



Научно-исследовательский журнал «International Law Journal»

<https://ilj-journal.ru>

2025, Том 8, № 8 / 2025, Vol. 8, Iss. 8 <https://ilj-journal.ru/archives/category/publications>

Научная статья / Original article

Шифр научной специальности: 5.1.4. Уголовно-правовые науки (юридические науки)

УДК 343.34

Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных и цифровых технологий: научные подходы к определению и проблемы законодательного закрепления

¹Середа С.П.,

¹Вологодский институт права и экономики ФСИН России

Аннотация: статья посвящена актуальной проблеме определения и законодательного закрепления понятия преступлений, совершаемых с использованием информационно-телекоммуникационных и цифровых технологий. Автор констатирует отсутствие единого понятийного аппарата как в российском уголовном законодательстве, так и в научной доктрине, что приводит к трудностям в квалификации и расследовании таких деяний. На основе анализа норм Уголовного кодекса РФ, судебной практики и научных подходов демонстрируется терминологическая разобщенность: понятия «киберпреступление», «компьютерное преступление» и «преступление в сфере компьютерной информации» используются хаотично и не имеют четких законодательных дефиниций. В работе обосновывается широкий подход к пониманию киберпреступлений как деяний, где информационно-телекоммуникационные и цифровые технологии являются ключевым средством совершения, независимо от основного объекта посяательства. По результатам исследования сформулированы авторские определения и предложены конкретные рекомендации по совершенствованию уголовного закона, в частности, путем закрепления легальных определений ключевых понятий в примечаниях к ст. 272 УК РФ для унификации правоприменения.

Ключевые слова: киберпреступления, информационно-телекоммуникационные технологии, цифровые технологии, уголовное право, понятийный аппарат, законодательное закрепление, преступления в сфере компьютерной информации

Для цитирования: Середа С.П. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных и цифровых технологий: научные подходы к определению и проблемы законодательного закрепления // International Law Journal. 2025. Том 8. № 8. С. 207 – 214.

Поступила в редакцию: 5 сентября 2025 г.; Одобрена после рецензирования: 3 ноября 2025 г.; Принята к публикации: 16 декабря 2025 г.

The concept of crimes committed using information, telecommunication and digital technologies: scientific approaches to definition and problems of legislative consolidation

¹Sereda S.P.,

¹Vologda Institute of Law and Economics of the FPS of Russia

Abstract: the article is devoted to the urgent problem of defining and legislating the concept of crimes committed using information, telecommunication and digital technologies. The author notes the lack of a unified conceptual framework in both Russian criminal legislation and scientific doctrine, which leads to difficulties in qualifying and investigating such acts. Based on the analysis of the norms of the Criminal Code of the Russian Federation, judicial practice and scientific approaches, terminological disunity is demonstrated: the concepts of "cybercrime", "computer crime" and "computer information crime" are used chaotically and do not have clear legislative definitions. The paper substantiates a broad approach to understanding cybercrimes as acts where information, telecommunication and digital technologies are the key means of committing, regardless of the main object of the en-

croachment. Based on the results of the research, the author's definitions are formulated and specific recommendations are proposed for improving the criminal law, in particular, by consolidating legal definitions of key concepts in the notes to art. 272 of the Criminal Code of the Russian Federation for the unification of law enforcement.

Keywords: cybercrimes, information and telecommunication technologies, digital technologies, criminal law, conceptual framework, legislative consolidation, crimes in the field of computer information

For citation: Sereda S.P. The concept of crimes committed using information, telecommunication and digital technologies: scientific approaches to definition and problems of legislative consolidation. International Law Journal. 2025. 8 (8). P. 207 – 214.

The article was submitted: September 5, 2025; Approved after reviewing: November 3, 2025; Accepted for publication: December 16, 2025.

Введение

Информационно-коммуникационные и цифровых технологии получили широкое распространение, став основой современного мира. Их развитие привело к появлению новой категории преступлений, известных как киберпреступления или преступления, совершаемые с использованием информационно-телекоммуникационных и цифровых технологий (далее – ИТК и ЦТ). Современные технологии предоставляют возможность совершать преступления дистанционно, без физического контакта между преступником и жертвой, что значительно осложняет расследование и квалификацию таких деяний. Такие преступления характеризуются высоким уровнем латентности, транснациональностью и сложностью выявления и доказывания вины. Борьба с преступлениями в данной области приобрела значительную актуальность в контексте глобальной цифровизации общества. При этом киберпреступления представляют собой широкий спектр противоправных действий, осуществляемых с использованием интернета и цифровых технологий, которые требует особого внимания со стороны законодателя и правоохранительных органов.

В этой связи особую актуальность приобретает исследование и изучение понятийного аппарата и правовой регламентации преступлений, совершаемых с использованием ИТК и ЦТ на основе анализа российского законодательства, судебной практики и научных взглядов, посвященных данной тематике. Практика показывает, что существующие правовые механизмы нуждаются в совершенствовании, чтобы эффективно реагировать на новые угрозы и вызовы, связанные с развитием цифровых технологий.

Проведение исследования в рассматриваемой области имеет особое значение, учитывая то, что в настоящее время и в законодательстве и научной литературе отсутствует единый подход к определению понятия и содержания преступлений, совершаемых с использованием ИТК и ЦТ. В юридической доктрине справедливо указывается на отсутствие в отечественном законодательстве единого и четкого определения таких понятий, как «киберпреступность» и «киберпреступления». Они либо вовсе не упоминаются, либо, как в случае с «преступлениями в сфере компьютерной информации», упоминаются без должного раскрытия их содержания, что порождает в науке множество различных трактовок [1]. Это приводит к различиям в понимании составов преступлений, затрудняя работу следователей и судей.

Цель нашего исследования видится в выявлении и комплексном анализе научных подходов к определению понятия преступлений, совершаемых с использованием ИТК и ЦТ, а также систематизация проблем их законодательного закрепления для разработки научно обоснованных предложений по совершенствованию уголовного закона.

Задачи исследования – анализ и систематизация существующих в отечественной доктрине уголовного права научных подходов к определению ключевых терминов в рассматриваемой области, выявление пробелов и противоречий в используемой терминологии в уголовном законодательстве, формулирование авторского определения понятия преступления, совершаемого с использованием ИТК и ЦТ, разработка конкретных предложений и рекомендаций по совершенствованию норм уголовного права.

Гипотеза нашего исследования состоит в том, что внедрение унифицированного понятийного аппарата в действующем уголовном законодательстве в части преступлений, совершаемых с использованием ИТК и ЦТ, будет способствовать повышению эффективности борьбы с киберпреступностью.

Материалы и методы исследований

Настоящее исследование основано на применении методов анализа и синтеза для обработки научной литературы, судебной практики и формулирования выводов, формально-логического метода, сравнительно-правового метода, историко-правовой метода, системного метода, метода правового моделирования.

Эмпирическая база и материалы исследования: действующие нормативно-правовые акты, судебная практика, научные источники, статистические данные.

Результаты и обсуждения

Как отмечается в рекомендательных документах, принятых по итогам Межпарламентской Ассамблеи государств-участников СНГ в г. Санкт-Петербурге 27.11.2020, преступность в области компьютерной информации и электронной коммерции в интернете постоянно видоизменяется, однако оценить реальный масштаб исходящих от нее угроз проблематично из-за нечеткости используемых определений и терминологической путаницы [2].

Согласно статистике МВД России, в 2024 году значительную часть от общего числа правонарушений составили преступления, совершенные с применением ИТК и ЦТ. В общей структуре преступлений их доля достигла 39,9%, а их раскрываемость не превышает 28% [3]. Согласно данным, в 2024 году был зафиксирован рост числа данных деяний на 13,1% в годовом исчислении. При этом количество тяжких и особо тяжких составов увеличилось на 7,8%, что стало одним из ключевых факторов, приведших к общему росту тяжких и особо тяжких преступлений на 4,8% за указанный период [3]. Негативные тенденции демонстрирует и официальная судебная статистика. Так, начиная с 2020 г. количество лиц, осужденных по статьям главы 28 Уголовного кодекса Российской Федерации (далее – УК РФ), ежегодно растет как в абсолютных, так и в относительных цифрах доля осужденных за преступления в сфере компьютерной информации от общего числа осужденных по всем составам преступлений (с 137 осужденных или 0,02% в 2020 г. до 380 или 0,07% в 2024 г.) [4].

В УК РФ ответственность за преступления в сфере цифровой среды в первую очередь охватываются и содержатся в нормах гл. 28 "Преступления в сфере компьютерной информации" [5]. Тем не менее, к преступлениям, совершаемым с применением ИТК и ЦТ, относятся и некоторые составы, предусмотренные другими главами УК РФ. Ярким примером служат статьи 158–159.6 Главы 21 УК РФ, устанавливающие ответственность за хищения с использованием современных технологий. При этом данные нормы расположены в уголовном законе достаточно хаотично и не образуют единой системы. Дополнительную сложность создаёт отсутствие в УК РФ и иных нормативных правовых актах определений ключевых понятий, а в ряде случаев - и самих этих унифицированных понятий для данной сферы.

Российская судебная практика сталкивается со сложностями в определении и квалификации преступлений, связанных с использованием ИТК и ЦТ. Эти трудности обусловлены быстрым развитием технологий и отсутствием единого подхода к определению ключевых понятий в этой области.

В УК РФ отсутствует и не используется понятие "киберпреступления", не используется понятие "преступления, совершаемые с использованием информационно-телекоммуникационных и цифровых технологий". Вместо них в названии главы 28 УК РФ используется понятие "преступления в сфере компьютерной информации", которое не имеет легально определения в УК РФ. В данной главе, в примечании 1 к ст. 272 УК РФ, закреплено только определение понятия "компьютерная информация", являющего ключевым для всех составов преступлений данной главы.

Тем не менее, тождественное понятие "киберпреступления" активно обсуждается и используется в юридической литературе в работах различных ученых, и даже на практике. Однако единого подхода к его пониманию и определению также нет, как и нет легального юридического закрепления. Ученые предлагают разные трактовки этого понятия, и даже разные понятия, выделяя различные признаки, такие как незаконное вмешательство в работу компьютеров, создание и распространение вредоносных программ, нарушение конфиденциальности информации и другие. Такая разобщенность мнений делает невозможным формирование единой системы оценки этих преступлений, что негативно сказывается на эффективности борьбы с ними.

В современном понимании киберпреступление – это деяние, совершенное либо с применением информационных технологий, либо в информационном пространстве. При этом под технологиями подразумеваются не только технические устройства (ПК, смартфоны), но и сами данные с их носителями, а под пространством - сети типа Интернет [6, 1]. Ряд авторов отождествляет киберпреступность с преступлениями в сфере информационных технологий, определяя их как общественно опасные деяния. Такие деяния совершаются с использованием компьютерной техники и посягают на информационную безопасность, а также на системы обработки данных с помощью ЭВМ [7].

Понятийный аппарат, описывающий киберпреступность в научной и специальной литературе, крайне разнороден. Встречаются такие термины-синонимы, как «информационные преступления», «преступления в сфере высоких технологий», «преступления с использованием компьютерных технологий», «ИТ-преступления» и другие схожие по смыслу формулировки. Во многом такое разнообразие схожих понятий

объясняется отсутствие в законодательстве единого подхода к их закреплению и пониманию, вообще отсутствие легального закрепления многих понятий в данной области.

Вместе с тем, понятие «киберпреступление» можно рассматривать в качестве родового, поскольку оно выходит за рамки только преступлений против компьютерной информации (гл. 28 УК РФ) и распространяется на все деяния, совершённые с применением ИТК и ЦТ, независимо от расположения их составов в УК РФ. Понятие преступлений, совершаемых с использованием ИТК и ЦТ является наиболее близким и тождественным понятию "киберпреступления", поскольку включает в себя любое преступление, связанное с использованием таких технологий, независимо от того, на причинение вреда каким общественным отношениям в первую очередь как основному объекту они направлены. Чаще всего, основным средством совершения таких преступлений выступает информационно-телекоммуникационная система "Интернет". Киберпреступлениями следует считать не только деяния против компьютерной информации (гл. 28 УК РФ), но и множество других преступлений, где цифровые технологии используются как инструмент. Яркими примерами служат:

Убийство с публичной демонстрацией в интернете (п. "о" ч. 2 ст. 105 УК РФ);

Доведение до самоубийства (п. "д" ч. 2 ст. 110 УК РФ) или склонение к нему (п. "д" ч. 3 ст. 110.1 УК РФ) в сети;

Клевета с использованием Интернета (ч. 2 ст. 128.1 УК РФ);

Организация азартных игр через сеть (ст. 171.2 УК РФ);

Публичные призывы к терроризму с использованием интернета (ч. 2 ст. 205.2 УК РФ);

Незаконный оборот оружия (п. "в" ч. 3 ст. 222 УК РФ) или наркотиков (п. "б" ч. 2 ст. 228.1 УК РФ), осуществляемый через Интернет.

При этом важно отметить два ключевых аспекта такой квалификации. Во-первых, во всех перечисленных случаях основной объект преступления – это не отношения в сфере компьютерной информации (безопасность данных), а другие охраняемые законом блага (жизнь, здоровье, общественная безопасность). Информационные технологии выступают именно средством совершения преступления, а не его предметом. Во-вторых, использование Интернета и цифровых технологий в большинстве из приведенных составов является квалифицирующим (отягчающим) признаком, что повышает наказание. Примечательно, что большинство таких норм были введены в УК РФ в последние несколько лет, что отражает реакцию законодателя на новые технологические вызовы.

Таким образом, преступления с использованием ИТК и ЦТ можно определить как деяния, где эти технологии играют ключевую роль в подготовке, совершении или сокрытии противоправных действий. В отличие от этого, законодательное понятие «преступления в сфере компьютерной информации» (гл. 28 УК РФ) имеет узкое, специальное значение. Оно объединяет лишь 9 статей (ст. 272-274.5 УК РФ), которые обладают следующими отличительными чертами:

1) Родовой объект: Это преступления против общественной безопасности и порядка (Раздел IX УК РФ);

2) Непосредственный объект: Они посягают на защищенность общественных отношений в сфере обработки компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их обработки (Примечание 1 к ст. 272 УК РФ);

3) Роль технологий: В этих составах компьютерная информация, ИТК и их носители являются прежде всего предметом преступления, через который осуществляется вредоносное воздействие на охраняемые законом отношения.

4) Это специальные составы преступлений, главное назначение которых в первую очередь и заключается в охране общественных отношений в сфере компьютерной информации и против последней.

В научной литературе существует и узкий подход к определению киберпреступлений. Ряд авторов отождествляет их исключительно с деяниями, где информация является основным объектом посягательства (например, взлом баз данных). Фактически, эти исследователи используют термин «киберпреступление» как синоним «преступлениям в сфере компьютерной информации», ограничивая его лишь составами главы 28 УК РФ [8]. На наш взгляд, такой подход ошибочен, поскольку он не позволяет провести четкую границу между специальными составами главы 28 УК РФ и более широким кругом преступлений, совершаемых с использованием ИТК и ЦТ. В противовес этой точке зрения, другие исследователи для обозначения широкой категории противоправных деяний используют термин «компьютерные преступления», сознательно отделяя его от узкого понятия преступлений в сфере компьютерной информации [9]. Однако сама категория "компьютерные преступления" по своему звучанию является, на наш взгляд, неудачной, неполной и неподходящей для обозначения и замены такой широкой категории, как преступления, совершаемые с использованием ИТК и ЦТ (киберпреступления). Поэтому наиболее правильным, на наш взгляд, является по-

зиция тех авторов, которые придерживаются широкого подхода к определению киберпреступлений или преступлений, совершаемых с использованием ИТК и ЦТ, и относят к ним любые преступления, где такие технологии используются как средство, но могут быть и предметом преступления [10], [11].

Следует отметить, что не содержат единого подхода к терминологии в области борьбы с киберпреступностью и международно-правовые документы. Так, Конвенция о киберпреступности (ETS № 185), не ратифицированная Россией, использует схожий с главой 28 УК РФ термин – «преступления в сфере компьютерной информации» [12]. Однако в Конвенции это понятие трактуется шире, поскольку охватывает три группы деяний, включая иные общественно опасные преступления, совершаемые с использованием ИТК и ЦТ.

Положения главы 28 УК РФ создают правовую основу для привлечения к ответственности преступников, действующих в виртуальном пространстве. Тем не менее, как подчеркивается в Постановлении Пленума ВС РФ от 15.12.2022 № 37 [13], в борьбе с киберпреступностью ключевую роль играют и иные нормы уголовного закона. Из текста документа следует, что Верховный Суд разделяет все киберпреступления на две категории: преступления в сфере компьютерной информации (гл. 28 УК РФ); иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет", ответственность за которые предусмотрена другими статьями УК РФ.

В Постановлении Пленума ВС РФ от 15.12.2022 № 37 содержатся определения ключевых понятий, в свою очередь являющихся составной частью и раскрывающих содержание и значение основных понятий, обозначающих рассматриваемые виды преступлений. Однако определение ключевого понятия преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, в данном документе не содержится. Кроме этого, данное понятие не упоминается буквально в УК РФ.

Отличная от УК РФ терминология в сфере противодействия киберпреступности также закреплена в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (далее – Соглашение), вступившем в силу для России 17 июля 2022 года [14]. Уже из названия документа следует, что в нем используется понятие «преступления в сфере информационных технологий». Хотя в УК РФ данный термин напрямую не применяется, используемое в главе 28 УК РФ понятие «преступления в сфере компьютерной информации» является схожим по своему содержанию. В тексте указанного Соглашения отсутствует определение ключевого понятия «преступления в сфере информационных технологий», однако закреплено определение другого ключевого понятия – "информационные технологии", близкое по своему содержанию к понятию компьютерной информации, указанному в п. 1 примечаний к ст. 272 УК РФ. Однако по своему содержанию данные понятия, а именно "компьютерная информация" и "информационные технологии", не являются тождественными, равнозначными, что свидетельствует и о том, что не совпадают в полной мере и понятия "преступления в сфере компьютерной информации" и "преступления в сфере информационных технологий". Понятие «компьютерная информация» раскрывается в статье 1 Соглашения иначе, чем в примечании 1 к статье 272 УК РФ. Но в целом речь идет об одном и том же явлении, но другими словами.

Сопоставление перечисленных в ст. 3 Соглашения преступлений в сфере информационных технологий с составами преступлений гл. 28 УК РФ и другими статьями УК РФ показывает, что они выходят за рамки гл. 28 УК РФ и охватывают как деяния, схожие по своей сути с предусмотренными статьями 272, 273 и 274 УК РФ, так и иные противоправные действия, совершённые с применением электронных или информационно-телекоммуникационных сетей. Можно заключить, что понятие "преступления в сфере информационных технологий" в Соглашении имеет более широкое содержание по сравнению с понятием "преступления в сфере компьютерной информации" по гл. 28 УК РФ и фактически соответствует понятию киберпреступлений, то есть преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей. Таким образом, следует отметить некоторую несогласованность положений УК РФ и Соглашения в части используемой терминологии для обозначения соответствующих видов преступлений.

Общественные отношения, охраняемые нормами главы 28 УК РФ и другими статьями, устанавливающими ответственность за преступления с использованием ИТК и ЦТ, частично регулируются Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [15]. Этот закон содержит определения базовых понятий отрасли, таких как «информация», «информационные технологии», «информационная система» и «информационно-телекоммуникационная сеть». Вместе с тем, Закон № 149-ФЗ не оперирует понятиями «киберпреступление», «компьютерное преступление» или иными смежными терминами, поскольку установление уголовной ответственности не входит в его предмет регулирования. Вопросы преступности и наказуемости деяний остаются исключительной прерогативой УК

РФ. В то же время закон указывает на возможность привлечения к уголовной ответственности за отдельные нарушения в сфере защиты информации.

Еще одной иллюстрацией отсутствия единой терминологии в сфере противодействия киберпреступности служат положения Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646) [16]. В данном документе используется только одно обозначение и понятие преступности и преступлений в рассматриваемой области – компьютерная преступность, компьютерные преступления. При этом определения данных понятий не содержится. Тем не менее, можно предположить, что в указанной Доктрине под компьютерными преступлениями и преступностью понимается максимально широкая категория и группа преступлений, а именно все преступления, совершаемые с использованием ИТК и ЦТ, электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет".

Выводы

Таким образом, по результатам проведенного исследования можно заключить, что понятие «киберпреступления» является наиболее широким. Оно охватывает не только преступления в сфере компьютерной информации (гл. 28 УК РФ), но и все иные деяния, совершенные с использованием ИТК и цифровых технологий, ответственность за которые предусмотрена другими статьями УК РФ. Наиболее точными синонимами «киберпреступлений» выступают следующие формулировки: «компьютерные преступления» и «преступления, совершаемые с использованием информационно-телекоммуникационных и цифровых технологий» (включая сети «Интернет»). Объединяющим признаком этих понятий является сам факт использования цифровых технологий для совершения деяния, независимо от того, какой именно объект (безопасность информации, собственность, личность) является основным.

Преступления в сфере компьютерной информации – это предусмотренные главой 28 УК РФ противоправные деяния, направленные против общественной безопасности и общественного порядка, посягающие на состояние защищенности общественных отношений и установленный законом порядок в области создания, использования, сбора, передачи, хранения, распространения, обеспечения доступности, конфиденциальности и целостности, и иной обработки компьютерной информации, представляющей собой сведения (сообщения, данные, в том числе персональные данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, а также в области эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Считаем необходимым закрепить легальное определение данного понятия в примечаниях к ст. 272 УК РФ.

Для обеспечения единообразия правовой терминологии в данной сфере, целесообразно закрепить также в примечаниях к ст. 272 УК РФ определение широкого понятия: «преступления, совершаемые с использованием информационно-телекоммуникационных или цифровых технологий». Данное понятие должно объединять все смежные формулировки и охватывать: преступления в сфере компьютерной информации (гл. 28 УК РФ) и иные преступления, совершенные с применением цифровых, электронных или компьютерных технологий, информационно-телекоммуникационных систем и сетей (включая сеть «Интернет»), либо в информационном пространстве, направленные против информационной безопасности, а также против других видов безопасности общества, государства и личности, ответственность за которые предусмотрена статьями различных разделов и глав Особенной части УК РФ.

Список источников

1. Ермоленко Ю.С. Криминалистическая характеристика преступлений в сфере информационно-коммуникационных технологий // Молодой ученый. 2024. № 27 (526). С. 140 – 142.
2. О Рекомендательных типологиях новых преступлений, совершаемых с использованием информационных технологий: постановление № 51-24 Межпарламентской Ассамблеи государств-участников СНГ (Принято в г. Санкт-Петербурге 27.11.2020) // Единый реестр правовых актов и других документов СНГ. URL: <http://cis.minsk.by/> (дата обращения: 28.07.2025)
3. Состояние преступности в Российской Федерации за январь-декабрь 2024 года [Электронный ресурс]: официальный сайт МВД России. URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328/> (дата обращения: 28.07.2025)
4. Данные судебной статистики [Электронный ресурс] : официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: <https://cdep.ru/?id=79> (дата обращения: 29.07.2025)
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.11.2025) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

6. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правовед. 2019. № 4 (91). С. 78 – 82.
7. Рассолов И.М. Право и Интернет. Теория кибернетического права: монография. 3-е изд., доп. Москва : Норма: ИНФРА-М, 2022. 304 с. URL: <https://znanium.ru/catalog/product/1852692> (дата обращения: 28.07.2025)
8. Сухаренко А. Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 2 – 5.
9. Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук. Казань, 2017. 243 с.
10. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45 – 55.
11. Простосердов М.А. Экономические киберпреступления: уголовно-правовая и криминологическая характеристика: учебное пособие. Москва: ИОП РГУП, 2023. 72 с. URL: <https://znanium.ru/catalog/product/2137497> (дата обращения: 28.08.2025)
12. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [Электронный ресурс]: заключена в г. Будапеште 23.11.2001. URL: <https://base.garant.ru/4089723/> (дата обращения: 28.07.2025)
13. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Бюллетень Верховного Суда РФ. 2023. № 3.
14. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Заключено в г. Душанбе 28.09.2018) // Собрание законодательства РФ. 2022. № 33. Ст. 5883.
15. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.
16. О Доктрине информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

References

1. Ermoolenko Yu.S. Forensic characteristics of crimes in the field of information and communication technologies. Young scientist. 2024. No. 27 (526). P. 140 – 142.
2. On the Recommended Typologies of New Crimes Committed with the Use of Information Technologies: Resolution No. 51-24 of the Interparliamentary Assembly of Member Nations of the CIS (Adopted in St. Petersburg on November 27, 2020). Unified Register of Legal Acts and Other Documents of the CIS. URL: <http://cis.minsk.by/> (date of access: 07.28.2025)
3. The state of crime in the Russian Federation for January-December 2024 [Electronic resource]: official website of the Ministry of Internal Affairs of Russia. URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328/> (date of access: 28.07.2025)
4. Judicial statistics data [Electronic resource]: official website of the Judicial Department under the Supreme Court of the Russian Federation. URL: <https://cdep.ru/?id=79> (date of access: 29.07.2025)
5. Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended on 17.11.2025). Collected Legislation of the Russian Federation. 1996. No. 25. Article 2954.
6. Buz S.I. Cybercrime: concept, essence and general characteristics. Jurist-Pravoved. 2019. No. 4 (91). P. 78 – 82.
7. Rassolov I.M. Law and the Internet. Theory of Cybernetic Law: Monograph. 3rd ed., suppl. Moscow: Norma: INFRA-M, 2022. 304 p. URL: <https://znanium.ru/catalog/product/1852692> (date of access: 28.07.2025)
8. Sukharensko A.N. Legislative Support of Information Security in Russia. Russian Justice. 2018. No. 2. P. 2 – 5.
9. Gaifutdinov R.R. Concept and Qualification of Crimes against Computer Information Security: Dis. ... Cand. of Law. Kazan, 2017. 243 p.
10. Nomokonov V.A., Tropina T.L. Cybercrime as a New Criminal Threat. Criminology: Yesterday, Today, Tomorrow. 2012. No. 1 (24). P. 45 – 55.
11. Prostoserdov M.A. Economic Cybercrimes: Criminal-Law and Criminological Characteristics: Study Guide. Moscow: IOP RGUP, 2023. 72 p. URL: <https://znanium.ru/catalog/product/2137497> (date of access: 28.08.2025)

12. Convention on Cybercrime (ETS No. 185) [Electronic resource]: concluded in Budapest on 23.11.2001. URL: <https://base.garant.ru/4089723/> (date accessed: 28.07.2025)

13. On certain issues of judicial practice in criminal cases concerning crimes in the sphere of computer information, as well as other crimes committed using electronic or information and telecommunications networks, including the Internet: Resolution of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37. Bulletin of the Supreme Court of the Russian Federation. 2023. No. 3.

14. Agreement on cooperation between the member states of the Commonwealth of Independent States in combating crimes in the sphere of information technology (Concluded in Dushanbe on 28.09.2018). Collected Legislation of the Russian Federation. 2022. No. 33. Art. 5883.

15. Federal Law of July 27, 2006 No. 149-FZ (as amended on June 24, 2025) "On Information, Information Technologies, and Information Protection". Collected Legislation of the Russian Federation. 2006. No. 31 (Part 1). Art. 3448.

16. On the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation of December 5, 2016 No. 646. Collected Legislation of the Russian Federation. 2016. No. 50. Art. 7074.

Информация об авторе

Середа С.П., доцент, Вологодский институт права и экономики ФСИН России, sta-sereda2006@yandex.ru

© Середа С.П., 2025