ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 30 декабря 2024 г. № 4154-р

МОСКВА

1. Утвердить прилагаемую Концепцию государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий (далее - Концепция).

2. Федеральным органам исполнительной власти руководствоваться в своей деятельности положениями Концепции, в том числе при разработке и реализации отраслевых документов стратегического планирования, государственных программ (подпрограмм) Российской Федерации и иных документов стратегического планирования.

3. Реализация Концепции осуществляется в пределах бюджетных ассигнований, предусмотренных федеральным органам исполнительной власти в федеральном бюджете на соответствующий финансовый год и плановый период.

4. Рекомендовать органам государственной власти субъектов Российской Федерации и органам местного самоуправления руководствоваться положениями Концепции при разработке и реализации региональных программ (подпрограмм) и иных документов.

5. МВД России совместно с заинтересованными федеральными органами исполнительной власти при участии Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации и Банка России разработать и внести в 6-месячный срок в установленном порядке в Правительство Российской Федерации проект плана мероприятий по реализации Концепции.

Председатель Правительства
Российской Федерации

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
4E4B48AC2B4A4793191877D128ED7D62
Действителен с 03.05.2024 по 27.07.2025
Владелец: Правительство Российской Федерации

М.Мишустин

УТВЕРЖДЕНА
распоряжением Правительства
Российской Федерации
от 30 декабря 2024 г. № 4154-р

К О Н Ц Е П Ц И Я

государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий

I. Общие положения

Настоящая Концепция определяет принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение ее создания и функционирования.

Правовую основу настоящей Концепции составляют Конституция Российской Федерации, федеральные законы "О стратегическом планировании в Российской Федерации", "Об основах системы профилактики правонарушений в Российской Федерации", "Об информации, информационных технологиях и о защите информации", указы Президента Российской Федерации от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации", от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы", от 2 июля 2021 г. № 400 "О Стратегии национальной безопасности Российской Федерации", от 7 мая 2024 г. № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года" и иные нормативные правовые акты Российской Федерации.

Для целей реализации настоящей Концепции используются следующие основные понятия:

"государственная система противодействия противоправным деяниям, совершаемым с использованием информационно-

коммуникационных технологий" (далее - государственная система) - совокупность федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих при участии Центрального банка Российской Федерации, финансовых и иных организаций функции по выработке и реализации государственной политики в сфере противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также разработку государственных требований и правил различного уровня и направленности в указанной сфере, созданных ими консультативных, совещательных и иных органов, а также организаций, деятельность которых связана со сбором, хранением персональных данных, созданием и функционированием информационной инфраструктуры, оборотом цифровой валюты, организаций, предоставляющих услуги связи и доступа к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), потребителей указанных услуг, институтов гражданского общества, объектов информационной инфраструктуры;

"информационно-коммуникационная сфера" - совокупность информационно-телекоммуникационных сетей, включая сеть "Интернет", технологической инфраструктуры, обеспечивающей их функционирование, и различных форм человеческой активности, осуществляемой посредством их использования;

"информационно-коммуникационные технологии" - процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления;

"противоправные деяния, совершенные с использованием информационно-коммуникационных технологий" (далее - противоправные деяния) - общественно опасные деяния, за которые предусмотрена уголовная либо административная ответственность, совершенные с использованием (применением) информационно-коммуникационных технологий или в сфере компьютерной информации, в том числе с использованием (применением) электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет", информационной инфраструктуры, компьютерной техники, программных средств, онлайн-сервисов, средств коммуникации (в том числе средств мобильной связи, сервисов обмена мгновенными сообщениями, IP-телефонии), электронных средств платежа, операций с цифровой валютой и цифровыми финансовыми активами;

"средства государственной системы" - технологии, аппаратно-программные, организационные и другие средства сбора, хранения и анализа информации, предназначенные для противодействия противоправным деяниям.

Противоправные деяния с учетом критериев их квалификации классифицируются по трем основным типам:

правонарушения и преступления в сфере компьютерной информации;

правонарушения и преступления, криминообразующим или квалифицирующим признаком которых является их совершение с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет";

правонарушения и преступления, при совершении которых применение информационно-коммуникационных технологий является альтернативным способом.

Назначением государственной системы является обеспечение проведения единой государственной политики по противодействию противоправным деяниям, направленной на защиту основных прав и свобод человека и гражданина и обеспечение национальной безопасности Российской Федерации в цифровой среде.

Создание и функционирование государственной системы осуществляется на основе следующих принципов:

гарантированности конституционных прав и свобод человека и гражданина при профилактике и противодействии противоправным деяниям;

обеспечения безопасности личности, общества и государства при противодействии противоправным деяниям;

единства государственного планирования, а также координации и контроля реализации комплекса технических и организационных мер;

рациональности использования сил и средств государственной системы.

II. Современное состояние противодействия противоправным деяниям

В Российской Федерации информационное общество характеризуется широким распространением и доступностью мобильных устройств, а также беспроводных технологий и сетей связи.

Пользователями российского сегмента сети "Интернет" в 2024 году стали более 130 млн. человек, что составляет около 90 процентов населения страны, активными пользователями социальных сетей - 106 млн. человек, или более 81 процента от всех российских пользователей сети "Интернет". Электронные средства массовой информации, информационные системы, социальные сети сегодня являются частью повседневной жизни россиян. Создана система предоставления государственных и муниципальных услуг в электронной форме.

Информационно-коммуникационные технологии стали частью современных управленческих систем практически во всех сферах жизни российского общества. Развитие инструментов финансового рынка, платежных систем, а также в целом цифровизация экономических процессов дали толчок к появлению специфических способов расчетов - электронных средств платежа и их использованию юридическими и физическими лицами для безналичных расчетов.

Бесконтрольный оборот электронных средств платежа после их получения от кредитных организаций, создающий условия для их последующего использования в целях совершения незаконных действий, несет общественную опасность.

Учитывая, что в Российской Федерации сформировалось информационное общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан, злоумышленники также перестроились на совершение преступлений в информационном пространстве.

Преступные посягательства в информационно-коммуникационной сфере с каждым годом занимают все более заметное место в структуре всех зарегистрированных преступлений в стране. За последние пять лет количество таких преступлений возросло более чем в два раза (с 294,4 тыс. преступлений в 2019 году до 677 тыс. в 2023 году). Также вырос их удельный вес в числе всех зарегистрированных деяний (с 14,5 процента в 2019 году до 34,8 процента в 2023 году). В настоящее время практически каждое третье преступление совершено в информационно-коммуникационной сфере либо с использованием информационно-коммуникационных технологий.

В структуре преступлений данной категории в 2023 году преобладали кражи и мошенничества, которые составили почти три четверти таких преступлений (70,2 процента). Каждое восьмое

преступление (12 процентов) совершалось с целью незаконного производства, сбыта или пересылки наркотических средств и психотропных веществ. Экономическую направленность имеют 3,4 процента преступлений, экстремистскую направленность и террористический характер - 0,2 процента.

Также отмечается существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации, их доля в общем числе преступлений, совершаемых с использованием информационно-коммуникационных технологий, по итогам 2023 года возросла в 6,8 раза. При этом раскрываемость таких преступлений остается на крайне низком уровне (5,6 процента).

Противоправные деяния, связанные с неправомерным доступом к компьютерной информации, как правило, сопровождаются утечками конфиденциальных сведений, что может нанести ущерб как отдельным лицам, так и организациям, функционирующим в том числе в сфере оборонно-промышленного комплекса и смежных отраслях промышленности. В связи с этим необходимо создание надежного барьера противодействия посягательствам в данной сфере.

В противоправном применении информационно-коммуникационных технологий особую активность проявляют организованные преступные группы. Они используют вредоносное программное обеспечение, фишинговые сайты, специальную технику, электронные платформы и колл-центры для совершения массовых мошеннических звонков.

Анализ совершенных противоправных деяний показывает, что все более широкое распространение получают хищения кредитных денежных средств, полученных как самими потерпевшими под непосредственным влиянием злоумышленников, так и в результате доступа преступников к системам дистанционного банковского обслуживания или регистрации на сайтах микрофинансовых организаций под учетными записями граждан.

Подходы к организации дистанционного банковского обслуживания нуждаются в адаптации в целях устранения уязвимостей и минимизации возможного ущерба при оказании услуг как для граждан, так и для самих кредитных организаций. Выводу на рынок связи новых видов услуг (IP-телефония, виртуальные автоматические телефонные станции) должна предшествовать их нормативная регламентация в целях снижения рисков анонимизации фактического потребителя.

Существенное негативное влияние на криминогенную обстановку в информационно-коммуникационной сфере оказывает сложная международная ситуация, в том числе связанная с деятельностью спецслужб недружественных государств и неонацистских формирований, курируемых иностранными спецслужбами. Основная масса преступлений совершается специализирующимися на мошенничествах транснациональными организованными преступными группами, связанными с организацией хищения персональных данных граждан Российской Федерации и работой действующих с территорий недружественных государств колл-центров, с использованием которых похищаются средства граждан.

Международные преступные группы и сообщества ввиду трансграничного характера информационного пространства и отсутствия должного уровня межгосударственного взаимодействия успешно используют имеющиеся в настоящее время уязвимости в нормативно-правовом и организационно-техническом обеспечении противодействия противоправным деяниям, нанося существенный материальный и репутационный вред гражданам и организациям Российской Федерации.

Все большее распространение получает использование цифровой валюты при совершении преступлений, особенно при отмывании преступных доходов, поскольку это позволяет скрыть источник происхождения средств и конечного бенефициара - их получателя, что фактически исключает возможность выявления и конфискации использовавшейся при совершении экономических преступлений цифровой валюты.

Рост числа противоправных деяний обусловлен не только активным развитием самих информационно-коммуникационных технологий, но и виктимным поведением потерпевших, в том числе низким уровнем правовой и финансовой грамотности граждан, применением новых способов совершения противоправных деяний, наличием условий для обеспечения анонимности преступников. Несмотря на принимаемые органами государственной власти меры, направленные на борьбу с преступными и иными противоправными посягательствами, необходимый уровень информационной безопасности не достигнут.

Ситуация, складывающаяся при взаимодействии правоохранительных органов с операторами связи, провайдерами хостинга, организаторами распространения информации и иными субъектами информационного обмена, свидетельствует о необходимости

адаптации бизнес-моделей предоставления услуг потребителям в сети "Интернет" с учетом рисков криминального использования информационно-коммуникационных технологий, в том числе связанных с неправомерным или случайным доступом к персональным данным, их уничтожением, изменением, блокированием, копированием, предоставлением, распространением, а также иными неправомерными действиями в отношении персональных данных. Существенным фактором, влияющим на эффективность противодействия противоправным деяниям, является отсутствие механизма обмена в режиме реального времени информацией между указанными организациями и правоохранительными органами, в том числе обеспечивающего передачу документов распорядительного (обязательного к исполнению) характера и конфиденциальной информации.

Предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют определены Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400 "О Стратегии национальной безопасности Российской Федерации", как одни из основных задач достижения целей обеспечения государственной и общественной безопасности.

Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации и неприкосновенности частной жизни при использовании информационных технологий, отнесены к национальным интересам Российской Федерации в информационной сфере согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

Для повышения эффективности противодействия противоправным деяниям требуются согласованные действия федеральных государственных органов и органов государственной власти субъектов Российской Федерации, а также их взаимодействие с Центральным банком Российской Федерации, финансовыми и иными организациями, институтами гражданского общества.

III. Цель, задачи и функции государственной системы

Целью государственной системы является защита государства, общества и граждан от противоправных деяний.

Основными задачами государственной системы являются:

прогнозирование противоправных деяний;

выявление противоправных деяний;

повышение результативности расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий;

совершенствование законодательства в сфере противодействия противоправным деяниям;

разработка и реализация правовых, организационных, технических и иных мер противодействия противоправным деяниям;

сбор, обработка, анализ и обмен информацией в сфере противодействия противоправным деяниям;

совершенствование инструментов и механизмов противодействия преступлениям и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий;

создание подразделений, специализирующихся на противодействии противоправным деяниям;

обеспечение защищенности российского общества от противоправных посягательств в информационном пространстве, включая обеспечение безопасности персональных данных;

содействие восстановлению имущественных и иных прав граждан, нарушенных в результате совершенных в отношении их противоправных деяний, оказание им правовой и психологической помощи;

обеспечение на системной основе максимально широкого информирования населения о новых приемах совершения противоправных деяний и способах противодействия им;

развитие цифровой грамотности населения, правосознания граждан и их ответственного отношения к использованию информационно-коммуникационных технологий, в том числе потребительской и пользовательской культуры, культуры поведения в цифровом пространстве, а также содействие активному применению программно-технических средств защиты от противоправных деяний;

укрепление международного сотрудничества в сфере противодействия противоправным деяниям.

Для выполнения основных задач государственная система осуществляет реализацию следующих функций:

создание специализированной цифровой платформы, обеспечивающей оперативный обмен информацией между правоохранительными органами, Центральным банком Российской Федерации, кредитными организациями, а также операторами связи о сведениях, необходимых для установления обстоятельств противоправных деяний и лиц, их совершивших, с использованием средств мобильной связи, сервисов сети "Интернет" и иных информационных технологий (за исключением компьютерных атак и компьютерных инцидентов);

формирование и поддержание в актуальном состоянии информационных ресурсов федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих выработку и реализацию государственной политики в сфере противодействия противоправным деяниям, организаций, деятельность которых связана со сбором, хранением персональных данных, созданием и функционированием информационной инфраструктуры, оборотом цифровой валюты, кредитно-финансовых организаций, организаций, предоставляющих услуги связи и доступа к сети "Интернет";

проведение мониторинга и ограничение доступа к противоправным ресурсам в информационно-телекоммуникационных сетях, включая сеть "Интернет";

обеспечение эффективного применения норм законодательства Российской Федерации в сфере противодействия противоправным деяниям, в том числе проведение систематического мониторинга правоприменительной практики в данной сфере;

адаптация законодательства Российской Федерации под новые реалии в целях регулирования порядка оказания услуг, при котором риски их предоставления в условиях анонимизации будут полностью исключены, за нарушение порядка оказания государственных услуг введена соответствующая ответственность, а также совершенствование законодательства Российской Федерации в части организации электронного обмена данными кредитно-финансовых учреждений с органами государственной власти;

принятие на региональном и муниципальном уровнях соответствующих целевых программ, предусматривающих формирование

системы профилактики правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий;

совершенствование вопросов, связанных с порядком выпуска, обращения и реализации ограничительных процедур в отношении цифровой валюты;

реализация механизма оперативного приостановления операций с денежными средствами, электронными денежными средствами, авансовыми платежами за услуги связи, использовавшимися в преступной деятельности;

формирование у бизнес-сообщества приоритета при предоставлении услуг на соблюдение прав потребителя и обеспечение его безопасности;

оказание содействия средствам массовой информации в широком и объективном освещении деятельности государственной системы;

повышение уровня международного сотрудничества и использование накопленного международного опыта в целях противодействия противоправным деяниям;

организация и проведение научно-исследовательских и опытно-конструкторских работ по разработке и применению криминалистических средств и методов выявления, раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также сбора доказательств;

расширение практики привлечения экспертного и научного сообществ при подготовке проектов нормативных документов в сфере противодействия противоправным деяниям;

повышение уровня материального и технического оснащения федеральных государственных органов и органов государственной власти субъектов Российской Федерации, осуществляющих функции по выработке и реализации государственной политики в сфере противодействия противоправным деяниям, а также уровня правовой и социальной защищенности их сотрудников, включая обеспечение правовой защиты сотрудников правоохранительных и следственных органов, специалистов, экспертов, использующих в своей деятельности методы, сопряженные с нарушением личной, банковской и иной охраняемой федеральными законами тайны;

организация мероприятий по повышению квалификации сотрудников и работников федеральных государственных органов, органов государственной власти субъектов Российской Федерации, финансовых

и иных организаций, участвующих в противодействии противоправным деяниям;

совершенствование уголовного законодательства в части определения видов преступлений, совершенных с использованием информационно-коммуникационных технологий, а также государственной статистической отчетности о таких преступлениях;

совершенствование профилактических мер по снижению доли несовершеннолетних, вовлеченных в противоправную деятельность в информационно-коммуникационной сфере;

повышение уровня осведомленности граждан, в первую очередь пожилых, о методах совершения противоправных деяний и способах защиты от них, подготовка и размещение социальной рекламы, направленной на воспитание у граждан цифровой грамотности, с привлечением к этой деятельности представителей культуры, науки, общественности и информационного сообщества;

выстраивание эффективного международного сотрудничества с правоохранительными органами, финансовыми и иными организациями иностранных государств по противодействию противоправным деяниям с учетом необходимости преодоления двойных стандартов в подходах зарубежных партнеров к уголовному преследованию лиц, совершивших преступления, а также адекватного использования имеющихся международных правовых инструментов.

IV. Нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение создания и функционирования государственной системы

Нормативно-правовое обеспечение создания и функционирования государственной системы включает в себя:

подготовку и принятие соответствующих правовых актов, направленных на повышение эффективности деятельности государственной системы, в том числе в части фиксации и обмена соответствующей информацией;

документы стратегического планирования, разработанные на федеральном и региональном уровнях;

порядок осуществления деятельности участников государственной системы;

порядок и периодичность проведения мероприятий по оценке степени защищенности российского общества от противоправных деяний.

Нормативно-правовая база противодействия противоправным деяниям должна соответствовать следующим требованиям:

совершенствование с учетом появления новых способов и форм совершения преступлений и правонарушений;

определение компетенции участников государственной системы;

учет международного опыта, реальных системообразующих, социальных, экономических и других модернизирующих факторов;

установление ответственности физических и юридических лиц за несоблюдение требований законодательства Российской Федерации в области противодействия противоправным деяниям;

обеспечение эффективности административного и уголовного преследования за преступления и правонарушения, совершаемые с использованием информационно-коммуникационных технологий.

Научно-техническое обеспечение создания и функционирования государственной системы включает в себя:

разработку теоретических и методологических основ противодействия преступлениям и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий, рекомендаций для решения практических задач по конкретным направлениям деятельности, включая обеспечение оперативно-разыскных и иных мероприятий (контроль за условно осужденными, лицами находящимися под административным надзором, мигрантами и др.), а также специальные и экспертные исследования в области противодействия противоправным деяниям;

проведение прикладных научных исследований для принятия правовых, организационных и управленческих решений в области противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, на разных уровнях;

изучение и анализ международного опыта противодействия противоправным деяниям, внесение заинтересованными государственными органами предложений по совершенствованию мер борьбы с противоправными деяниями;

исследование основных факторов, определяющих сущность и актуальное состояние противодействия преступлениям

и правонарушениям, совершаемым с использованием информационно-коммуникационных технологий;

анализ информации о политических, социально-экономических и иных общественных процессах в Российской Федерации и мире, оказывающих негативное влияние на криминогенную ситуацию в информационно-коммуникационной сфере;

совершенствование сил государственной системы, в том числе на основе внедрения современных информационно-коммуникационных технологий, информационно-аналитического обеспечения деятельности по противодействию противоправным деяниям;

разработку и внедрение в деятельность государственных органов, органов государственной власти субъектов Российской Федерации и организаций, участвующих в противодействии противоправным деяниям, информационных банков (баз) данных, информационно-телекоммуникационных сетей, автоматизированных систем и аппаратно-программных комплексов с применением передовых информационных технологий;

своевременную подготовку предложений по созданию и совершенствованию нормативно-правовой базы информационно-аналитического обеспечения противодействия противоправным деяниям;

систематическое повышение профессиональной подготовки специалистов в области противодействия противоправным деяниям.

Приоритетными направлениями научно-технических разработок в области противодействия противоправным деяниям должны стать создание и внедрение новых программных продуктов для совершенствования деятельности сил государственной системы, способных существенно повысить эффективность борьбы с преступлениями и правонарушениями, совершаемыми с использованием информационно-коммуникационных технологий, и сократить время на проведение оперативных мероприятий.

Информационно-аналитическое обеспечение создания и функционирования государственной системы включает в себя сбор, хранение, систематизацию, анализ, оценку информации о правонарушениях и преступлениях, совершаемых с использованием информационно-коммуникационных технологий, а также обмен такой информацией с заинтересованными органами и организациями.

Информационно-аналитическое обеспечение может включать создание и разработку единого методического подхода (криминалистической методики) расследования преступлений, связанных с использованием информационно-коммуникационных технологий, который позволит аккумулировать отечественный и иностранный положительный опыт в указанном направлении в целях повышения эффективности расследования уголовных дел данной категории преступлений.

К деятельности по информационно-аналитическому обеспечению создания и функционирования государственной системы привлекаются научно-исследовательские организации, а также общественные объединения и другие институты гражданского общества.

Продуманная кадровая политика является одним из основных направлений успешного создания и функционирования государственной системы. Подразделения, участвующие в противодействии противоправным деяниям, должны быть укомплектованы высококвалифицированными специалистами, обладающими необходимыми качествами и навыками. Приоритетным направлением кадровой политики является повышение престижа службы в указанных подразделениях.

Кадровое обеспечение создания и функционирования государственной системы осуществляется по следующим основным направлениям:

систематическое повышение квалификации, подготовка и переподготовка сотрудников, участвующих в противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий;

специализация сотрудников подразделений безопасности негосударственных организаций с учетом специфики решаемых ими задач;

создание экспертно-консультативных групп из числа сотрудников, обладающих специальными знаниями и навыками.

Организационно-штатное обеспечение создания и функционирования государственной системы осуществляется за счет имеющейся штатной численности заинтересованных государственных органов и соответствующих институтов гражданского общества.

Финансовое обеспечение создания и функционирования государственной системы осуществляется за счет средств федерального

бюджета, бюджетов субъектов Российской Федерации, местных бюджетов и средств хозяйствующих субъектов.

V. Основные направления совершенствования деятельности по выявлению, раскрытию, пресечению и предупреждению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий и ожидаемые результаты реализации настоящей Концепции

Принимая во внимание специфику рассматриваемых противоправных деяний, наиболее эффективным способом их пресечения и выявления можно считать выработку модели взаимодействия правоохранительных, финансовых и иных государственных органов, а также привлечение к сотрудничеству организаций и институтов гражданского общества.

Основными направлениями совершенствования деятельности по выявлению, раскрытию, пресечению и предупреждению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, являются:

организация и проведение мероприятий, направленных на профилактику противоправных деяний;

совершенствование законодательства в сфере противодействия противоправным деяниям;

выработка дополнительного инструментария, направленного на возмещение причиненного ущерба.

Ожидаемыми результатами реализации настоящей Концепции являются:

снижение темпов прироста преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий, и увеличение доли возмещенного материального ущерба, причиненного потерпевшим;

совершенствование взаимодействия государственных органов, реализующих настоящую Концепцию;

повышение уровня раскрываемости преступлений, совершенных с использованием информационно-коммуникационных технологий;

активное участие институтов гражданского общества в профилактике и предупреждении преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий;

повышение уровня правовой, финансовой и цифровой грамотности граждан в информационно-коммуникационной сфере;

развитие эффективного международного сотрудничества в сфере противодействия противоправным деяниям.

VI. Механизмы координации и организации межведомственного взаимодействия государственных органов, организаций и институтов гражданского общества по вопросам противодействия правонарушениям и преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Реализацию настоящей Концепции осуществляют федеральные органы исполнительной власти, иные государственные органы, органы государственной власти субъектов Российской Федерации и органы местного самоуправления в соответствии с их компетенцией.

Обеспечение согласованных действий федеральных государственных органов, органов государственной власти субъектов Российской Федерации, Центрального банка Российской Федерации, финансовых и иных организаций при реализации мер в области противодействия противоправным деяниям осуществляется на площадке сформированных межведомственных комиссий, реализующих в том числе функции, направленные на обеспечение общественной безопасности и борьбу с преступностью, предупреждение преступлений и правонарушений, развитие информационных технологий и расширение их использования.

Реализация настоящей Концепции осуществляется в соответствии с планом мероприятий, утверждаемым Правительством Российской Федерации.

_____