Научная статья
УДК 343.34:004

Равиль Хасанович Гиззатуллин[1], Игорь Александрович Владимиров[2], Радмир Аузагиевич Иксанов[3]
[1, 2, 3] Уфимский университет науки и технологий, Уфа, Россия
[1] ravil73@mail.ru, ORCID: 0000-0001-7748-9113
[2] docentufa@mail.ru, ORCID: 0000-0003-0891-1573
[3] iksanov333@yandex.ru, ORCID: 0000-0002-9216-543X

ПРОБЛЕМЫ СУДЕБНОЙ ПРАКТИКИ ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. Статья посвящена проблемам правоприменения в сфере киберпреступлений, квалификации и доказывания по уголовным делам, возникающим в условиях быстрого развития цифровых технологий. Обращается внимание на недостаточную эффективность норм действующего законодательства и методик расследования, отсутствие стандартизации процессов сбора и анализа цифровых доказательств. По мнению авторов, это является одной из причин возникновения пробелов в правоприменительной практике. Судебная практика показывает, что остаются нерешенными множество проблем, связанных с квалификацией преступлений. Например, процесс квалификации неправомерного доступа к компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации) нередко вызывает разночтения среди судов относительно завершенности преступления и его материального ущерба. Существует необходимость в разъяснении позиций Пленума Верховного Суда Российской Федерации в вопросах унификации правоприменительной практики по преступлениям в сфере компьютерной информации. Значение для рассмотрения дел по информационным правонарушениям имеет разработка специализированных стандартов экспертиз и повышение квалификации сотрудников правоохранительных органов в области цифровых технологий. Актуальным является совершенствование законодательной базы для борьбы с киберпреступностью в условиях меняющейся цифровой среды. Понимание правовых вопросов, касающихся киберпреступлений, становится критически важным для формирования эффективной правоприменительной практики и обеспечения правовой безопасности в цифровом пространстве.

Ключевые слова: компьютерные преступления, уголовная ответственность, судебная практика, компьютерная информация, квалификация, неправомерный доступ

Для цитирования: Гиззатуллин Р. Х., Владимиров И. А., Иксанов Р. А. Проблемы судебной практики по преступлениям в сфере компьютерной информации // Общество, право, государственность: ретроспектива и перспектива. 2026. № 1 (25). С. 29–38.

Original article

Ravil Kh. Gizzatullin[1], Igor A. Vladimirov[2], Radmir A. Iksanov[3]
[1, 2, 3] Ufa University of Science and Technology, Ufa, Russia
[1] ravil73@mail.ru, ORCID: 0000-0001-7748-9113
[2] docentufa@mail.ru, ORCID: 0000-0003-0891-1573
[3] iksanov333@yandex.ru, ORCID: 0000-0002-9216-543X

PROBLEMS OF COURT PRACTICE IN CRIMES IN THE FIELD OF COMPUTER INFORMATION

Abstract. The article is devoted to the problems of law enforcement in the field of cybercrimes, the problems of qualification and proof in criminal cases that arise in the context of the rapid development of digital technologies. The authors draw attention to the insufficient effectiveness of the existing legislation and investigation methods, the lack of standardization of the processes of collection and analysis of digital evidence. According to the authors, this is one of the reasons for the gaps in law enforcement practice. Judicial practice shows that a host of problems relating to the qualification of offenses remains unresolved. For example, the process of qualifying unlawful access to computer information (Article 272 of the Criminal Code of the Russian Federation) often leads to differences among courts regarding the completeness of the offense and its material damage. There is a need to clarify the positions of the Plenum of the Supreme Court of the Russian Federation on the unification of law enforcement practice on crimes in the field of computer information. The importance for the consideration of information crime cases has the development of specialized peer review standards and the upskilling of law enforcement personnel in the field of digital technologies. Improving the legislative framework to tackle cybercrime in the context of the changing digital environment is relevant. Understanding the legal issues surrounding cybercrimes becomes critical to shaping effective law enforcement practice and ensuring legal safety in the digital space.

Keywords: computer crimes, criminal responsibility, trial practice, computer information, qualification, illegal access

For citation: Gizzatullin R. Kh., Vladimirov I. A., Iksanov R. A. Problems of court practice in crimes in the field of computer information // Society, law, statehood: retrospective and perspective. 2026. No. 1 (25). P. 29–38. (In Russ.)

Введение

В правоприменительной практике возникают трудности при квалификации преступлений, связанных с использованием компьютерных сетей. По мнению В. В. Полякова, при расследовании и рассмотрении уголовных дел особое внимание уделяется вопросам сбора и оценки доказательств, особенно электронных [1]. Автор выделяет несколько групп компьютерных преступлений:

1) преступления, совершаемые лицами с низкими техническими навыками: большинство преступлений осуществляется людьми, имеющими ограниченное понимание компьютерных технологий. Они используют простые методы, такие как применение стандартных программ для взлома аккаунтов или сетей;

2) преступления, совершаемые лицами с ограниченными техническими знаниями: эта группа включает лиц, имеющих базовые знания в области информационных технологий, которые позволяют им совершать преступления, такие как нелегальное подключение к Интернету или установка пиратского программного обеспечения (далее – ПО);

3) преступления, связанные с незаконным распространением нелицензионного ПО: значительное количество преступлений имеют отношение к нарушению авторских прав посредством распространения контрафактного ПО;

4) высокотехнологические преступления: самая маленькая группа, включающая высококвалифицированных специалистов, способных скрывать свою личность и деятельность, что значительно усложняет расследование.

В. В. Поляковым обозначены некоторые проблемы доказывания, обусловленные недостаточностью нормативных актов и методик расследования, отсутствием единых стандартов для фиксации и анализа цифровых следов, что, в свою очередь, усложняет сбор и оценку доказательств. Трудности с идентификацией электронных доказательств связаны также с тем, что они могут храниться на множестве носителей и не иметь четкого статуса оригинала или копии.

По мнению С. Р. Бикчентеевой и А. В. Васечкиной, существует потребность в разъяснении позиций Верховного Суда

Российской Федерации, направленных на обеспечение единообразия правоприменительной практики в делах о преступлениях в информационной среде [2]. Считаем необходимым акцентировать внимание на важности установления факта посягательства на охраняемую законом компьютерную информацию и правильного оформления доказательств.

Методы

Использованы общенаучные, частнонаучные и специальные методы познания, включая анализ и синтез, логический метод, системно-структурный, сравнительный, функциональный, формально-юридический и статистический методы.

Результаты

Судебная практика по уголовным делам, связанным с преступлениями в сфере компьютерной информации, свидетельствует о наличии проблем квалификации, доказывания и назначения наказаний за подобные правонарушения. Статистика судебных решений по киберпреступлениям, а также данные о количестве осужденных за преступления в сфере компьютерной информации и связанных с ними нарушениях указывают на растущую потребность в разъяснениях и изменениях в законодательстве, вызванную быстрым развитием цифровых технологий и увеличением числа кибератак. Судебная практика подтверждает наличие трудностей в квалификации неправомерного доступа к компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации[1] (далее – УК РФ)). Фиксируются разногласия среди судов относительно того, считать ли преступление оконченным сразу после несанкционированного доступа или только после нанесения реального ущерба. Заслуживают внимания ситуации, когда хакеры получают доступ к данным, но не используют их. Здесь мнения судов расходятся: одни считают это подготовительными действиями, другие квалифицируют как оконченное преступление.

Сложности, связанные с доказательствами киберпреступлений, включают вопросы установления виновности при создании и распространении вредоносных программ (ст. 273 УК РФ). Следует обратить внимание на проблему недостаточной определенности в законодательстве относительно понятий, используемых в киберпреступности, и на отсутствие четких критериев оценки ущерба, нанесенного компьютерам и сетям. Согласимся с мнением Ю. В. Иванова и В. Е. Новичкова, которые в качестве решений некоторых проблем предлагают разработать специализированные стандарты экспертиз, а также обучение сотрудников правоохранительных органов цифровым технологиям и повышение юридической грамотности населения в области информационной безопасности [3].

Разъяснению некоторых аспектов судебной практики по уголовным делам, связанным с преступлениями в сфере компьютерной информации, а также иными преступлениями, совершенными с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, посвящено постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37[2].

Данным постановлением определено понятие компьютерной информации как любых сведений, представленных в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. К таким средствам относятся персональные компьютеры, мобильные телефоны, планшеты и прочие устройства, способные обрабатывать информацию. Неправомерный доступ к компьютерной информации означает получение или использование информации без

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) // Собрание законодательства Российской Федерации.1996. № 25, ст. 2954.

[2] 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 Верхов. Суда Рос. Федерации от 15 дек. 2022 г. № 37 // Бюллетень Верховного Суда Российской Федерации. 2023. № 3.

согласия владельца или в нарушение нормативных требований.

Постановлением разъясняется понятие информационно-телекоммуникационной сети; указано, что Интернет является одной из форм таких сетей. Это необходимо для правильной квалификации преступлений, совершенных с их использованием. Также в данном документе уделяется внимание некоторым правилам территориальной подсудности. Устанавливается правило, согласно которому местом преступления, совершенного с использованием Интернета, является место, где обвиняемый совершил соответствующие действия. Постановлением рекомендована практика привлечения специалистов в области информационных технологий для разрешения сложных технических вопросов, возникающих в процессе судебного разбирательства. Постановление направлено на унификацию подхода судов к рассмотрению дел, связанных с киберпреступностью, и позволяет избежать разночтений в толковании норм права. Таким образом, постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 играет важную роль в обеспечении законности и справедливости судебных решений в указанной сфере.

Проблемы квалификации преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, связываются также по признаку их совершения организованной группой. По мнению А. А. Бессонова, значительное число таких преступлений остается нераскрытым, несмотря на широкую распространенность [4]. Основной причиной этого является сложность доказывания факта совершения преступления именно организованной группой. Статистика показывает, что примерно четверть всех преступлений связана с использованием цифровых технологий, большинство из которых совершаются организованными группами. Это создает серьезные трудности для правоохранительных органов в плане выявления и привлечения к ответственности всех участников таких группировок. Практика квалификации подобных преступлений различается в зависимости от региона и уровня суда. Отсутствие единого подхода к определению понятия «организованная группа» и составляющих его элементов усложняет работу следователей и судей.

Проанализируем апелляционное постановление Свердловского областного суда от 18 декабря 2017 г. по уголовному делу № 22-9487/2017[1], касающееся рассмотрения апелляционных жалоб осужденного и его адвоката на приговор Первоуральского городского суда Свердловской области от 10 октября 2017 г. Осужденный признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, повлекшем ее модификацию, совершенном из корыстной заинтересованности, по ч. 2 ст. 272 УК РФ. Преступление было совершено путем несанкционированного проникновения в электронную почту третьих лиц и отправки поддельных писем с просьбой о пожертвованиях. Решением суда первой инстанции было назначено лишение свободы сроком на 2 года 4 месяца с отбыванием наказания в исправительной колонии общего режима. На указанное решение была подана апелляционная жалоба, в которой осужденный и его защитник утверждали, что действия виновного лица следовало квалифицировать как попытку мошенничества, а не как неправомерный доступ к компьютерной информации. Суд апелляционной инстанции отклонил эти аргументы, сочтя квалификацию верной и наказание справедливым. По итогам рассмотрения дела Свердловский областной суд вынес решение (постановление) об оставлении приговора суда первой инстанции без изменения, апелляционные жалобы – без удовлетворения. Таким образом, апелляционное постановление Свердловского областного суда официально

[1] Апелляционное постановление Свердловского областного суда от 18 дек. 2017 г. по делу № 22-9487/2017. Доступ из справ.-правовой системы «КонсультантПлюс».

подтвердило законность решения нижестоящего суда.

Обратимся к определению судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 4 апреля 2024 г. по делу № 77-УД23-10-К1[1]. В Верховном Суде Российской Федерации рассматривалась кассационная жалоба адвоката на решение нижестоящих судов в отношении подсудимого К., обвиняемого в совершении ряда преступлений, связанных с нарушением авторских прав и неправомерным доступом к компьютерной информации, а именно: в неправомерном доступе к охраняемой законом компьютерной информации (ч. 2 ст. 272 УК РФ), выразившемся в модификации компьютерной информации, вызванной изменением программного обеспечения игровых консолей Sony PlayStation 3, а также в использовании и распространении компьютерных программ, предназначенных для модификации компьютерной информации и нейтрализации средств защиты (ч. 2 ст. 273 УК РФ): в использовании вредоносных программ для запуска нелицензионных игр и обхода защиты производителя.

Гражданин К. приобрел несколько игровых консолей Sony PlayStation 3, установил на них специальные программы для возможности запуска нелицензионных игр, после чего продавал консоли третьим лицам. Действия подсудимого рассматривались как нарушение авторских прав компании «Сони Интерэктив Интертеймент Инк.».

По мнению адвоката, нарушение лицензий не является основанием для квалификации преступлений по ст. 272 УК РФ, поскольку программное обеспечение консолей регулируется нормами авторского права, а не нормами УК РФ, также неправильно определены признаки преступления и осуществлена квалификация деяния. Верховный Суд Российской Федерации согласился с частью аргументов адвоката и отменил предыдущие решения, передав дело на новое апелляционное рассмотрение. Основной причиной стало неправильное применение судами понятия «компьютерная информация» и отсутствие четких доказательств наличия специальной защиты, установленной производителем, которая бы подпадала под понятие «охраняемые законом сведения».

Таким образом, Верховный Суд Российской Федерации признал необходимость повторного судебного разбирательства ввиду существенных нарушений процессуального порядка и неправильного применения норм уголовного права. Это судебное решение демонстрирует сложность юридических аспектов, связанных с киберпреступностью и защитой авторских прав в цифровой среде.

Обратимся к апелляционному постановлению Московского городского суда от 25 ноября 2013 г. по делу № 10-11502/2013[2]. Постановление касается уголовного дела, в котором трое обвиняемых осуждены за неправомерный доступ к охраняемой законом компьютерной информации, повлекший блокировку и нарушение работы системы электронных вычислительных машин (далее – ЭВМ) и их сети. Преступление было совершено группой лиц по предварительному сговору. В начале июля 2010 г. гражданин, будучи генеральным директором закрытого акционерного общества «Х», решил устранить конкурента – общество с ограниченной ответственностью (далее – ООО) «А», обеспечивающего продажу электронных авиабилетов открытого акционерного общества (далее – ОАО) «А». Для этого он поручил сотрудникам создать условия для блокировки работы сайта ООО «А». Была организована DDoS-атака, в результате которой пользователи не смогли приобрести авиабилеты на сайте ОАО «А». В судебном заседании подсудимые признали факт осуществления

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 4 апр. 2024 г. № 77-УД23-10-К1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Апелляционное постановление Московского городского суда от 25 нояб. 2013 г. по делу № 10-11502/2013. Доступ из справ.-правовой системы «КонсультантПлюс».

DDoS-атаки, но утверждали, что их действия не привели к доступу к охраняемой законом информации. Однако суд установил, что атака привела к блокировке работы системы ЭВМ ООО «А», что квалифицируется как неправомерный доступ к компьютерной информации. Подсудимые были признаны виновными и осуждены по ч. 2 ст. 272 УК РФ. Им было назначено наказание в виде лишения свободы сроком на два с половиной года с отбыванием наказания в исправительной колонии общего режима. В апелляционной жалобе адвокаты и осужденные оспаривали приговор, утверждая, что новая редакция ст. 272 УК РФ декриминализует их действия. Однако суд апелляционной инстанции оставил приговор в силе, изменив только вид исправительного учреждения, вследствие чего осужденные должны отбывать наказание в колонии-поселении. Таким образом, апелляционным постановлением подтверждена вина осужденных и правильность решения суда первой инстанции. Незначительные изменения коснулись порядка исполнения наказания.

По мнению М. А. Рухловой, необходимо внедрять современные технические средства защиты информации и организационные меры профилактики преступлений [5]. Следует сфокусироваться на проблемах квалификации и назначения наказания за киберпреступления с целью выработки путей улучшения действующего законодательства.

Изучим значение апелляционного постановления Московского городского суда от 5 августа 2013 г. по делу № 10-7098[1], касающегося рассмотрения апелляционной жалобы адвоката С. В. Никитенкова на приговор Кузьминского районного суда г. Москвы от 19 июня 2013 г. в отношении гражданина Ш. Ш. признан виновным в нарушении авторских прав и использовании вредоносных компьютерных программ, направленных на несанкционированное копирование и нейтрализацию средств защиты компьютерной информации. Он приобрел контрафактную компьютерную программу, установил ее на чужой компьютер, использовал средства обхода защиты программного продукта и получил оплату за установку программы. Суд подтвердил правильность квалификации действий Ш. и назначил наказание в виде лишения свободы условно на 1 год со штрафом в размере 30 тыс. рублей. Решением суда апелляционной инстанции наказание признано справедливым, соответствующим тяжести преступления и данным о личности виновного лица. Таким образом, Московский городской суд оставил первоначальный приговор без изменений, отклонив апелляционные доводы защиты.

Проанализируем кассационное определение Московского городского суда от 24 апреля 2013 г. по делу № 22-2480[2], касающееся уголовного дела, связанного с кражей, совершенной группой лиц по предварительному сговору, покушением на кражу и неправомерным доступом к охраняемой законом компьютерной информации. По данному делу два лица были признаны виновными в следующих преступлениях: в неправомерном доступе к охраняемой законом компьютерной информации, повлекшем модификацию и копирование информации, совершенном группой лиц по предварительному сговору; в краже, совершенной группой лиц по предварительному сговору, в особо крупном размере; в покушении на кражу, совершенном группой лиц по предварительному сговору, в крупном размере. Осужденные получили реальные сроки лишения свободы. Суд первой инстанции установил вину осужденных на основе показаний представителей потерпевших, свидетелей, результатов судебных экспертиз и других доказательств, признанных достоверными и непротиворечивыми.

[1] Апелляционное постановление Московского городского суда от 5 авг. 2013 г. по делу № 10-7098. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Кассационное определение Московского городского суда от 24 апр. 2013 г. по делу № 22-2480. Доступ из справ.-правовой системы «КонсультантПлюс».

Довод осужденного М. о снижении наказания и изменении категории преступлений был отклонен, так как суд счел назначение наказания соответствующим тяжести преступлений и данным о личности осужденных. Кассационная инстанция подтвердила правильность выводов суда первой инстанции и оставила приговор без изменений. Анализ конкретных судебных решений иллюстрирует сложность квалификации преступлений, связанных с использованием компьютерной информации и компьютерных сетей.

Обратимся к определению Верховного Суда Российской Федерации[1], которое касается рассмотрения кассационной жалобы адвоката в защиту интересов осужденного С. Дело связано с обвинением последнего в неправомерном доступе к охраняемой законом компьютерной информации и использовании компьютерных программ, предназначенных для несанкционированного блокирования такой информации. Его вина была признана судом первой инстанции, но впоследствии оспорена в апелляционном и кассационном порядке. Советским районным судом г. Липецка 5 апреля 2022 г. гр. С. был признан виновным по двум статьям УК РФ (ч. 1 ст. 272 и ч. 1 ст. 273). Впоследствии наказание было смягчено апелляционным решением Липецкого областного суда, а кассационная инстанция оставила решение без изменений. Адвокат утверждал, что доказательства виновности его клиента недостаточны и содержат ряд процессуальных нарушений. Например, суд первой инстанции неправильно определил объекты правонарушения и не учел различия между нарушениями прав интеллектуальной собственности и нарушением режима защиты информации. Было отмечено, что программа, установленная на игровую приставку, изначально имела свойство незащищенности уже до приобретения приставки осужденным, что ставит под сомнение обвинение в нарушении авторских прав.

Верховный Суд Российской Федерации признал, что нижестоящие суды не провели должного анализа обстоятельств дела и допустили серьезные нарушения процессуального порядка. В частности, речь идет о несоответствиях в квалификации деяний и неполноте исследования доказательств. Было принято решение отменить апелляционные и кассационные постановления, дело направить на новое апелляционное рассмотрение другим составом суда.

Изучим определение Московского городского суда от 21 сентября 2011 г. по делу № 22-11347[2]. Оно касается кассационного рассмотрения дела о незаконном использовании объектов авторского права и вредоносных программ для ЭВМ. Суд оставил без изменений приговор Солнцевского районного суда г. Москвы от 15 июня 2011 г., согласно которому подсудимый С. был признан виновным в трех эпизодах незаконного использования объектов авторского права и в незаконном использовании вредоносных программ для ЭВМ, которые привели к несанкционированному копированию информации. Его наказание включало условное лишение свободы на срок шесть месяцев и штрафы. Исковые заявления представителей потерпевших были переданы на рассмотрение в порядке гражданского судопроизводства. Обратимся к определению Московского городского суда от 5 сентября 2011 г. по делу № 22-11062[3]. Суд оставил без изменения приговор по делу и установил, что процедура рассмотрения дела была проведена в соответствии с нормами УК РФ и Уголовно-процессуального кодекса Российской Федерации. Суд отметил, что основания

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 17 апр. 2025 г. № 77-УД25-1-К1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Определение Московского городского суда от 21 сент. 2011 г. по делу № 22-11347. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Определение Московского городского суда от 5 сент. 2011 г. по делу № 22-11062. Доступ из справ.-правовой системы «КонсультантПлюс».

для прекращения уголовного дела в связи с примирением сторон отсутствовали, так как прекращение дела за примирением сторон является правом, а не обязанностью суда. Таким образом, кассационная жалоба адвоката и осужденной была отклонена, а приговор оставлен в силе.

Среди исследований проблем и путей совершенствования уголовно-правового законодательства Российской Федерации в сфере информационной безопасности и борьбы с киберпреступностью интерес представляет работа О. А. Савченко [6]. Автор рассматривает существующие пробелы и противоречия в действующих нормах УК РФ, относящихся к преступлениям в сфере компьютерной информации и информационно-телекоммуникационных технологий. Автор подчеркивает, что действующая глава 28 УК РФ («Преступления в сфере компьютерной информации») нуждается в модернизации. Заслуживают внимания отдельные труды авторов, исследующих терминологическую неопределенность, приводящую к трудностям в квалификации преступлений [7]. Например, различия между «преступлениями в сфере компьютерной информации» и «преступлениями в сфере информационно-телекоммуникационных технологий» создают путаницу и затрудняют эффективное применение законодательства. Также на квалификацию преступного деяния в сфере компьютерной информации оказывает существенное влияние способ совершения преступлений [8].

Компьютерные преступления включают широкий спектр деяний, начиная от взлома компьютеров и кражи информации до изготовления и распространения вредоносных программ. Они охватывают нарушения авторских прав, мошенничество, создание фальшивых документов и подделку кредитных карт. Эти преступления часто связаны с нарушением прав и интересов частных лиц, организаций и государства.

Проблема компьютерных преступлений приобрела международный масштаб, особенно с развитием Интернета. Специальная конвенция, принятая Советом Европы в 2001 г.[1], направлена на борьбу с киберпреступностью. По мнению К. И. Попова, преступления в киберпространстве характеризуются высокой степенью латентности, достигающей 80 %, что затрудняет выявление и расследование [9]. Массовая доступность компьютеров и широкополосного Интернета способствует росту числа таких правонарушений. К. И. Попов подчеркивает необходимость комплексного подхода к решению проблемы компьютерных преступлений, включая сотрудничество правоохранительных органов разных стран, разработку унифицированных норм и стандартов, а также усиление мер профилактики и защиты информации. А. М. Каримов исследует проблемы правового регулирования преступлений, связанных с использованием современных информационных и телекоммуникационных технологий [10]. Так, автор разграничивает преступления в сфере компьютерной информации и преступления, совершенные с использованием информационно-телекоммуникационных технологий.

Заключение

Анализ проблем судебной практики в области компьютерных преступлений показал, что существует необходимость дальнейшей разработки эффективных методов борьбы с киберпреступностью, включая повышение квалификации сотрудников правоохранительных органов и совершенствование законодательной базы. Понимание правоприменителями меняющейся специфики компьютерных преступлений важно для решения проблем профилактики и пресечения таких видов правонарушений. Выводы исследования имеют важное значение для дальнейшего развития правовой базы, касающейся защиты информационной инфраструктуры государства и общества.

[1] Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] : заключена в г. Будапеште 23 нояб. 2001 г. (с изм. от 28.01.2003). Доступ из справ.-правовой системы «КонсультантПлюс».

СПИСОК ИСТОЧНИКОВ

1. Поляков В. В. Анализ судебной практики Алтайского края по преступлениям в сфере компьютерной информации // Вестник Новосибирского государственного университета. Сер.: Право. 2014. Т. 10, № 1. С. 99–103.

2. Бикчентеева С. Р., Васечкина А. В. Актуальные проблемы судебной практики по уголовным делам о преступлениях в сфере компьютерной информации // Научное обеспечение агропромышленного комплекса : сб. статей по материалам 78-й науч.-практ. конф. студентов по итогам НИР за 2022 год : в 3 ч., Краснодар, 1–31 марта 2023 г. / отв. за выпуск А. Г. Кощаев. Краснодар : Кубанский государственный аграрный университет имени И. Т. Трубилина, 2023. Ч. 3. С. 41–44.

3. Иванов Ю. В., Новичков В. Е. Некоторые вопросы судебной практики по уголовным делам о преступлениях в сфере компьютерной информации // Наука и образование: отечественный и зарубежный опыт : сб. статей по материалам 78-я Междунар. науч.-практ. конф., Белгород, 23 июня 2025 г. Белгород : ООО «ГиК», 2025. С. 90–94.

4. Бессонов А. А. Проблемные вопросы установления признаков организованной группы по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий // Журнал российского права. 2024. Т. 28, № 1. С. 108–119. https://doi.org/10.61205/S160565900027800-4.

5. Рухлова М. А. Криминологические и уголовно-правовые меры борьбы с преступлениями в сфере компьютерной информации // Вестник науки. 2025. Т. 1, № 6 (87). С. 589–598.

6. Савченко О. А. Совершенствование уголовно-правового законодательства в сфере компьютерной информации на современном этапе развития информационных технологий // Законность и правопорядок в современном обществе. 2016. № 29. С. 156–161.

7. Камалиев Д. С. О соотношении понятий «преступления в сфере компьютерной информации», «компьютерные преступления», «киберпреступления» // Актуальные научные исследования в современном мире. 2021. № 4-6 (72). С. 87–90.

8. Николаев В. Ю. Способы совершения компьютерных преступлений и использование компьютерных (информационных) технологий как способ совершения преступления // Правовая идея. 2013. № 4. С. 40–44.

9. Попов К. И. Компьютерные преступления – преступления мирового масштаба // Правопорядок: история, теория, практика. 2013. № 1 (1). С. 28–31.

10. Каримов А. М. Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. 2023. Т. 14, № 1 (51). С. 75–82. https://doi.org/10.37973/KUI.2023.93.91.010.

REFERENCES

1. Polyakov V. V. Analysis of jurisprudence of computer crime for Altai region // Vestnik of Novosibirsk State University. Series: Law. 2014. Vol. 10, no. 1. P. 99–103. (In Russ.)

2. Bikchenteyeva S. R., Vasechkina A. V. Topical problems of judicial practice in criminal cases of crimes in the field of computer information // Scientific support for the agro-industrial complex : a collection of articles from the 78th scientific and practical conference of students based on the results of research and development for 2022 : in 3 parts, Krasnodar, March 1–31, 2023 / responsible for release A. G. Koshchaev. Krasnodar : Kuban State Agrarian University named after I. T. Trubilin, 2023. Part 3. P. 41–44. (In Russ.)

3. Ivanov Yu. V., Novichkov V. E. Some issues of judicial practice in criminal cases in the field of computer information // Science and education: domestic and foreign experience : collection of articles from the 78th International scientific and practical conference, Belgorord, June 23, 2025. Belgorod : OOO “GiK”, 2025. P. 90–94. (In Russ.)

4. Bessonov A. A. Problematic issues of establishing the signs of an organized group for crimes committed using information and telecommunication technologies // Journal of Russian law. Vol. 28, no. 1. P. 108–119. https://doi.org/10.61205/S160565900027800-4. (In Russ.)

5. Rukhlova M. A. Criminological and criminal-legal measures to combat crimes in sphere of computer information // Bulletin of science. 2025. Vol. 1, no. 6 (87). P. 589–598. (In Russ.)

6. Savchenko O. A. Improving criminal legislation in the field of computer information at the current stage of information technology development // Law and order in modern society. 2016. No. 29. P. 156–161. (In Russ.)

7. Kamaliyev D. S. On the relationship between the concepts of “crimes in the field of computer information”, “computer crimes”, “cybercrimes” // Topical research in the modern world. 2021. No. 4-6 (72). P. 87–90. (In Russ.)

8. Nikolaev V. Yu. Ways of commission of computer crimes and use of computer (information) technologies as way of commission of crime // Legal idea. 2013. No. 4. P. 40–44. (In Russ.)

9. Popov K. I. Computer crimes as crimes on a world scale // Legal order: history, theory, practice. 2013. No. 1 (1). P. 28–31. (In Russ.)

10. Karimov A. M. Computer crimes and crimes committed through the use of modern technology: a comparative legal aspect // Bulletin of Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2023. Vol. 14, no. 1 (51). P. 75–82. https://doi.org/10.37973/KUI.2023.93.91.010. (In Russ.)

Информация об авторах:
Гиззатуллин Р. Х. – доктор юридических наук, доцент;
Владимиров И. А. – кандидат юридических наук, доцент;
Иксанов Р. А. – без ученой степени.

Information about the authors:
Gizzatullin R. Kh. – Doctor of Law, Associate Professor;
Vladimirov I. A. – Candidate of Law, Associate Professor;
Iksanov R. A. – no academic degree.

Статья поступила в редакцию 06.11.2025; одобрена после рецензирования 13.11.2025; принята к публикации 19.03.2026.

The article was submitted 06.11.2025; approved after reviewing 13.11.2025; accepted for publication 19.03.2026.