Дата поступления рукописи в редакцию: 08.06.2026 г.
Дата принятия рукописи в печать: 20.07.2026 г.
DOI: 10.24412/2224-9133-2026-6-443-449

МАКЕЕВА Инна Владимировна,
Кандидат юридических наук, доцент ФГБОУ ВО
«МИРЭА – Российский технологический университет»,
Доцент кафедры государственно-правовых дисциплин,
e-mail: makeevainna2011@yandex.ru

КАНАТОВ Дмитрий Петрович,
ОУП ВО «Академия труда и социальных отношений»
Магистрант кафедры уголовного права,
процесса и криминалистики,
e-mail: dimakanatov@gmail.com

КИБЕРПРЕСТУПЛЕНИЯ: ВИДЫ, ОСОБЕННОСТИ РАССЛЕДОВАНИЯ И ПРОФИЛАКТИЧЕСКИЕ МЕРЫ

Аннотация. *В течение последних десятилетий повсеместное использование информационных технологий создало широкие возможности для развития самых разных сфер жизни. В то же время спектр цифровых возможностей и информационных технологий (электронные транзакции, смс-банкинг, различные приложения и пр.) приводит и к расширению сферы их применения в противозаконных целях. Такие преступления направлены как против безопасности самой информации, так и против других объектов (собственность, авторские права и пр.). Широкое распространение получили такие преступления как хищения в системе дистанционного РКО, POS-терминалов, распространение в сети противозаконной информации и пр. В статье анализируется актуальность борьбы с киберпреступностью, виды киберпреступлений, способы их совершения, а также предлагаются меры профилактики. Фокусируется внимание на особенностях расследования отдельных видов киберпреступлений. Кроме того, делается акцент на международном характере киберпреступности, рассматриваются меры, которые принимаются на государственном и межгосударственном уровнях для борьбы с данного вида преступностью.*

Ключевые слова: *киберпреступность; киберпространство; информационные технологии; виртуальная среда; расследование киберпреступлений.*

MAKEEVA Inna Vladimirovna,
PhD in Law, Associate professor Federal State
Budget Educational Institution of Higher Education
«MIREA – Russian Technological University»
Associate professor of the Department of Public Law Disciplines

KANATOV Dmitry Petrovich,
Master's Student of the Department of Criminal Law,
Process and Criminalistics Academy of Labour and Social Relations

CYBER CRIMES: TYPES, INVESTIGATION FEATURES, AND PREVENTIVE MEASURES

Annotation. *Over the past decades, the widespread use of information technology has created wide opportunities for the development of various spheres of life. At the same time, the range of digital capabilities and information technologies (electronic transactions, SMS banking, various applications, etc.) leads to the expansion of their scope for illegal purposes. Such crimes are directed both against the security of the infor-*

mation itself and against other objects (property, copyrights, etc.). Crimes such as theft in the remote-control system, POS terminals, distribution of illegal information on the network, etc. have become widespread. The article analyzes the relevance of combating cybercrime, the types of cybercrimes, and the methods of committing them, and proposes preventive measures. It focuses on the specific features of investigating certain types of cybercrimes. Additionally, the article emphasizes the international nature of cybercrime and discusses the measures taken at the national and international levels to combat this type of crime.

Key words: *cybercrime; cyberspace; information technology; virtual environment; investigation of cybercrimes.*

Сегодня в период быстрого развития цифровых технологий противоправная деятельность посягает на безопасность в сфере информации, широко используя для этого цифровые возможности. Кроме того, преступники все чаще используют цифровые технологии и сети для совершения различных видов преступлений в цифровом пространстве. Опасность проблемы киберпреступности признана на международном уровне. Это явление, свойственное не какой-либо одной стране, а в целом отражающее уровень информационного и цифрового развития в мире.

Прежде, чем рассмотреть виды киберпреступлений, обратимся к пониманию данного явления в нашей стране и за рубежом. Так, эксперты ООН под киберпреступностью понимают любые преступления, которые совершаются при помощи сети, в рамках компьютерных систем и сетей, либо против них. Международное сообщество склонно понимать киберпреступность широко, включая в это понятие не только собственно компьютерные или сетевые преступления, но и те, что совершаются посредством киберпространства. Это всякое вмешательство в работу сетей, ПО, а также прочие незаконные опасные действия с помощью компьютерных сетей или программ [2, с. 79].

Такой подход представляется верным. Ведь при более узком понимании киберпреступлений целый ряд противоправных действий с использованием ПО и электронных сетей остался бы за пределами этого понятия, и, следовательно, меры противодействия таким преступлениям не прорабатывались бы с аналогичным подходом.

В нашей стране официальное понятие киберпреступлений в уголовном законе отсутствует. В УК РФ глава 28 объединила в себе нормы о преступлениях в сфере компьютерной информации. Это преступления, посягающие на информационную безопасность и влекущие существенные последствия, в том числе возможно уничтожение данных, нарушение работы автоматизированных систем и пр. Однако неверно было бы ограничивать понятие киберпреступлений составами преступлений гл. 28 УК РФ. Действительно, в составе уголовного закона предусмотрен еще ряд составов, которые сопряжены с понятием киберпреступности. Например, это кибермошенничество (ст. 159.3, 159.6), предоставление за вознаграждение банковских счетов и иных средств платежа для незаконных операций (ст. 187), распространение противозаконной информации в сети (ч. 2 ст. 205.2, 207.1, 207.2) и др.

Сюда же следует относить любые иные преступления, которые связаны с применением информационных технологий в рамках других составов. Речь может идти, например, о нарушении авторских прав, сбыте запрещенных веществ в сети Интернет, нарушении тайны сообщений и пр.).

Если обратиться в имеющимся в доктрине теоретическим подходам к понятию киберпреступности, то, например, Т.М. Хусяинов киберпреступлением считает любое преступление в сфере информационных технологий [6, с. 120].

В свою очередь М.Е. Батухтин отмечает, что киберпреступление есть всякое преступление в электронной сфере, которое совершается с помощью компьютеров или сети, либо против них [1, с. 28].

Считаем широкий подход к определению киберпреступности обоснованным. Кроме того, в ряде развитых стран киберпреступность определяется максимально широко. Например, в США ее понимают как всякую противозаконную деятельность, связанную с компьютерными устройствами, подключенными к сети, включая мобильные телефоны, радионяню и пр. То есть, она связывается в любым электронным устройством, подключенным к сети. При этом американская юстиция делит киберпреступления на такие группы:

- деяния, где само устройство выступает целью преступления;
- в которых устройство выступает орудием;
- в которых устройства выступает как источник хранения [4, с. 79].

Полагаем, что не вполне правильно отождествлять понятие компьютерной преступности и киберпреступности. Представляется, что в случае с киберпреступностью прежде всего имеется в виду сфера осуществления преступлений (киберсреда, цифровая среда), а не использование компьютерных устройств как орудия престу-

пления. Таким образом, является актуальным такое определение киберпреступлений: преступления, совершаемые в цифровом, виртуальном пространстве, в которых компьютерные устройства, сети, иные устройства, подключенные к сети, могут применяться как орудие, цель, средство их совершения. При этом киберпреступления характеризуются рядом признаков:

1) они имеют анонимный характер, так как глобальная сеть позволяет злоумышленникам выдавать себя за других лиц, изменять свои данные;
2) высокая степень латентности: не все случаи становятся известны правоохранительным органам, отчасти ввиду незначительности убытка потерпевшего и нежелания обращаться с заявлением;
3) транснациональный характер, отсутствие как таковых территориальных границ для преступников в киберпространстве. Кроме того, технические системы и стандарты не относятся к регулируемой правом сфере;
4) профессионализм преступников: для совершения большинства киберпреступлений требуется набор знаний и навыков, не свойственный обычному пользователю.

Если говорить о разновидностях киберпреступлений, то уместной является их классификация по объекту посягательства. Так, все подобные преступления можно условно разделить на преступления:

– против таких базовых прав человека как неприкосновенность частной жизни, тайны переписки;
– против чести и достоинства. Это, прежде всего, распространение в сети клеветы и иной порочащей информации;
– против жизни и здоровья. Это, пожалуй, очень малочисленные случаи, однако возможность совершения преступления против жизни посредством сети возможно. Например, можно внести изменения в программу аппаратуры жизнеобеспечения. А пропаганда запрещенных веществ в сети приводит к утрате здоровья;
– против безопасности компьютерной информации. Речь идет о таких преступлениях как незаконный доступ к сведениям и ПО;
– против безопасности государства и правопорядка. При помощи сети Интернет злоумышленники могут получать доступ к сведениям, которые являются гостайной. Распространены публичные призывы к экстремистской деятельности, к террору;
– против международного правопорядка. К сожалению, кибертерроризм имеет транснациональный характер;
– против собственности. Это, пожалуй, наиболее часто совершаемые киберпреступления. И самый часто встречающийся в последние годы вид таких преступлений – это кибермошенничество, совершаемое разными способами и формами. Это во многом обусловлено заключением сделок удаленно, а также развитием интернет-торговли;
– финансовые преступления, которые предполагают применение фишинговых сайтов для доступа к данным клиентов финуслуг, а также к инфраструктуре финансовых организаций.

Также можно классифицировать рассматриваемые преступления по территориальному признаку: совершаемые внутри страны и транснациональные.

В зависимости от количества потерпевших можно выделить киберпреступления, от которых пострадало одно конкретное лицо или несколько лиц, либо неограниченное число пользователей.

С.И. Буз предлагает разделить все киберпреступления на две большие группы, по месту совершения и предмету посягательства:

1) компьютерные. Направлены на получение доступа к сведениям, находящимся в памяти устройства или в компьютерной сети. Предметом посягательства злоумышленников здесь будет информация, которую они собираются изменить, уничтожить, завладеть и пр.;
2) совершаемые в киберпространстве. В отличие от непосредственно компьютерных преступлений, они имеют состав, сходный с составом традиционного варианта преступления, но совершается оно в виртуальном пространстве, с применением специфических средств. Например, совершение мошенничества в области онлайн-продаж. Здесь предметом посягательства могут выступать деньги, другое имущество, запрещенные предметы, информация и пр. Подобные преступления стали совершаться почти одновременно с распространением электронных сетей в сфере экономики и торговли [2].

В литературе предлагается много вариантов классификации киберпреступлений. В том числе предлагается следующая:

– кибермошенничество;
– вымогательство;
– дропперство;
– легализация доходов;
– совершение кибератак;
– сваттинг [3, с. 65].

В связанном с киберпреступностью лексиконе часто используются англицизмы. Одним из

наиболее распространенных киберпреступлений является фишинг, целью которого является получить доступ к скрытой информации. Однако фишинг может обозначать и способ совершения других киберпреступлений, и в таком случае он означает способ передачи вредоносной программы. Двойственность данного понятия отражается также в позиции Пленума ВС РФ в Постановлении «О судебной практике по делам о мошенничестве, присвоении и растрате» [8].

Цели киберпреступлений различные, в зависимости от интересов преступников. Способы совершения таких преступлений также разнообразны. Потерпевшими могут стать самые разные люди, от взрослых состоятельных людей до подростков.

Еще одним довольно популярным видом преступлений в виртуальной среде является легализация преступных доходов. Среди неординарных способов совершения преступления – анонимные криптовалюты, применение специальных программ для создания цепочки транзакций – криптомиксеров, вывод средств через цифровые ценности (фиктивное создание, приобретение и пр.). В любом из подобных случаев действия квалифицируются по ст. 174 или 174.1 УК РФ. Далее денежные средства выводятся в наличный оборот с помощью дропперов, то есть, лиц, которые помогают обналичить средства. Такие лица чаще всего выступают исполнителями, а не организаторами преступлений. Часто они привлекаются к ответственности как соучастники или посредники. Основная роль дропперов состоит в приобретении, хранении и использовании карт банков, которые зарегистрированы на иных лиц. С помощью сети дропперов злоумышленникам удается выводить немалые суммы денег. В настоящее время действия дропперов могут квалифицироваться по ст. 174 и 187 УК, а максимальное наказание достигает семи лет заключения.

Отметим также еще одно нередко совершаемое киберпреступление – сваттинг, то есть, ложная информация об угрозе преступления. Злоумышленник в электронной или иной форме сообщает правоохранителям о наличии такой угрозы. Целью при этом может быть дестабилизация работы учреждения или госоргана, а также в ряде случаев подростки совершают его из хулиганства. Виновным может быть предъявлено обвинение по ст. 207 УК.

Эффективное противодействие киберпреступности предполагает активное взаимодействие на межгосударственном уровне и меры внутри страны. Как известно, в конце 2024 г. членами ООН была принята Конвенция против киберпреступности [9], которая на сегодня является наиболее универсальным документом в отношении преступлений в цифровой сфере. Россия также присоединилась к этому документу (соответствующее распоряжение последовало 23.10.2025 г.) [10].

Еще ранее в нашей стране введена в действие Концепция госсистемы противодействия противоправным деяниям с использованием информационных технологий [11]. На законодательном уровне продолжает совершенствоваться регулирование ответственности за преступления в сфере информации и технологий. Например, в июле 2025 г. вступили в силу дополнения в ст. 187 УК, которые предусмотрели дополнительные меры ответственности для дропперов, то есть, лиц, которые передают свои средства платежа для проведения незаконных финансовых операций.

Тем не менее, количество преступлений в сети, а также с использованием сети и ПО остается крайне высоким. Для снижения рисков стать потерпевшими от такого рода преступлений пользователям рекомендуется использовать обновленное ПО и приложения, иметь актуальное антивирусное ПО, избегать общественных сетей, и, конечно, не делать перечислений незнакомым лицам и не выполнять их указания в телефонном или интернет-режиме.

К сожалению, нередко жертвами киберпреступности становятся несовершеннолетние. Одним из наиболее тяжелых последствий воздействия на подростков является суицид. Массовое вовлечение лиц, не достигших правовой зрелости, в специально создаваемые группы в социальных сетях навязывание онлайн-книг, рекомендации конкретной литературы и обсуждения в сети в конечном итоге направлены на то, чтобы подтолкнуть человека к уходу из жизни. Подобные действия образуют составы преступлений, предусмотренных ст. 110.1 (склонение к совершению самоубийства) и ст. 110.2 УК РФ (организация деятельности, направленной на побуждение к самоубийству).

Для эффективного расследования киберпреступлений следует учитывать их характерные особенности, а также черты киберпреступников.

Чаще всего киберпреступность имеет корыстный характер, но возможны и иные мотивы преступников (самоутверждение, правовой нигилизм, реже – разрушительные, хулиганские побуждения). Тем не менее, часто для киберпреступника это является основным источником дохода. Поэтому он, как правило, совершает не одно, а серию сходных преступлений, его действия регулярны.

Также следует учитывать, что киберпреступник – это часто человек с довольно высоким уровнем образования, и он не изолирован от социума. То есть, он может получать новые знания, приобретать оборудование, осуществлять

поиск сообщников. Чаще всего это мужчины в возрасте от 18 до 35 лет, не привлекавшиеся ранее к уголовной ответственности. Киберпреступность характеризуется крайне быстрой адаптацией к новым технологиям, что делает ее одним из наиболее динамичных сегментов преступности.

Среди причин киберпреступности логично выделить как основные обширный процесс цифровизации и автоматизации, доступность, прибыльность, удаленный характер совершения преступлений, что затрудняет их раскрытие.

Как показывает статистика, в 2024 г. в нашей стране было зарегистрировано свыше 765 тыс. киберпреступлений, что на тринадцать процентов больше по сравнению с 2023 годом. По данным за 2025 г., их количество снизилось на десять процентов по сравнению с прошлым годом [12]. При этом киберпреступления приносят не только финансовый, но и репутационный и иной ущерб компаниям и физическим лицам. Для граждан совершенные в отношении них киберпреступления могут вызвать подделку их данных, подрыв доверия, панические настроения и моральный вред и пр.

Правовые меры имеют весьма важное значение для противодействия преступности. Одним из видов противодействия киберпреступникам является комплекс уголовно-правовых мер, в том числе гл. 28 УК РФ. Не менее важным является выработка концепции дальнейшего развития законодательства, а также тактическое планирование противодействия киберпреступности, в том числе идеологическое воспитание, мониторинг эффективности правоприменения.

Киберпреступники действуют агрессивно и принимают все меры к сокрытию следов, чтобы затруднить получение доказательной базы. Это определяет сложность доказывания по подобным делам. Расследование по делам о киберпреступлениях может также осложняться ввиду следующего: несвоевременное обнаружение преступления и обращения в полицию, а также несвоевременные действия следствия, из-за чего информация может быть утрачена, отсутствие должной технической оснащенности правоохранительных органов новейшими технологиями, отсутствие в их распоряжении IT-специалистов.

Традиционный подход к расследованию не дает в полной мере противостоять киберпреступности. Необходимо понимание правоохранителями специфики цифровой среды, ее трансграничного характера, умение взаимодействовать со специалистами в области цифровых технологий. К киберпреступлениям часто не применимы стандартные алгоритмы расследования, а действия, предусмотренные в процессуальном законе, не будут столь эффективны. Например, если в расследовании большинства других преступлений ключевую роль играет качественный осмотр места происшествия, то в случае с киберпреступлениями даже определить место его совершения крайне сложно. Так, при совершении атаки хакерами местом может считаться место создания вредоносного ПО, место жительства потерпевших, место нахождения преступников или иное. Кроме того, фиксацию электронных цифровых следов нельзя сравнить с фиксацией следов традиционного преступления.

Аналогично и со следственным экспериментом, при расследовании киберпреступлений, он по сути утрачивает смысл. Сложности могут возникать и с допросами лиц. Например, при допросе потерпевшего или обвиняемого они могут применять специальные термины, ссылаться на процессы, в которых следователь не может разобраться. Для помощи следствию привлекается специалист, что с одной стороны неизбежно, а с другой – дает понять обвиняемым, что следователь не разбирается во многих аспектах дела.

В расследовании киберпреступлений важно знание специфики тех или иных преступлений. Например, при получении сведений о доступе к компьютерной информации по сети компании, следователь может существенно сузить круг подозреваемых до тех, у кого был доступ к локальной сети. Ключевым элементом предмета доказывания выступают орудия и средства совершения преступления в цифровой среде [5, с. 10].

Немалую роль в расследовании киберпреступлений играют назначаемые экспертизы. С этой целью осуществляется выемка техники, при этом процесс изъятия несет риск потери информации. При необходимости назначают компьютерно-техническую экспертизу, и здесь многие исследователи и практики отмечают ряд сложностей, связанных с загруженностью учреждений и длительными сроками проведения исследований. Кроме того, проблемой может являться грамотная постановка вопросов экспертам, что связано со сложностью терминов, отсутствием специальных знаний у следователей и небольшой практикой расследования такой категории дел [7, с. 15].

Таким образом, киберпреступления представляют собой общемировую угрозу. Они подрывают компьютерную безопасность, а также общественный порядок, отношения собственности, посягают даже на государственную безопасность, на личные нематериальные блага граждан. Особую опасность киберпреступности придает ее неограниченный территориально и по кругу возможных жертв характер, а также латентность, затрудняющая выявление и расследование преступлений. С каждым годом преступники используют новые способы совершения преступлений.

Жертвами киберпреступников становятся в том числе несовершеннолетние дети, которые попадают под влияние сайтов террористической направленности, игровых сайтов, сайтов суицидальной направленности и пр. Отдельная большая проблема – кибермошенничество, в том числе на рынке сделок с недвижимостью, в онлайн-торговле.

Эффективная борьба с киберпреступностью требует не только повышения уровня законодательного регулирования ответственности за подобные деяния, но также интеграции норм права с международным правом, с учетом транснационального характера киберпреступности. Борьба с киберпреступлениями требует слаженной работы правоохранительных органов и учета всех последних изменений в цифровых технологиях.

Список литературы:

[1] Батухтин, М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия / М.Е. Батухтин // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: материалы Междунар. научной конф., 2018. – С. 28–31.

[2] Буз, С.И. Киберпреступления: понятие, сущность и общая характеристика / С.И. Буз // Юристъ-Правоведъ. – 2019. – № 4 (91). – С. 78–82.

[3] Дзетль, Р.Р., Соколенко, Н.А., Кузнецов, А.А. Виды киберпреступлений и методы их совершения / Р.Р. Дзетль, Н.А. Соколенко, Кузнецов А.А. // Цифровое право. – 2025. - № 2. – С. 64–68.

[4] Кучерков, И.А. О понятии «киберпреступление» в законодательстве и научной доктрине / И.А. Кучерков // Юридическая наука. – 2019. – № 10. – С. 78-81.

[5] Поляков, В.В. Основы методики расследования компьютерных преступлений: учебное пособие / В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2024. – 121 с.

[6] Хусяинов, Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Т.М. Хусяинов // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всеросс. круглого стола. – Иркутск, 2015. – С. 120–125.

[7] Шевко, Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения / Н.Р. Шевко // Ученые записки Казанского юридического института МВД России. – 2016. – № 1 (1). – С. 13-16.

[8] Постановление Пленума ВС РФ от 30.11.2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (ред. от 15.12.2022 г.) // Бюллетень ВС РФ. – 2018. – № 2.

[9] Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года / ООН // URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 05.05.2026).

[10] Распоряжение Президента Российской Федерации от 23.10.2025 г. № 409-рп / Официальные сетевые ресурсы Президента России // URL: http://www.kremlin.ru/acts/bank/52503 (дата обращения: 05.05.2026).

[11] См.: Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий / ЭПС «Система ГАРАНТ» // URL: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения: 05.05.2026).

[12] В России в 2024 году IT-преступления достигли пика за последние пять лет / ТАСС // URL: https://tass.ru/proisshestviya/22978955 (дата обращения 06.05.2026).

References:

[1] Batukhtin, M.E. Cybercrimes: causes, types, forms, consequences, directions of counteraction/M.E. Batukhtin//Problems and prospects for the development of the penitentiary system of Russia at the present stage: materials International. scientific conf., 2018. - S. 28-31.

[2] Buz, S.I. Cybercrimes: concept, essence and general characteristics/S.I. Buz//Lawyer-Pravoveda. – 2019. – № 4 (91). - S. 78-82.

[3] Dzetl, R.R., Sokolenko, N.A., Kuznetsov, A.A. Types of cybercrimes and methods of their commission/R.R. Dzetl, N.A. Sokolenko, Kuznetsov A.A.// Digital Law. – 2025. - № 2. - S. 64-68.

[4] Kucherkov, I.A. On the concept of “cybercrime” in legislation and scientific doctrine/I.A. Kucherkov//Legal science. – 2019. – № 10. - S. 78-81.

[5] Polyakov, V.V. Fundamentals of the methodology for investigating computer crimes: a textbook/V.V. Polyakov. - Barnaul: Publishing House Alt. University, 2024. - 121 s.

[6] Khusyainov, T.M. Internet crimes (cybercrimes) in Russian criminal law/T.M. Khusyainov// Criminal law of the Russian Federation: problems of law enforcement and prospects for improvement: all-Russian materials. round table. - Irkutsk, 2015. - S. 120-125.

[7] Shevko, N.R. Features of disclosure and investigation of cybercrimes: problems and solutions/N.R. Shevko//Scientific notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. – 2016. – № 1 (1). - S. 13-16.

[8] Resolution of the Plenum of the Armed Forces of the Russian Federation of 30.11.2017 No. 48 “On judicial practice in cases of fraud, embezzlement and embezzlement” (as amended on 15.12.2022)//Bulletin of the Armed Forces of the Russian Federation. – 2018. – № 2.

[9] United Nations Convention against Cybercrime; Strengthening international cooperation in combating certain crimes committed using information and communication systems and in the exchange of evidence in electronic form relating to serious crimes Adopted by the General Assembly in resolution 79/243 of 24 December 2024/UN//URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (accessed: 05.05.2026).

[10] Order of the President of the Russian Federation of 23.10.2025 No. 409-rp/Official Network Resources of the President of Russia//URL: http://www.kremlin.ru/acts/bank/52503 (accessed: 05.05.2026).

[11] See: Decree of the Government of the Russian Federation of December 30, 2024 No. 4154-r On approval of the Concept of the State System for Countering Illegal Acts Committed Using Information and Communication Technologies/EPS “GARANT System “//URL: https://www.garant.ru/products/ipo/prime/doc/411152413/ (date of reference: 05.05.2026).

[12] In Russia in 2024, IT crimes peaked over the past five years/TASS//URL: https://tass.ru/proisshestviya/22978955 (date of appeal 06.05.2026).