционном (онлайн) и (или) в автономном режиме с использованием специализированных программно-технических средств;

механизм обратного отслеживания – совокупность технических и организационных процедур, позволяющих идентифицировать источник подозрительной коммуникации в сетях связи и информационно-коммуникационной сети «Интернет», в том числе с использованием средств государственной информационной системы противодействия правонарушениям, совершаемым с использованием ИКТ, и ведомственных информационных систем;

Платформа – государственная информационная система противодействия правонарушениям, совершаемым с использованием ИКТ;

платформа согласий – функциональность единой системы идентификации и аутентификации, обеспечивающая управление согласиями субъектов персональных данных на обработку их персональных данных операторами в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

показатель развития системы противодействия правонарушениям, совершаемым с использованием ИКТ – количественная или качественная характеристика масштаба и уровня развития системы противодействия (ее отдельных механизмов);

показатель эффективности системы противодействия правонарушениям, совершаемым с использованием ИКТ – количественная или качественная характеристика достигаемых эффектов работы системы противодействия;

профилактика виктимизации – система мер, направленных на снижение подверженности граждан и организаций риску стать жертвами правонарушений, совершаемых с использованием ИКТ, в том числе посредством правового просвещения, правового информирования и повышения уровня цифровой гигиены, цифровой и финансовой грамотности;

противоправная инфраструктура – совокупность доменных имен, хостинг-ресурсов, информационных систем, программ для электронных вычислительных машин, учетных записей, абонентских номеров, идентификационных модулей абонента (сим-карт), абонентских терминалов пропуска трафика, виртуальных телефонных станций, платежных реквизитов, цифровых кошельков и иных идентификаторов, используемых для подготовки и совершения правонарушений с использованием ИКТ;

уровни защиты – совокупность субъектов, инструментов и механизмов (законодательных, технологических, правоприменительных и просветительских), задействованных в противодействии на каждом этапе правонарушения, совершаемого с использованием ИКТ;

фрод-потенциал – совокупность рисков и возможностей получения злоумышленником прямой выгоды при нарушении функционирования информационного процесса, реализуемого информационной системой, в результате осуществления мошеннических действий в сфере компьютерной информации;

цифровая грамотность – набор компетенций, необходимых для безопасного и эффективного использования цифровых инструментов

и технологий, а также ресурсов информационно-коммуникационной сети «Интернет»;

цифровая гигиена – совокупность знаний, навыков и правил безопасного поведения граждан и организаций в цифровой среде, направленных на предупреждение правонарушений, совершаемых с использованием ИКТ, и снижение риска виктимизации;

финансовая грамотность – совокупность знаний, навыков и установок в сфере финансового поведения, обеспечивающих способность граждан принимать обоснованные решения и противостоять методам социальной инженерии, применяемым при совершении правонарушений с использованием ИКТ;

цифровая идентификация личности – совокупность данных, атрибутов, учетных записей и поведенческих характеристик, формирующих цифровое представление физического лица в информационных системах и позволяющих идентифицировать его, взаимодействовать с ним и оказывать ему услуги в цифровой среде, в том числе оценивать его состояние, обнаруживать аномалии и прогнозировать угрозы.

II. Вызовы развития системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий

В Российской Федерации проблема противодействия правонарушениям, особенно в цифровой сфере, находится на особом контроле государства. Принятые за последние годы системные меры, включая Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон № 41-ФЗ), Федеральный закон от 26 июня 2026 г. № 210-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации», а также Концепцию государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, утвержденную распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р, создали необходимую нормативную основу в сфере противодействия ИКТ-правонарушениям.

Несмотря на то, что в соответствии со статистикой МВД России, по итогам 2025 года в результате принятых на законодательном уровне комплексных мер по противодействию правонарушениям, совершаемым

с использованием ИКТ, количество ИКТ-преступлений по отношению к 2024 году снизилось на 11,8 % (с 765,4 тыс. до 675,4 тыс.), обозначенная проблема остается актуальной, в том числе потому, что инструменты мошенников постоянно совершенствуются.

Решение задачи противодействия правонарушениям, совершаемым с использованием ИКТ, предполагает комплексный подход и оперативное взаимодействие всех заинтересованных участников на каждом уровне системы противодействия.

В современных условиях организациям критически важно выстраивать проактивную защиту информационных систем и данных и системного укреплять уровень безопасности с учетом скоординированной работы бизнеса и государства.

В соответствии со статьей 1 Федерального закона № 41-ФЗ с целью обеспечения оперативного предоставления всем участникам взаимодействия (в том числе правоохранительным органам, уполномоченным федеральным органам исполнительной власти, Банку России, финансовым организациям, операторам связи и цифровым платформам) необходимой информации о попытках совершения мошеннических действий для их оперативной блокировки и последующего предотвращения с 1 марта 2026 г. создана Платформа.

Государственный органы, финансовые организации, операторы связи, цифровые платформы и иные участники взаимодействия перестают работать в одиночку против мошенников – создается общий «цифровой иммунитет».

Платформа является единой оперативной информационно-аналитической интеграционной средой, при взаимодействии с которой локальные (ведомственные и корпоративные) и отраслевые инструменты противодействия мошенничеству будут синхронизированы.

Оперативный обмен обезличенными сигналами об атрибутах мошенников и их жертв между всеми участниками взаимодействия создает условия, при которых противоправное применение данных граждан (платежных инструментов, абонентских номеров, учетных записей пользователей цифровых платформ) становится нерезультативным.

Платформа должна сыграть роль центра информационного взаимодействия участников, при этом задачи оперативного противодействия мошенничеству, совершаемому с использованием ИКТ, распределяются между участниками взаимодействия в рамках сценариев противодействия правонарушениям.

Эффективное взаимодействие информационных систем всех участников Платформы является основой формирования цифровой безопасности граждан.

Несмотря на предпринимаемые меры, динамичный характер развития ИКТ и адаптивность преступной среды требуют постоянного совершенствования системы противодействия правонарушениям, совершаемым с использованием ИКТ.

В целях обеспечения высокого уровня защиты от незаконного оборота персональных данных необходимо совершенствование законодательства в сфере обработки персональных данных, предусматривающее внедрение и развитие правовых и технологических механизмов эффективного управления гражданином своими персональными данными.

В рамках существующей модели противодействия требуется дальнейшее совершенствование мер по пресечению и предупреждению административных правонарушений в сфере ИКТ, предотвращение которых имеет первоочередное значение для недопущения перерастания таких деяний в преступления.

Сохраняется потребность в развитии индивидуальных подходов, методов, инструментов и механизмов противодействия отдельным видам преступлений, совершаемых с использованием ИКТ, в числе которых – дистанционные мошенничества, наркопреступления, преступления экстремистской и террористической направленности, преступления против несовершеннолетних и непосредственно компьютерные преступления, с учетом особенностей каждого из указанных направлений.

Самостоятельным вызовом является недостаточная развитость профилактической составляющей противодействия, в том числе деятельности по правовому просвещению и правовому информированию населения, формированию навыков цифровой гигиены и финансовой грамотности. Предусмотренная статьей 6 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» деятельность по правовому просвещению не содержит особенностей, учитывающих специфику правонарушений, совершаемых с использованием ИКТ, а уровень виктимности отдельных категорий граждан (прежде всего лиц пожилого возраста и несовершеннолетних) остается высоким.

Системными вызовами текущей модели противодействия правонарушениям, совершаемым с использованием ИКТ, являются:

Непрерывный процесс развития. Необходимость совершенствования нормативно-правового и кадрового обеспечения для эффективного и оперативного выявления, раскрытия и расследования преступлений, совершаемых с использованием ИКТ.

Унификация. Совершенствование мер профилактического характера с учетом обеспечения последовательной систематизации и унификации применяемых подходов, в том числе разработки единых методик

и алгоритмов взаимодействия с населением, используемых методических ресурсов, а также повышения уровня квалификации лиц, ответственных за осуществление указанной деятельности.

Фрагментация информационного пространства. В целях наращивания эффективности совместной работы требуется дальнейшее развитие согласованной модели взаимодействия финансовых организаций, операторов связи, цифровых платформ, иных участников цифровой среды и государственных информационных систем, позволяющей перейти от автономной работы к согласованным действиям.

Временной разрыв реагирования. Временной разрыв между обнаружением мошеннических действий и реакцией участников создает окно возможностей для злоумышленников. Необходимо развитие инструментов оперативного взаимодействия и автоматизированных процедур реагирования, позволяющих свести этот период к минимально допустимому значению.

Централизация. Создание единых централизованных баз данных для обмена информацией требует усиленных мер защиты. Концентрация данных может повышать интерес злоумышленников, что требует учета всех потенциальных рисков и внедрения соответствующих мер безопасности.

Избыточность. Однотипные персональные данные граждан (такие как фамилия, имя, отчество, дата рождения, место регистрации, номера телефонов и другие) накапливаются различными операторами. Увеличение их общего объема, обогащение новыми типами данных (в том числе автоматически собираемые при посещении ресурсов в информационно-коммуникационной сети «Интернет» (далее – сеть «Интернет»), обрабатываемые с использованием технологий искусственного интеллекта) создает риски незаконного профилирования, использования в социальной инженерии против самих граждан.

Текущая ситуация показывает, что постоянное инкрементальное совершенствование существующих механизмов демонстрирует различную степень результативности. Необходим переход к принципиально новой модели, которая обеспечивает:

оперативную координацию между всеми участниками процесса защиты от правонарушений, совершаемых с использованием ИКТ;

защиту данных по принципу «нулевого знания» – без концентрации данных в одной точке;

связь между отдельными элементами цифровой идентичности, допускающую формальную (математическую) проверку достоверности;

автоматизированное реагирование на угрозы в режиме близкому к реальному времени.

III. Цели, приоритеты и задачи Доктрины

Целью Доктрины является создание условий для развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, обеспечивающей защиту прав и законных интересов граждан, бизнеса и государства в цифровой среде Российской Федерации.

Основополагающим принципом, заложенным в положения Доктрины, является принцип борьбы с первопричинами совершения правонарушений в сфере ИКТ.

Доктрина призвана способствовать обеспечению следующих национальных целей и интересов:

совершенствование методов, инструментов и механизмов противодействия дистанционным мошенничествам, наркопреступлениям, экстремизму и терроризму, преступлениям против детей, в том числе совершаемым с использованием сети «Интернет», компьютерным преступлениям и иным правонарушениям, совершаемым с использованием ИКТ;

обеспечение информационной безопасности в сети «Интернет» и формирование у граждан соответствующих навыков в сферах цифровой грамотности, цифровой гигиены и финансовой грамотности;

сокращение оборота персональных данных, путем разработки и внедрения принципиально новых подходов к обработке персональных данных операторами и идентификации граждан в цифровой среде;

инфраструктурное и кадровое обеспечение технологического развития;

регуляторное обеспечение технологического развития;

развитие кадрового потенциала государственной системы противодействия правонарушениям, совершаемым с использованием ИКТ, и научное обеспечение деятельности;

развитие государственно-частного взаимодействия с кредитными организациями, операторами связи, организациями в сфере информационной безопасности и иными организациями, осуществляющими деятельность в сфере ИКТ;

обеспечение безопасности граждан и государства;

развитие международного сотрудничества для противодействия правонарушениям, совершаемым с использованием ИКТ.

Приоритетными направлениями реализации Доктрины являются:

совершенствование нормативно-правового регулирования, в том числе уголовного, уголовно-процессуального и оперативно-разыскного законодательства в части развития института цифровых (электронных)

доказательств, новых форм и средств доказывания, а также фиксации и легализации цифровых следов;

развитие технологической инфраструктуры и экспертного обеспечения противодействия правонарушениям, совершаемым с использованием ИКТ, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших;

создание механизмов активного пресечения противоправной инфраструктуры на ранних этапах;

обеспечение безопасности цифровых услуг, предоставляемых гражданам, и предотвращение использования цифровых услуг в противоправных целях;

совершенствование организационно-управленческой инфраструктуры противодействия мошенничеству, совершаемому с использованием ИКТ,

повышение эффективности профилактики и укрепление вовлеченности гражданского общества;

повышение уровня правовой, финансовой и цифровой грамотности граждан, правовое просвещение и информирование населения, в том числе с использованием потенциала институтов гражданского общества и профильных некоммерческих организаций;

развитие международного сотрудничества в рамках Содружества Независимых Государств, БРИКС, Шанхайской организации сотрудничества, Ассоциации государств Юго-Восточной Азии, Организации Объединенных Наций, в том числе с учетом подписанной 25 октября 2025 г. Российской Федерацией Конвенции Организации Объединенных Наций против киберпреступности.

Для достижения поставленной цели реализации Доктрины необходимо решение взаимосвязанных задач в рамках следующих сфер деятельности:

повышение эффективности правоохранительной и контрольной деятельности;

развитие кадрового потенциала и научное обеспечение противодействия правонарушениям, совершаемым с использованием ИКТ;

развитие государственно-частного взаимодействия;

технологическое развитие и инфраструктура;

профилактика и взаимодействие с гражданами;

финансовое взаимодействие и возмещение ущерба;

обеспечение достоверности и защиты данных;

защита персональных данных;

международное взаимодействие.

IV. Основные направления реализации Доктрины

1. Повышение эффективности правоохранительной и контрольной деятельности

Реализация Доктрины в сфере повышения эффективности правоохранительной и контрольной деятельности предполагает решение следующих задач:

создание и укрепление специализированных подразделений по противодействию правонарушениям, совершаемым с использованием ИКТ, их оснащение современными аппаратно-программными и научно-техническими средствами;

развитие межведомственного взаимодействия и координации деятельности правоохранительных органов, в том числе с использованием программно-технических комплексов и информационных систем (включая использование технологий искусственного интеллекта), их совершенствование, разработка и внедрение новых инструментов, а также механизмов их автоматизированного применения для целей выявления, предупреждения и пресечения противоправных деяний и доказывания;

совершенствование мер для эффективного и оперативного устранения обстоятельств, способствовавших совершению правонарушений с использованием ИКТ;

усиление контрольной (надзорной) деятельности в отношении участников цифровой среды в части исполнения ими требований законодательства;

совершенствование методов и способов выявления, предупреждения, пресечения и раскрытия преступлений, а также выявление и установление лиц, их подготавливающих (совершающих, совершивших) или обеспечивающих техническую и финансовую инфраструктуру организованной преступной деятельности, а также передачу организаторам преступлений персональных данных граждан, средств коммуникации и финансовых инструментов;

совершенствование механизмов и инструментов борьбы с бесконтактным и дистанционным формам сбыта наркотических средств и психотропных веществ, в том числе через теневые цифровые ресурсы, криминализация деяний по созданию, технической поддержке и администрированию информационных ресурсов, заведомо предназначенных для организации противоправной деятельности;

усиление уголовно-правовых инструментов за посягательства на половую неприкосновенность и половую свободу детей, совершаемые с использованием сети «Интернет» и иных информационно-

телекоммуникационных сетей, рассмотрение вопроса о создании реестра лиц, совершивших противоправные посягательства на половую неприкосновенность несовершеннолетних, и применении в отношении них дополнительных мер контроля, в том числе с использованием технических средств;

совершенствование положений Кодекса Российской Федерации об административных правонарушениях, обеспечение их пресечения и предупреждения как первоочередного направления борьбы с преступностью в сфере ИКТ.

2. Развитие кадрового потенциала и научное обеспечение противодействия

В сфере кадрового потенциала и научного обеспечения противодействия правонарушениям, совершаемым с использованием ИКТ, необходимо решение следующих задач:

разработка и внедрение специализированных программ обучения и повышения квалификации работников органов, осуществляющих противодействие правонарушениям, совершаемым с использованием ИКТ, с привлечением в качестве экспертов и преподавателей представителей организаций, осуществляющих деятельность в сфере ИКТ, организаций в сфере информационной безопасности, кредитных организаций, операторов связи, цифровых платформ;

формирование и развитие в образовательных организациях высшего образования профильных направлений подготовки специалистов в сферах юриспруденции в области информационной безопасности, компьютерного права, компьютерной (цифровой) криминалистики и судебной компьютерно-технической экспертизы;

проработка возможности внесения новой специальности «Антифрод-специалист» в Общероссийской классификатор специальностей по образованию, создания национальной программы подготовки специалистов, программу повышения квалификации сотрудников антифрод-подразделений организаций;

внедрение специализированных программ обучения и повышения квалификации студентов и сотрудников федеральных органов исполнительной власти, органов власти субъектов Российской Федерации, муниципальных образований, финансовых и иных организаций, задействованных в противодействии правонарушениям в сфере ИКТ, либо осуществляющих функции по обработке информации, а равно материально-техническое обеспечение их деятельности;

организационно-штатное и материально-техническое обеспечение деятельности правоохранительных, надзорных и контрольных органов, осуществляющих функции в сфере противодействия правонарушениям,

совершаемым с использованием информационно-коммуникационных технологий, включая закрепление в их структуре специализированных подразделений;

развитие межведомственного и государственно-частного взаимодействия в сфере научно-исследовательских и опытно-конструкторских работ по совершенствованию методик противодействия правонарушениям, совершаемым с использованием ИКТ, с участием Российской академии наук, ведомственных научных и образовательных организаций, а также организаций, осуществляющих деятельность в сфере ИКТ.

3. Развитие государственно-частного взаимодействия

Обеспечение условий для государственно-частного взаимодействия в сфере противодействия правонарушениям, совершаемым с использованием ИКТ, при условии консолидации ресурсов и распределения рисков между сторонами, способствует наращиванию технологического потенциала государственных органов в указанной сфере.

Задачи реализации Доктрины в сфере развития государственно-частного взаимодействия предполагают реализацию следующих мероприятий:

развитие форматов взаимодействия государственных органов с кредитными организациями, операторами связи, организациями, осуществляющими деятельность в сфере ИКТ, организациями в сфере информационной безопасности, цифровыми платформами и иными участниками цифровой экономики в целях своевременного выявления, пресечения и расследования правонарушений, совершаемых с использованием ИКТ;

использование потенциала профильных некоммерческих организаций в формировании планов и стратегий профилактики правонарушений в сфере ИКТ, разработке учебных программ, организации мероприятий правового просвещения;

привлечение экспертов из числа представителей коммерческих организаций в сфере ИКТ, организаций в сфере информационной безопасности и кредитных организаций к проведению обучающих мероприятий для сотрудников правоохранительных, надзорных и контрольных органов, а также к выработке регуляторных решений и методических рекомендаций;

создание условий и нерегуляторных стимулов для инвестиций бизнеса в реализацию мер противодействия правонарушениям,

совершаемым с использованием ИКТ, обмен лучшими практиками между участниками государственно-частного взаимодействия.

4. Технологическое развитие и инфраструктура

В целях обеспечения внедрения передовых технологий в рамках развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, реализация Доктрины предполагает решение следующих задач:

формирование методологической и технологической основы для создания защищенной государственной системы, обеспечивающей возможность верифицировать принадлежность юридически значимых идентификаторов конкретному субъекту;

совершенствование технологий предоставления субъектами цифровой среды по запросам правоохранительных органов сведений в машиночитаемых форматах, унификация форматов и протоколов такого обмена;

регламентация порядка сбора, проверки и оценки электронных (цифровых) доказательств, в том числе полученных в дистанционном (онлайн) режиме, а также легализации сведений, извлеченных с использованием специализированных программно-технических средств;

развитие принципиально новой системы криминалистического учета и идентификации на основе цифрового следа компьютерного или электронного устройства, включая сбор, хранение и обработку данных, существующих в сетевом пространстве, развитие специализированных аналитических программных продуктов для проведения исследований и судебных компьютерно-технических экспертиз;

нормативное закрепление порядка использования сведений, полученных в рамках разведки по открытым источникам, в качестве доказательственной базы по уголовным и иным делам, с учетом требований законодательства;

совершенствование механизмов использования средств видео-конференц-связи (в том числе с применением беспилотных технических средств) для проведения отдельных следственных действий, включая осмотр места происшествия, в случаях, когда традиционный формат проведения процессуального мероприятия создает угрозу жизни или здоровью его участников;

проработка перспективных технологических решений в области цифрового представления личности и связанных с ними координационных инструментов при условии их научно-технической готовности, ресурсной

обеспеченности и безусловного соблюдения конституционных прав и свобод граждан;

совершенствование механизмов идентификации и аутентификации, в том числе на основе биометрических персональных данных физических лиц, и их защиты, как фундаментального элемента цифровой инфраструктуры, в том числе:

в целях обеспечения максимальной достоверности размещенных биометрических данных в государственной информационной системе «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее – ЕБС) разработать и внедрить механизм, позволяющий исключить возможность подмены биометрических данных третьим лицом при процедурах биометрической регистрации и обновления биометрических данных, как в дистанционных каналах, так и в организациях, уполномоченных осуществлять сбор биометрических данных,

в целях безопасного использования биометрии в процессах и сценариях подтверждения юридически значимых действий обеспечить закрепление на законодательном уровне соответствующие условия применения биометрических персональных данных,

комплексно проработать задачу наполнения единой базы образцов лицевой биометрии ЕБС государством, финансовыми организациями, операторами связи и операторами цифровых платформ с целью исключения возможности подмены личности или использования биометрии мошенниками при подтверждении юридически значимых действий;

внедрение технологий искусственного интеллекта в сфере выявления потенциальных уязвимостей и выработке стратегии по их защите;

повышение эффективности работы Платформы с учетом мониторинга показателей степени функциональной полноты, охвата участников взаимодействия, качества, полноты и связности передаваемых данных, эффективности использования для блокировки мошеннических действий, развития используемых технологий (включая использование моделей искусственного интеллекта);

совершенствование механизмов управления финансовыми инструментами, используемыми гражданами (информация о банковских картах, счетах, кредитах), предоставляющих возможность отказа от услуг и расторжения договоров банковского счета;

совершенствование механизмов информационного обмена и состава данных при взаимодействии организаций и граждан, а также подходов к оказанию гражданам финансовых и иных дистанционных услуг;

внедрение системы контрольных показателей уровня риска с учетом отраслевых особенностей деятельности участников цифровой среды

с обеспечением соответствующего режима конфиденциальности обрабатываемых сведений;

внедрение механизмов прогнозирования, выявления и анализа новых видов правонарушений в сфере ИКТ с использованием передовых технологий (искусственный интеллект, дипфейк, новые способы социальной инженерии);

установление отраслевых стандартов, определяющих требуемый уровень антифрод-мер для участников высокорисковых отраслей;

создание нерегуляторных стимулов инвестиций бизнеса в реализацию антифрод-мер, в том числе стимулирующих мер финансового и нефинансового характера;

проработка вопроса внедрения антифрод-аудита (обязательного планового аудита антифрод-систем организаций, с учетом их организационно-правовой формы и источника финансирования);

проработка вопроса внедрения оценки фрод-потенциала информационных систем с учетом обеспечения соответствующего режима конфиденциальности сведений;

проработка вопроса формирования стимулирующих мер финансового и нефинансового характера для участников рынка с антифрод-системами, подтвердившими свою высокую эффективность;

проработка вопроса внедрения стандартов и условий обязательности использования средств речевой и текстовой аналитики;

обеспечение анализа существующих и вновь вводимых цифровых услуг на предмет безопасности.

5. Профилактика и взаимодействие с гражданами

Реализация Доктрины в сфере профилактики и взаимодействия с гражданами предполагает решение следующих задач:

повышение уровня правовой, финансовой и цифровой грамотности граждан;

формирование восприятия профилактики правонарушений как ориентира в вопросах планирования, организации работы и взаимодействия государственный органов и частных организаций при реализации государственной политики в области информационной безопасности;

укрепление вовлеченности институтов гражданского общества в профилактику и предупреждение правонарушений, совершаемых с использованием ИКТ, привлечение к проведению профилактических мероприятий профильных некоммерческих организаций и объединений в сферах ИКТ и информационной безопасности;

повышение уровня осведомленности граждан о наиболее распространенных схемах мошенничества и иных видов и форм правонарушений, совершаемых с использованием ИКТ, формирование культуры безопасной цифровой среды;

проведение адресных профилактических мероприятий для отдельных категорий граждан (несовершеннолетние, лица пожилого возраста, государственные служащие, специалисты в сфере ИКТ), включая работу с социально незащищенными категориями граждан, наиболее подверженными виктимизации;

совершенствование инструментов взаимодействия кредитных организаций и операторов связи с правоохранительными органами власти в рамках осуществления мер информирования граждан о совершаемых (совершенных) в их отношении ИКТ-правонарушениях;

внедрение инструмента обучения, основанного на имитации мошенничества, совершаемого с использованием ИКТ, или преступления в сфере компьютерной информации (тренажер, предполагающий проведение учебных атак, с целью осуществления спонтанной проверки знаний);

реализация программы профилактической работы с населением, демонстрирующей принцип неотвратимости ответственности за совершение преступлений в сфере ИКТ;

внедрение и развитие специализированных учебных курсов по цифровой гигиене, цифровой грамотности и финансовой грамотности в образовательные программы общего, среднего профессионального и высшего образования;

разработка и реализация алгоритма непроцессуальных форм профилактики правонарушений, совершаемых с использованием ИКТ, предусматривающего вовлечение федеральных и муниципальных органов власти, общественных объединений, коммерческих организаций, государственных и негосударственных корпораций, градообразующих предприятий, учебных заведений всех образовательных ступеней, средств массовой информации федерального и регионального уровня, религиозных конфессий, лидеров общественного мнения, представителей науки и творчества и иных участников;

расширение объемов социальной рекламы, ее распространение на официальных сайтах органов государственной власти и местного самоуправления, в средствах массовой информации;

создание общероссийской площадки (ежегодной конференции, фестиваля), посвященной вопросам повышения цифровой грамотности, цифровой гигиены и финансовой грамотности;

организация регулярного сбора и анализа обратной связи от населения с целью ее учета при формировании новых мер противодействия правонарушениям, совершаемым с использованием ИКТ.

6. Финансовое взаимодействие и возмещение ущерба

Задачи реализации Доктрины в сфере финансового взаимодействия и возмещения ущерба основываются на справедливом распределении ответственности сторон и предполагают:

установление на законодательном уровне полномочий кредитных организаций по совместному принятию решений о возврате денежных средств отправителям при переводах, осуществленных без добровольного согласия клиента, путем взыскания сумм со счетов получателей, причастных к мошенническим действиям (механизм «обратного взыскания»);

совершенствование порядка возврата похищенных средств со счетов клиентов, включая установление регламентированных сроков и ответственности участников;

реализацию кредитной организацией, обслуживающей получателя денежных средств-потенциального участника мошеннической схем, соответствующих антифрод-мер;

внедрение механизмов, стимулирующих организации к активному предотвращению мошеннических операций, включая применение контрольных показателей эффективности, а также рейтинговую систему, основанную на внедрении антифрод-инструментов, предотвращении инцидентов и ликвидации их последствий, с учетом обеспечения соответствующего режима конфиденциальности сведений;

мониторинг эффективности применяемых финансовыми организациями механизмов противодействия мошенническим операциям и их совершенствование по результатам мониторинга, с учетом обеспечения соответствующего режима конфиденциальности сведений.

7. Обеспечение достоверности и защиты данных

В сфере обеспечения достоверности и защиты данных реализация Доктрины предполагает решение следующих задач:

совершенствование механизма аудита систем защиты государственных информационных систем, в которых осуществляется накопление и обработка персональных данных, а также коммерческих информационных систем, получающих персональные данные из государственных информационных систем, с учетом разработки

соответствующего порядка, определяемого Правительством Российской Федерации;

разработка механизма сверок и соответствующей ревизии имеющихся учетных записей в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА) на предмет актуальности, в том числе с использованием сведений о государственной регистрации смерти;

обеспечение однозначности, актуальности и достоверности сведений в государственных информационных системах, являющихся источниками сведений для ЕСИА и используемых для создания единого профиля;

проработка возможностей использования биометрических персональных данных при проведении профилактических проверок, а также при выявлении подозрительных операций, совершаемых в дистанционном формате, как одного из возможных способов подтверждения таких операций;

совершенствование инструментов и механизмов (для физических лиц, потребителей данных и поставщиков данных), обеспечивающих:

выявление и немедленное реагирование на любые расхождения в данных о физическом лице в различных информационных системах;

автоматизированное уведомление всех участников информационного взаимодействия о выявленных ошибках и несоответствиях;

возможность для физического лица оперативно инициировать проверку и исправление своих данных без административных барьеров;

регламентированные сроки устранения расхождений с контролем исполнения.

8. Защита персональных данных

Важным направлением противодействия правонарушениям в сфере ИКТ остается защита персональных данных, которые нередко используются злоумышленниками в противоправных целях. Задачи реализации Доктрины в сфере снижения масштабов сбора персональных данных, возможностей их обогащения и незаконного профилирования граждан, доступности персональных данных для мошенников предполагают:

создание на базе ЕСИА платформы согласий, обеспечивающей процессы выдачи, хранения и отзыва всех согласий на обработку персональных данных граждан, а также создание правовых условий для сокращения случаев, при которых операторы будут вправе осуществлять

обработку персональных данных на основании согласий на обработку персональных данных;

проработку методов и внедрение механизмов идентификации граждан организациями без передачи им персональных данных граждан в случаях, определяемых Правительством Российской Федерации.

9. Международное взаимодействие

С учетом существующей геополитической обстановки, действующих санкций и нарастающих угроз в цифровой среде развитие партнерства Российской Федерации с другими странами в области противодействия правонарушениям в сфере ИКТ приобретает стратегическое значение. Такое сотрудничество поможет усилить защиту отечественной цифровой инфраструктуры и одновременно продемонстрировать готовность Российской Федерации выступать в роли ответственного и эффективного участника международного цифрового диалога.

В сфере международного взаимодействия задачи реализации Доктрины предполагают:

развитие сотрудничества с государствами – участниками Содружества Независимых Государств, странами БРИКС, Шанхайской организацией сотрудничества, Ассоциацией государств Юго-Восточной Азии, а также профильными структурами Организации Объединенных Наций, в том числе с учетом подписанной 25 октября 2025 г. Российской Федерацией Конвенции Организации Объединенных Наций против киберпреступности, в целях:

проработки в рамках Содружества Независимых Государств, Шанхайской организации сотрудничества и БРИКС вопросов согласованной криминализации деяний, связанных с администрированием криминальных цифровых ресурсов, и взаимной правовой помощи при пресечении деятельности теневых рынков и расследовании правонарушений в сфере ИКТ;

обмена передовым опытом и информацией о новых видах преступных угроз;

расширения действующих механизмов взаимодействия кредитных организаций, операторов связи, организаций, осуществляющих деятельность в сфере ИКТ, организаций в сфере информационной безопасности, цифровых платформ и иных участников цифровой экономики;

координации действий по пресечению деятельности транснациональных организованных преступных групп, использующих ИКТ;

выработки согласованных подходов к регулированию цифровой среды и обеспечению безопасности трансграничных платежей;

участия в работе международных профильных площадок в части, не противоречащей интересам Российской Федерации;

организации работы по подготовке законодательных и организационных изменений, необходимых для ратификации Российской Федерацией Конвенции Организации Объединенных Наций против киберпреступности, с особым вниманием к регламентации сбора, хранения и предоставления цифровых доказательств в процессуальной деятельности, применению технических средств для их агрегации, развитию материально-технического и кадрового потенциала компетентных органов;

использования каналов полицейского и прокурорского взаимодействия в целях возврата выведенных за рубеж денежных средств и привлечения к ответственности виновных в организации правонарушений, совершаемых с использованием информационно-коммуникационных технологий;

формирования и (или) развитие действующих площадок (конференций, форумов) по вопросам совершенствования мер по борьбе с правонарушениями, совершаемыми с использованием ИКТ, с расширением международного представительства и представительства ИКТ-сектора национальной экономики.

V. Механизмы реализации Доктрины

Для комплексной оценки развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, используется система показателей управления процессами противодействия, определяемая Правительством Российской Федерации.

Перечень показателей состояния развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, может уточняться по результатам ежегодного мониторинга реализации Доктрины.

Для оценки реализации Доктрины применяется двухуровневая система показателей.

Показатели развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, характеризуют масштаб и уровень развития системы противодействия (ее отдельных механизмов, в том числе Платформы).

Показатели развития системы противодействия носят индикативный характер, целевые значения по ним не устанавливаются.

Показатели эффективности системы противодействия правонарушениям, совершаемым с использованием ИКТ, характеризуют достигаемый эффект работы системы противодействия.

Реализация Доктрины учитывает три сценария – базовый, целевой, а также опережающий.

Риски реализации сценариев оцениваются участниками реализации Доктрины в рамках осуществления ее ежегодного мониторинга.

1. Базовый и целевой сценарии

Базовый сценарий предполагает дальнейшее развитие существующих подходов к противодействию правонарушениям, совершаемым с использованием ИКТ, совершенствование механизмов информационного обмена и состава данных при взаимодействии организаций и граждан, а также подходов к оказанию гражданам цифровых услуг.

Целевой сценарий (дополнительно к инструментарию базового сценария) учитывает необходимость и обязательность координированных действий всех участников на всех уровнях системы противодействия правонарушениям, совершаемым с использованием ИКТ.

Реализация цели и задач Доктрины при этом предполагает разработку и внедрение участниками системы противодействия правонарушениям, совершаемым с использованием ИКТ, методологии противодействия на основе этапов жизненного цикла правонарушения и уровней защиты системы, а также процессный подход, рассматривающий правонарушение в сфере ИКТ как последовательность стадий (этапов).

Понимание всех этапов жизненного цикла правонарушения, совершаемого с использованием ИКТ, имеет ключевое значение для выбора мер защиты и рационального распределения ресурсов в условиях постоянно меняющихся угроз. Для каждой стадии определяются целевые меры противодействия, дифференцированные по уровням ответственности и функционала субъектов системы противодействия правонарушениям, совершаемым с использованием ИКТ.

Целевой сценарий предполагает разработку и внедрение методики оценки зрелости системы защиты.

2. Сценарий опережающего развития

В качестве сценария опережающего развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, на долгосрочную перспективу рассматриваются перспективные направления, реализация которых обусловлена результатами научно-исследовательских и опытно-конструкторских работ, оценкой технологической готовности и обеспеченностью необходимых финансовых ресурсов. К таким направлениям относятся развитие технологий цифрового представления личности, единого профиля и связанных с ними координационных инструментов, рассматриваемых в качестве дополнительного инструмента противодействия правонарушениям, совершаемым с использованием ИКТ.

Реализация сценария опережающего развития осуществляется при обязательном соблюдении приоритета конституционных прав и свобод граждан, недопущении необоснованной концентрации сведений о гражданах в единых хранилищах, обеспечении технологического суверенитета Российской Федерации, поэтапной апробации соответствующих технологических решений в рамках экспериментальных правовых режимов и при условии их положительной оценки независимыми экспертами в сферах информационной безопасности, защиты персональных данных и обеспечения национальной безопасности.

Сценарий опережающего развития предполагает формирование принципиально нового подхода к противодействию правонарушениям, совершаемым с использованием ИКТ, и создание принципиально новых возможностей для формирования безопасных клиентских путей в экосистеме цифровой экономики и разработки инновационных антифрод-продуктов государственной децентрализованной системы, в которых атака на цифровую личность человека в любой точке цифрового пространства мгновенно мобилизует коллективную защитную реакцию во всех точках цифрового присутствия такой цифровой личности – без централизованного хранения и накопления данных о гражданине и соблюдением безусловного приоритета конституционных прав и свобод гражданина.

Положения настоящего раздела носят перспективный характер и реализуются в рамках сценария опережающего развития. Условия реализации сценария опережающего развития устанавливаются Правительством Российской Федерации.

Для целей настоящего раздела под цифровым токеном (далее – ЦТ) понимается криптографический объект, являющийся верифицируемым цифровым отпечатком совокупности данных о физическом лице, распределенных между участниками экосистемы цифровой экономики, и служащий инструментом координации мер по защите цифровой личности.

ЦТ не является традиционным идентификатором и не подлежит применению для идентификации гражданина при осуществлении повседневных транзакций. Функциональное назначение ЦТ – обеспечение координации мер безопасности: ЦТ выступает связующим элементом, позволяющим объединять разрозненные фрагменты данных, находящиеся у различных участников цифровой среды, в единый защищенный периметр.

В настоящий момент фактически гражданин имеет сложно сформированный цифровой профиль, который состоит из разрозненных учетных записей в разных экосистемах, что не позволяет выстроить непрерывный процесс его защиты от угроз в сфере ИКТ.

Сформированный подход, планируемый к реализации в рамках сценария опережающего развития, позволит преодолеть ряд вызовов

существующей модели противодействия правонарушениям, совершаемым с использованием ИКТ, в том числе некоторые ограничения метода двухфакторной аутентификации, проблемы в части централизованного управления гражданами своими аккаунтами, проблемы потери цифровой личности.

Цифровой токен формируется математически (с определенной периодичностью), как результат криптографического свертывания фрагментов данных, хранящихся у каждого участника отдельно, что обеспечивает одновременно высокий уровень защиты приватности и возможность мгновенной координации действий при обнаружении атаки.

Фундаментальным принципом построения такой архитектуры предполагается отказ от централизованного хранения каких-либо данных об объекте защиты.

ЦТ должен обладать следующими обязательными свойствами:

Производность: ЦТ не содержит персональных данных в открытом виде, является результатом криптографического преобразования фрагментов данных, предоставляемых каждым участником экосистемы.

Уникальность: каждому физическому лицу должен соответствовать только один ЦТ. При этом алгоритм формирования гарантирует невозможность создания дублирующих токенов.

Неотчуждаемость: ЦТ должен быть неразрывно связан с физическим лицом и не может быть передан, скопирован или использован от имени другого лица.

Динамичность: ЦТ обновляется при изменении существенных параметров цифрового двойника (смена документов, номера телефона, открытие новых счетов), сохраняя при этом непрерывность идентичности.

Регенерация: ЦТ не имеет постоянного идентификатора в привычном виде, он предполагает регенерацию с определенной периодичностью.

Реализация сформированного подхода предполагает решение следующих задач:

рассмотрение возможности обеспечения в рамках существующей или вновь создаваемой информационной системы формирования ЦТ на основании криптографических производных данных участников системы и цифрового двойника каждого физического лица, существующего в цифровом пространстве без накопления дешифрованных данных в рамках одного хранилища;

внедрение единого механизма запросов на подтверждение достоверности действий, совершаемых пользователем посредством ИКТ, с использованием ЦТ;

предоставление гражданам Российской Федерации инструментов контроля, анализа и самозащиты в рамках системы противодействия правонарушениям, совершаемым с использованием ИКТ.

Реализация подхода основывается на следующих принципах:

данные не покидают периметр их держателей, в системе противодействия правонарушениям, совершаемым с использованием ИКТ, не создается единая централизованная база персональных данных;

приоритет защиты прав и интересов граждан;

баланс безопасности и приватности, исключающий применения инструментов необоснованного ограничения прав и свобод личности;

технологический суверенитет, предполагающий внедрение отечественных технологий и независимость от иностранных компонентов;

межотраслевое взаимодействие и единая координация государственных органов и организаций;

принцип коллективного иммунитета, предполагающий обеспечение ЦТ системного ответа на локальную угрозу;

принцип обеспечения конституционных прав граждан, предполагающий отсутствие ограничения на действия граждан в сети «Интернет» в случае отсутствия оснований для подозрений в осуществлении указанных действий под воздействием злоумышленников.

В долгосрочной перспективе Доктрина формирует основы для реализации эволюционного развития принципов идентификации, в том числе предполагая:

возможность бесшовной верификации в том числе за счет внутренних запросов в ЦТ, биометрии и иных способов;

существенное снижение уровня социальной инженерии и мошеннических атак через вредоносное программное обеспечение, а также улучшение клиентского пути пользователей в части аутентификации пользователей с учетом возможного отказа от метода двухфакторной аутентификации;

возможность отказа от иерархической цепочки аккаунтов;

выявление посредством ЦТ изменений профиля пользователя в одном из элементов экосистемы и последующее предотвращение использования гражданина, не являющимся стороной договора об использовании электронного средства платежа, заключенного с оператором по переводу денежных средств, для осуществления неправомерных операций;

использование ЦТ для построения клиентских путей, в которых возможно обеспечить снижение уязвимостей и потенциальных рисков атак;

скоординированные действия элементов ЦТ (в том числе фиксация подозрительных операций, совершаемых с использованием ИКТ, обмен

сведениями о соответствующих подозрительных операциях между участниками взаимодействия) в случае компрометации через вредоносное программное обеспечение.

Биометрические персональные данные в концепции ЦТ и системе противодействия мошенничеству могут стать ядром безопасной и бесшовной идентификации, в том числе благодаря действующим процессам безопасной обработки биометрических персональных данных, размещенных в единой биометрической системе. При этом использование биометрии для граждан должно оставаться исключительно добровольным.

Доктрина предполагает расширение сценариев применения контроля аномалий и защиты физических лиц от мошеннических действий посредством использования (но не ограничиваясь) биометрических персональных данных в связке с ЦТ.

Взаимодействие между участниками экосистемы в концепции ЦТ должно происходить на основе криптографических производных – векторов, из которых невозможно восстановить исходные данные.

С развитием технологий искусственного интеллекта возникают новые угрозы, в частности – использование дипфейков для имитации внешности и голоса пользователя с целью обхода систем безопасности или введения граждан в заблуждение о целях и намерениях злоумышленников.

Для их противодействия Доктрина закладывает переход к многофакторной защите в том числе с учетом возможностей (но не ограничиваясь) биометрических технологий. Устойчивость системы предполагает сочетание технологий контроля «живости» лица (лайвнесс), выявления атак на биометрические предъявления, инъекционных атак, новых видов биометрических персональных данных (например, ладонь) и поведенческого анализа действий пользователя.

Таким образом, ЦТ в сочетании в том числе с биометрическими технологиями может стать основой новой парадигмы безопасности, обеспечивая достоверность цифровых операций, защиту цифровой личности и создание фундамента для инновационного развития цифровой экономики Российской Федерации.

VI. Нормативное регулирование реализации Доктрины

Действующая нормативно-правовая база содержит ряд неурегулированных вопросов, требующих проработки, в том числе:

отсутствие правового механизма для реализации сервисов «обратного взыскания» похищенных средств;

отсутствие формализованных критериев эффективности работы субъектов цифровой среды по противодействию правонарушениям, совершаемым с использованием ИКТ;

отсутствие правовых механизмов, предполагающих адресную ответственность участников информационного обмена за полноту, качество, достоверность и скорость передачи данных;

недостаточная проработанность комплексного регулирования вопросов подготовки профильных кадров и системной профилактики правонарушений;

низкий уровень законодательной базы для этапа расследования, включая:

недостаточную эффективность механизмов борьбы с незаконным администрированием информационных ресурсов, заведомо предназначенных для совершения правонарушений (теневых цифровых ресурсов, функционирующих в анонимных сетях);

необходимость совершенствования нормативного регулирования процессуальных процедур, связанных с цифровой валютой (изъятие, конфискация, обращение в доход государства), а также в закреплении однозначных оснований для отнесения операций с цифровой валютой к действиям по легализации (отмыванию) имущества, полученного преступным путем;

отсутствие согласованной нормативной основы для государственно-частного взаимодействия в сфере противодействия правонарушениям, совершаемым с использованием ИКТ, в том числе в части привлечения экспертов организаций, осуществляющих деятельность в сфере ИКТ, сферы информационной безопасности и кредитных организаций к обучающим, экспертным и методическим мероприятиям;

отсутствие особенностей деятельности по правовому просвещению и правовому информированию населения в части противодействия правонарушениям, совершаемым с использованием ИКТ.

Реализация Доктрины предполагает проведение регулярного анализа правоприменительной практики с целью совершенствования законодательства, в том числе возможного исключения из нормативных правовых актов неэффективных или потерявших свою актуальность для целей борьбы с правонарушениями, совершаемыми с использованием ИКТ, положений.

VII. Организационные основы обеспечения реализации Доктрины

Мониторинг реализации Доктрины осуществляется в течение всего периода ее действия на основе сбора и оценки данных о фактических значениях показателей реализации Доктрины и других связанных с ними показателях развития технологий противодействия правонарушениям

в сфере ИКТ, об осуществленных и запланированных основных мероприятиях государственной политики в сфере противодействия правонарушениям в сфере ИКТ с определением рисков и возможностей их устранения или снижения.

Конкретизация и развитие положений настоящей Доктрины, осуществляются при разработке межотраслевой стратегии развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, являющейся основным документом стратегического планирования в указанной сфере, а также других документов стратегического планирования и нормативных правовых актов.

План реализации Доктрины, кроме перечня основных мероприятий по ее реализации, включает в себя задачи, ответственных исполнителей, сроки и порядок координации деятельности и взаимодействия государственных органов и организаций при реализации Доктрины.

Мониторинг, оценку и прогнозирование состояния развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, осуществляет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации с участием заинтересованных федеральных органов исполнительной власти и организаций.

Реализация Доктрины осуществляется во взаимодействии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы безопасности Российской Федерации, Следственного комитета Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, иных заинтересованных федеральных органов исполнительной власти, при участии Генеральной прокуратуры Российской Федерации, Банка России, исполнительных органов субъектов Российской Федерации, а также организаций, в том числе кредитных организаций, операторов связи, цифровых платформ и иных организаций в сфере информационных технологий в пределах их компетенции и в порядке, не противоречащем законодательству Российской Федерации.

Мероприятия по реализации Доктрины учитываются при формировании и корректировке государственных программ Российской Федерации, программ субъектов Российской Федерации по развитию системы противодействия правонарушениям, совершаемым с использованием ИКТ.

На региональном и муниципальном уровнях в целях реализации Доктрины принимаются соответствующие целевые программы по профилактике правонарушений, совершаемых с использованием ИКТ, учитывающие положения настоящей Доктрины и плана мероприятий

по реализации Концепции, утвержденного распоряжением Правительства Российской Федерации от 14 августа 2025 г. № 2207-р.

Результаты мониторинга, оценки и прогнозирования состояния развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, отражаются в ежегодном докладе Правительства Российской Федерации Президенту Российской Федерации.

Корректировка настоящей Доктрины осуществляется по решению Президента Российской Федерации на основании предложений, подготовленных Правительством Российской Федерации с учетом результатов мониторинга, оценки и прогнозирования состояния развития системы противодействия правонарушениям, совершаемым с использованием ИКТ, а также по согласованию с Банком России в части мероприятий, влияющих на деятельность кредитных организаций и иных организаций финансового рынка.