Дата поступления рукописи в редакцию: 08.06.2026 г.
Дата принятия рукописи в печать: 03.08.2026 г.
DOI: 10.24412/2076-1503-2026-7-729-736

КИРИЛЛОВА Татьяна Константиновна,

доктор юридических наук, профессор кафедры гражданского права Санкт-Петербургского государственного университета аэрокосмического приборостроения,

e-mail: tania.kirillova.gmail.com@yandex.ru

СОСНОВСКИЙ Евгений Сергеевич,

преподаватель кафедры публичного права Санкт-Петербургского государственного университета аэрокосмического приборостроения,

e-mail: jacksos730@gmail.com

КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ТЕНДЕНЦИИ

Аннотация. *В статье рассматриваются актуальные проблемы квалификации преступлений в сфере кибербезопасности. Обосновывается, что цифровизация общественных отношений существенно изменила механизм совершения преступлений, структуру преступной деятельности, способы причинения вреда и характер доказывания. Особое внимание уделяется разграничению преступлений в сфере компьютерной информации и смежных составов: мошенничества, незаконного оборота средств платежей, нарушения тайны переписки, неправомерного доступа к охраняемой законом информации, преступлений против критической информационной инфраструктуры. Отмечается, что использование информационно-телекоммуникационных технологий не всегда означает наличие состава преступления в сфере компьютерной информации: в ряде случаев цифровая среда выступает лишь способом совершения традиционного преступления. Делается вывод о необходимости комплексного подхода к квалификации киберпреступлений, основанного на сочетании уголовно-правового, криминологического и цифрово-криминалистического анализа.*

Ключевые слова: *кибербезопасность, киберпреступность, квалификация преступлений, компьютерная информация, неправомерный доступ, вредоносные программы, цифровые доказательства, критическая информационная инфраструктура, информационно-телекоммуникационные технологии.*

KIRILLOVA Tatiana Konstantinovna,

Doctor of Law, Professor of the Department of Public Law, St. Petersburg State University of Aerospace Instrumentation

SOSNOVSKY Evgeny Sergeevich,

Lecturer at the St. Petersburg State University of Aerospace Instrumentation

QUALIFICATION OF CRIMES IN THE FIELD OF CYBERSECURITY: PROBLEMS AND TRENDS

Annotation. *The article examines current problems of criminal-law qualification of crimes in the field of cybersecurity. It is argued that the digitalization of social relations has significantly changed the mechanism of committing crimes, the structure of criminal activity, methods of causing harm and the nature of proof. Particular attention is paid to distinguishing crimes in the field of computer information from related offences: fraud, illegal circulation of payment instruments, violation of secrecy of correspondence, unlawful access to legally protected information, and crimes against critical information infrastructure. The article notes that the use of information and telecommunication technologies does not always mean the existence of a crime in the field of computer information: in some cases, the digital environment is only a method of committing a traditional crime. The author concludes that a comprehensive approach to the qualification of cybercrimes is necessary, based on a combination of criminal-law, criminological and digital-forensic analysis.*

Key words: *cybersecurity, cybercrime, qualification of crimes, computer information, unlawful access, malware, digital evidence, critical information infrastructure, information and telecommunication technologies.*

Цифровизация общественных отношений привела к существенной трансформации современной преступности. Информационно-телекоммуникационные технологии стали не только средством коммуникации, но и самостоятельной средой совершения преступлений, пространством хранения имущественных и личных ценностей, инструментом управления социально значимой инфраструктурой. В этих условиях кибербезопасность приобретает значение одного из ключевых направлений уголовно-правовой охраны.

Современная киберпреступность уже не сводится к неправомерному доступу к компьютерной информации или созданию вредоносных программ. Она включает сложные формы преступного поведения: фишинг, атаки программ-вымогателей, использование ботнетов, неправомерный оборот персональных данных, хищения с применением электронных средств платежа, атаки на критическую информационную инфраструктуру, использование криптовалют для сокрытия преступных доходов. Как справедливо отмечается в зарубежной литературе, киберпреступность развивается не только за счет технологических инноваций, но и вследствие изменения социальных практик использования цифровой среды [1; 3; 4].

Для уголовного права это означает необходимость переосмысления ряда традиционных подходов к квалификации преступлений. В цифровой среде усложняется установление объекта посягательства, момента окончания преступления, характера наступивших последствий, причинной связи, субъективной стороны и роли каждого участника. Особую проблему представляет разграничение преступлений, непосредственно посягающих на компьютерную информацию, и преступлений, в которых информационно-телекоммуникационные технологии используются только как способ совершения деяния.

Актуальность темы обусловлена также тем, что правоприменительная практика сталкивается с высокой латентностью киберпреступлений, трансграничностью атак, использованием анонимизирующих технологий, криптовалютных сервисов, облачных хранилищ и распределенных сетей. При этом неверная квалификация может привести либо к необоснованному расширению уголовной ответственности, либо к неполному отражению общественной опасности содеянного.

Цель настоящей статьи – выявить основные проблемы квалификации преступлений в сфере кибербезопасности и определить современные тенденции их уголовно-правовой оценки.

Для достижения указанной цели поставлены следующие задачи: определить содержание понятия преступлений в сфере кибербезопасности; рассмотреть особенности квалификации неправомерного доступа к компьютерной информации и оборота вредоносных программ; проанализировать проблемы разграничения киберпреступлений и смежных составов; определить значение цифровых доказательств для квалификации; сформулировать основные тенденции развития уголовно-правовой оценки преступлений в сфере кибербезопасности.

Методологическую основу исследования составили формально-юридический, системный, сравнительно-правовой, логический и криминологический методы. Использован также междисциплинарный подход, предполагающий учет технических особенностей цифровой среды при толковании признаков состава преступления.

В российском уголовном праве традиционно используется категория преступлений в сфере компьютерной информации. Она связана прежде всего с нормами главы 28 Уголовного кодекса Российской Федерации, предусматривающими ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также неправомерное воздействие на критическую информационную инфраструктуру.

Однако понятие преступлений в сфере кибербезопасности является более широким. Оно охватывает не только деяния, непосредственным объектом которых выступает безопасность компьютерной информации, но и преступления, совершаемые с использованием цифровых технологий. В отечественной литературе справедливо подчеркивается, что цифровая среда изменяет не только способ совершения преступления, но и механизм причинения вреда, структуру соучастия, характер следов преступной деятельности и особенности доказывания [14; 15].

В зарубежной доктрине для описания данного явления используется разграничение

cyber-dependent crimes (преступления, невозможные без использования цифровой среды) и cyber-enabled crimes (преступления, совершаемые с использованием цифровых технологий) [3; 4]. К первой группе относятся преступления, невозможные вне цифровой среды: неправомерный доступ, создание и распространение вредоносного программного обеспечения, DDoS-атаки, вмешательство в работу информационных систем. Ко второй группе относятся традиционные преступления, которые могут совершаться и без использования цифровых технологий, но в цифровой среде приобретают новые масштабы и формы: мошенничество, вымогательство, незаконная торговля, оборот персональных данных, распространение запрещенной информации.

Для российской квалификации данное разграничение имеет принципиальное значение. Если компьютерная информация является самостоятельным объектом посягательства, содеянное может квалифицироваться по нормам о преступлениях в сфере компьютерной информации. Если же информационно-телекоммуникационная сеть используется только как канал коммуникации или способ введения потерпевшего в заблуждение, основная квалификация должна определяться характером непосредственного объекта посягательства: собственность, личные права, общественная безопасность, порядок управления и т.д.

Так, если лицо с использованием мессенджера убеждает потерпевшего перевести денежные средства под ложным предлогом, информационная технология выступает способом обмана. В такой ситуации центральное значение имеет имущественное посягательство. Иная правовая оценка требуется, если лицо получает неправомерный доступ к учетной записи потерпевшего, изменяет данные, копирует охраняемую информацию, блокирует доступ к системе или использует вредоносную программу.

Следовательно, преступления в сфере кибербезопасности можно определить как совокупность уголовно наказуемых деяний, направленных против конфиденциальности, целостности и доступности компьютерной информации, безопасности информационной инфраструктуры либо совершаемых с использованием цифровых технологий в качестве существенного способа преступного воздействия.

Неправомерный доступ к компьютерной информации является одним из базовых составов в системе уголовно-правовой охраны кибербезопасности. Его квалификация предполагает установление нескольких ключевых обстоятельств: наличия охраняемой законом компьютерной информации, факта доступа к ней, неправомерности такого доступа, наступления предусмотренных законом последствий, а также умышленной формы вины.

Основная сложность заключается в определении неправомерности доступа. В техническом смысле доступ может осуществляться различными способами: подбором пароля, использованием похищенных учетных данных, эксплуатацией уязвимости, обходом средств идентификации и аутентификации, применением вредоносного программного обеспечения, использованием служебных полномочий вопреки установленным правилам. Однако уголовно-правовая оценка не может сводиться только к техническому факту подключения к системе.

В российской доктрине обращается внимание на то, что неправомерный доступ должен оцениваться с учетом правового режима информации, пределов предоставленных лицу полномочий, наличия либо отсутствия согласия обладателя информации, а также последствий, наступивших в результате такого доступа [16; 17]. Иными словами, необходимо установить не только то, что лицо получило техническую возможность взаимодействия с информационной системой, но и то, что оно не имело правового основания для соответствующих действий.

Особенно сложными являются ситуации, связанные с инсайдерами. Работник организации может иметь законные учетные данные и доступ к определенным информационным ресурсам, однако использовать их для копирования базы клиентов, передачи коммерчески значимых сведений конкурентам, удаления информации или изменения программных настроек. В подобных случаях вопрос о неправомерности доступа должен решаться через анализ пределов предоставленных полномочий. Если лицо имело доступ только для выполнения служебных задач, но использовало его вопреки установленному назначению и с причинением предусмотренных законом последствий, содеянное может приобретать признаки преступления в сфере компьютерной информации.

Не менее важна проблема последствий неправомерного доступа. Уголовно-правовое значение имеют уничтожение, блокирование, модификация либо копирование компьютерной информации. При этом копирование информации нередко вызывает дискуссии: в отличие от уничтожения или блокирования оно может не нарушать работоспособность системы и не лишать владельца доступа к данным. Однако незаконное копирование охраняемой информации нарушает ее конфиденциальность и может причинять существенный вред интересам

личности, организации или государства.

Таким образом, квалификация неправомерного доступа требует установления не только технического механизма проникновения, но и правового режима информации, пределов полномочий субъекта, характера совершенных операций, наступивших последствий и направленности умысла.

Создание, использование и распространение вредоносных компьютерных программ представляет собой самостоятельное направление киберпреступности. Современное вредоносное программное обеспечение используется для шифрования данных, кражи учетных данных, скрытого майнинга криптовалюты, удаленного управления устройством, перехвата сообщений, организации DDoS-атак, обхода средств защиты.

Особенность квалификации состоит в том, что вредоносная программа может выступать одновременно предметом преступления, средством его совершения и элементом преступной инфраструктуры. Лицо может разработать вредоносный код, приобрести его на теневом ресурсе, модифицировать, передать другим участникам, разместить на зараженном сайте или использовать для атаки на конкретную систему.

При этом важно разграничивать самостоятельный состав, связанный с оборотом вредоносных программ, и иные преступления, в которых такая программа является способом совершения деяния. Например, если вредоносное программное обеспечение используется для хищения денежных средств, содеянное может требовать квалификации по совокупности преступлений: как деяние, связанное с вредоносной программой, и как преступление против собственности. Если же лицо создало программу, заведомо предназначенную для неправомерного уничтожения, блокирования, модификации или копирования информации, но не применило ее к конкретной системе, возникает вопрос о моменте окончания преступления и о соотношении с приготовлением к иным преступлениям.

Существенную проблему образуют программы двойного назначения. Многие инструменты тестирования защищенности сетей, сканеры уязвимостей, средства удаленного администрирования, криптографические приложения и программы анализа трафика могут использоваться как законно, так и противоправно. Поэтому уголовно-правовая оценка не должна строиться исключительно на технической способности программы причинить вред.

Для вывода о вредоносном характере программы необходимо учитывать ее назначение, функциональные особенности, контекст создания и распространения, наличие механизмов сокрытия, обхода защиты, несанкционированного копирования или блокирования информации, а также осведомленность лица о предназначении соответствующего программного продукта. В зарубежных исследованиях отмечается, что криминальные рынки вредоносного программного обеспечения все чаще функционируют по модели сервисной экономики, когда лицо может не обладать глубокими техническими знаниями, но приобретает готовые инструменты, инструкции, инфраструктуру рассылки или аренду ботнета [2; 13]. Данное обстоятельство повышает значение доказывания субъективной стороны.

Следовательно, квалификация деяний, связанных с вредоносными программами, должна опираться не на формальное наличие программного инструмента, а на установление его вредоносного назначения, характера использования и умысла виновного.

Одной из наиболее сложных задач является разграничение преступлений в сфере компьютерной информации и смежных составов. На практике это особенно актуально для мошенничества, незаконного оборота средств платежа, нарушения тайны переписки, незаконного получения и распространения персональных данных, вымогательства и легализации преступных доходов.

В отечественной уголовно-правовой литературе неоднократно подчеркивалось, что квалификация преступления должна исходить из точного установления всех признаков состава, а не из внешнего сходства способов совершения деяния [22]. Применительно к киберпреступности это означает, что сам факт использования сети Интернет, мобильного приложения или электронного устройства еще не свидетельствует о наличии преступления в сфере компьютерной информации.

Если виновный вводит потерпевшего в заблуждение посредством сайта, телефонного звонка, электронной почты или мессенджера, а потерпевший самостоятельно переводит денежные средства, ключевым признаком выступает обман как способ завладения имуществом. В таком случае цифровая среда лишь обеспечивает коммуникацию между виновным и потерпевшим. Иная ситуация возникает, когда виновный получает неправомерный доступ к банковскому приложению, использует похищенные учетные данные, изменяет реквизиты платежа, вмешивается в работу информационной системы или применяет вредоносное программное обеспечение. Здесь посягательство может

затрагивать не только отношения собственности, но и безопасность компьютерной информации.

Особого внимания требует незаконный оборот персональных данных. Массовые утечки баз данных могут быть результатом неправомерного доступа, действий инсайдера, нарушения правил эксплуатации информационной системы либо последующей покупки уже похищенной информации. В зависимости от фактических обстоятельств содеянное может затрагивать различные объекты уголовно-правовой охраны: неприкосновенность частной жизни, тайну связи, коммерческую тайну, безопасность компьютерной информации, интересы собственности. Поэтому квалификация должна учитывать источник получения данных, способ доступа, характер информации и роль конкретного лица.

Отдельный блок составляют атаки на критическую информационную инфраструктуру. Технически они могут напоминать иные кибератаки: использование вредоносного кода, подбор учетных данных, DDoS-воздействие, эксплуатация уязвимости. Однако их повышенная общественная опасность обусловлена специальным объектом посягательства – устойчивым и безопасным функционированием информационных систем, обеспечивающих значимые сферы жизни общества и государства. Атака на сервер обычной коммерческой организации и атака на систему, связанную с энергетикой, транспортом, связью, здравоохранением или финансовой инфраструктурой, могут быть сходны по техническому механизму, но различны по юридической природе и последствиям.

Таким образом, при разграничении киберпреступлений и смежных составов необходимо исходить не из технологического ярлыка деяния – «фишинг», «ботнет», «ransomware» (вредоносная программа-вымогатель), «DDoS», а из уголовно-правовых признаков состава: объекта, объективной стороны, последствий, причинной связи, субъективной стороны и специальных признаков субъекта.

Киберпреступления часто совершаются распределенными группами, участники которых находятся в разных регионах или государствах и взаимодействуют через анонимные каналы связи. Один участник может создавать вредоносное программное обеспечение, другой – предоставлять серверную инфраструктуру, третий – осуществлять фишинговую рассылку, четвертый – выводить денежные средства через электронные кошельки или криптовалютные сервисы, пятый – легализовать преступные доходы.

Такая структура осложняет установление признаков соучастия. В классической уголовно-правовой модели необходимо доказать совместность действий, умышленный характер участия и осознание общего преступного результата. В цифровой среде эти признаки могут подтверждаться перепиской в закрытых каналах, распределением ролей, оплатой услуг, предоставлением доступа к инфраструктуре, использованием единых инструкций, технической координацией действий.

Однако недопустимо автоматически признавать соучастником всякое лицо, оказавшее техническую услугу. Например, администратор хостинга может не знать, что размещенный ресурс используется для фишинга или распространения вредоносного программного обеспечения. Иная оценка возможна, если лицо осознанно обеспечивает функционирование преступной инфраструктуры, принимает меры по сокрытию владельцев ресурса, реагирует на блокировки путем переноса данных, получает оплату в условиях очевидной анонимизации и продолжает оказывать услуги после уведомлений о противоправном характере деятельности.

Субъективная сторона имеет особое значение и при оценке программ двойного назначения. Наличие у лица технического инструмента не всегда свидетельствует о преступном умысле. Необходимо установить, осознавало ли лицо вредоносное назначение программы, намеревалось ли использовать ее для неправомерного воздействия на информацию или информационную систему, понимало ли последствия своих действий.

В современных исследованиях подчеркивается, что человеческий фактор остается центральным элементом киберпреступности: даже сложные технические атаки часто опираются на социальную инженерию, ошибку пользователя, слабую организацию информационной безопасности или инсайдерский доступ [5; 7]. Поэтому квалификация должна учитывать не только технологический механизм преступления, но и поведение конкретных лиц, их информированность, роль и направленность умысла.

Квалификация преступлений в сфере кибербезопасности тесно связана с собиранием, исследованием и оценкой цифровых доказательств. Логи доступа, IP-адреса, сведения о сетевом трафике, хеш-суммы файлов, данные доменной регистрации, криптовалютные транзакции, переписка в мессенджерах, образы жестких дисков, данные мобильных устройств и облачных хранилищ имеют значение не только для доказывания факта совершения преступления, но и для установления его юридических признаков.

Например, журналы событий могут подтверждать момент доступа,

последовательность действий и используемые учетные данные; анализ вредоносного кода – его функциональное назначение; хеш-суммы – неизменность изъятых файлов; сетевые логи – направление и интенсивность атаки; данные блокчейн-аналитики – движение похищенных средств. Без такого анализа затруднительно установить, имел ли место неправомерный доступ, произошло ли копирование или модификация информации, была ли программа вредоносной, наступили ли юридически значимые последствия.

В российской криминалистической литературе отмечается, что цифровые следы отличаются высокой изменяемостью, зависимостью от программно-аппаратной среды и необходимостью специальной экспертной интерпретации [18; 19]. Поэтому правовая квалификация не должна строиться на единственном техническом идентификаторе. IP-адрес, например, не всегда указывает на конкретное лицо, поскольку могут использоваться VPN, прокси-серверы, публичные сети Wi-Fi, ботнеты или зараженные устройства третьих лиц.

Юридически значимая связь между деянием и конкретным субъектом должна подтверждаться совокупностью доказательств: результатами осмотров и экспертиз, сведениями о платежах, перепиской, данными об устройствах, логами авторизации, показаниями свидетелей, информацией о владении учетными записями, а также иными цифровыми и традиционными доказательствами.

В связи с этим цифровые доказательства выполняют двойную функцию. С одной стороны, они позволяют установить фактический механизм кибератаки. С другой стороны, они помогают определить уголовно-правовые признаки состава: способ совершения преступления, последствия, причинную связь, форму вины, роль соучастников и момент окончания преступления.

Анализ современной доктрины и практики позволяет выделить несколько тенденций квалификации преступлений в сфере кибербезопасности.

Первая тенденция состоит в расширении значения цифрового способа совершения преступления. Информационные технологии все чаще рассматриваются не как нейтральный канал коммуникации, а как фактор, повышающий общественную опасность деяния. Это связано с масштабируемостью атак, возможностью автоматизации, трансграничностью, высокой латентностью и сложностью идентификации виновных лиц.

Вторая тенденция заключается в усилении уголовно-правовой защиты критической информационной инфраструктуры. В современном обществе нарушение работы информационных систем может привести не только к имущественному ущербу, но и к сбоям в энергетике, транспорте, здравоохранении, связи, финансовой системе. Поэтому атаки на такие объекты требуют самостоятельной и более строгой уголовно-правовой оценки.

Третья тенденция выражается в увеличении числа ситуаций, когда требуется квалификация по совокупности преступлений. Одна кибератака может одновременно затрагивать отношения собственности, безопасность компьютерной информации, тайну связи, персональные данные, коммерческую тайну и порядок функционирования организации. Ограничение квалификации одним составом не всегда отражает полный объем общественной опасности.

Четвертая тенденция связана с необходимостью разграничения уголовной, административной, гражданско-правовой и дисциплинарной ответственности. Нарушение пользовательского соглашения, корпоративной политики информационной безопасности или внутренних правил доступа само по себе не всегда должно влечь уголовную ответственность. Уголовное право должно сохранять значение крайнего средства реагирования и применяться при наличии общественно опасного деяния, содержащего все признаки состава преступления.

Пятая тенденция состоит в росте значения междисциплинарной компетенции правоприменителя. Корректная квалификация киберпреступлений невозможна без понимания особенностей облачных сервисов, сетевых протоколов, вредоносного программного обеспечения, криптовалютных операций, цифровых следов и методов компьютерно-технической экспертизы. При этом техническое описание деяния должно быть переведено на язык уголовно-правовых признаков состава преступления.

Наконец, шестая тенденция связана с транснационализацией киберпреступности. Преступник, потерпевший, сервер, платежная инфраструктура и цифровые следы могут находиться в разных государствах. Это осложняет не только расследование, но и юридическую оценку места совершения преступления, роли соучастников и объема причиненного вреда.

Заключение

Квалификация преступлений в сфере кибербезопасности является одной из наиболее сложных проблем современного уголовного права. Ее сложность обусловлена не только технологической новизной способов совершения преступлений, но и трансформацией самих общественных отношений, охраняемых

уголовным законом.

Основной вывод состоит в том, что преступления в сфере кибербезопасности не могут квалифицироваться исключительно через техническое описание деяния. Термины «фишинг», «ботнет», «ransomware», «DDoS-атака», «вредоносный код» имеют важное криминалистическое значение, однако уголовно-правовая оценка должна опираться на признаки состава преступления: объект, объективную сторону, последствия, причинную связь, субъективную сторону и признаки субъекта.

Представляется необходимым различать две группы преступлений: во-первых, деяния, непосредственно посягающие на компьютерную информацию и информационную инфраструктуру; во-вторых, традиционные преступления, совершаемые с использованием информационно-телекоммуникационных технологий. Такое разграничение позволяет избежать как необоснованного расширения уголовной ответственности, так и недооценки общественной опасности современных цифровых атак.

Для повышения качества квалификации киберпреступлений необходимо развитие единообразной судебной практики, повышение технической компетентности следователей, прокуроров, судей и экспертов, уточнение критериев неправомерности доступа, выработка подходов к оценке программ двойного назначения, совершенствование методик исследования цифровых доказательств и учет транснационального характера киберпреступности.

Список литературы:

[1] Lavorgna A. Cybercrimes: Critical Issues in a Global Context. London: Palgrave Macmillan, 2020.

[2] Holt T.J., Bossler A.M., Seigfried-Spellar K.C. Cybercrime and Digital Forensics: An Introduction. 3rd ed. New York: Routledge, 2022.

[3] The Oxford Handbook of Cyber Security / ed. by P. Cornish. Oxford: Oxford University Press, 2021

[4] Yar M., Steinmetz K.F. Cybercrime and Society. 3rd ed. London: SAGE Publications, 2019.

[5] Leukfeldt E.R., Holt T.J. The Human Factor of Cybercrime. London; New York: Routledge, 2019.

[6] Clough J. Principles of Cybercrime. 2nd ed. Cambridge: Cambridge University Press, 2015.

[7] Gillespie A.A. Cybercrime: Key Issues and Debates. London; New York: Routledge, 2016.

[8] Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007.

[9] Brenner S.W. Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston: Northeastern University Press, 2012.

[10] Kerr O.S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes // New York University Law Review. 2003. Vol. 78. No. 5. P. 1596–1668.

[11] Kerr O.S. Norms of Computer Trespass // Columbia Law Review. 2016. Vol. 116. No. 4. P. 1143–1184.

[12] Button M., Cross C. Cyber Frauds, Scams and Their Victims. London; New York: Routledge, 2017.

[13] Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses / ed. by T.J. Holt, A.M. Bossler. London; New York: Routledge, 2016.

[14] Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: монография. М.: Юрлитинформ, 2021.

[15] Уголовное право России. Особенная часть: учебник / под ред. А.И. Рарога. М.: Проспект, 2022.

[16] Комментарий к Уголовному кодексу Российской Федерации: в 4 т. Т. 4. Особенная часть. Разделы X–XII / отв. ред. В.М. Лебедев. М.: Юрайт, 2023.

[17] Российское уголовное право. Особенная часть: учебник / под ред. В.С. Комиссарова. М.: Проспект, 2021.

[18] Криминалистика: учебник / под ред. Е.П. Ищенко. М.: Проспект, 2022.

[19] Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. М.: Норма; ИНФРА-М, 2021.

[20] Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / под ред. Н.А. Лопашенко. М.: Юрлитинформ, 2016.

[21] Бриллиантов А.В. Уголовное право России. Части Общая и Особенная: учебник. М.: Проспект, 2021.

[22] Кудрявцев В.Н. Общая теория квалификации преступлений. М.: Юридическая литература, 1972.

References:

[1] Lavorgna A. Cybercrimes: Critical Issues in a Global Context. London: Palgrave Macmillan, 2020.

[2] Holt T.J., Bossler A.M. , Seigfried-Spellar K.C. Cybercrime and Digital Forensics: An Introduction. 3rd ed. New York: Routledge, 2022.

[3] The Oxford Handbook of Cyber Security

/ ed. by P. Cornish. Oxford: Oxford University Press, 2021

[4] Yar M., Steinmetz K.F. Cybercrime and Society. 3rd ed. London: SAGE Publications, 2019.

[5] Leukfeldt E.R., Holt T.J. The Human Factor of Cybercrime. London; New York: Routledge, 2019.

[6] Clough J. Principles of Cybercrime. 2nd ed. Cambridge: Cambridge University Press, 2015.

[7] Gillespie A.A. Cybercrime: Key Issues and Debates. London; New York: Routledge, 2016.

[8] Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007.

[9] Brenner S.W. Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston: Northeastern University Press, 2012.

[10] Kerr O.S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes // New York University Law Review. 2003. Vol. 78. No. 5. P. 1596–1668.

[11] Kerr O.S. Norms of Computer Trespass // Columbia Law Review. 2016. Vol. 116. No. 4. P. 1143–1184.

[12] Button M., Cross C. Cyber Frauds, Scams and Their Victims. London; New York: Routledge, 2017.

[13] Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses / ed. by T.J. Holt, A.M. Bossler. London; New York: Routledge, 2016.

[14] E.A. Russkevich. Criminal law counteraction to crimes committed using information and communication technologies: monograph. M.: Yurlitinform, 2021.

[15] Russian criminal law. Special part: textbook/ed. A.I. Raroga. M.: Prospect, 2022.

[16] Commentary to the Criminal Code of the Russian Federation: 4 vol. 4. Special part. Sections X-XII/resp. ed. V.M. Lebedev. M.: Yurayt, 2023.

[17] Russian criminal law. Special part: textbook/ed. V.S. Komissarova. M.: Prospect, 2021.

[18] Forensics: textbook/ed. E.P. Ishchenko. M.: Prospect, 2022.

[19] Rossinskaya E.R. Forensic examination in civil, arbitration, administrative and criminal proceedings: monograph. M.: Norma; INFRA-M, 2021.

[20] Cybercrime: criminological, criminal law, criminal procedure and forensic analysis: monograph/ ed. N.A. Lopashenko. M.: Yurlitinform, 2016.

[21] A.V. Brilliantov. Criminal Law of Russia. Parts General and Special: textbook. M.: Prospect, 2021.

[22] Kudryavtsev V.N. General theory of crime qualification. M.: Legal literature, 1972.