О совершенствовании названия главы 28 Уголовного кодекса Российской Федерации

Мосечкин Илья Николаевич
кандидат юридических наук, доцент, доцент кафедры уголовного права, процесса и национальной безопасности, юридический институт, Вятский государственный университет, usr09858@vyatsu.ru

Статья посвящена анализу названия главы 28 УК РФ в контексте соответствия родовому и видовому объектам посягательств, а также содержанию включенных в нее статей. Для структурных элементов уголовного закона наиболее типичной является словесная конструкция «преступления против», однако глава 28 УК РФ является одним из немногочисленных исключений. Автор доказывает, что указание на сферу компьютерной информации в большей степени характеризует специфику соответствующих преступлений и место их совершения, чем объект. В статье также обосновывается, что категория «компьютерная информация» является устаревшей и не такой точной, по сравнению с категорией «цифровая информация». Не соответствует действующее название главы 28 УК РФ и ее содержанию, которое существенно расширилось после введения статей 272.3-272.4 УК РФ, посвященных противодействию преступления не только против безопасности цифровой информации, но и связи. В многочисленных работах ученых прогнозируется дальнейшая криминализация общественно опасных деяний, в том числе связанных с искусственным интеллектом. На основе проведенного исследования автор предлагает сменить название главы 28 УК РФ «Преступления против безопасности цифровой информации, искусственного интеллекта и связи».

Ключевые слова: компьютерная информация, цифровая информация, безопасность, искусственный интеллект, связь, название, ЭВМ.

Введение

В последнее время сформировалась тенденция к повышению частоты внесения изменений в Уголовный кодекс Российской Федерации. В частности, в 2019 году поправки вносились 12 федеральными законами, в 2020 году – их число составило 13, в 2022 году – 11, в 2023 году – 13, а в 2024 году – 20. Таким образом, система уголовного законодательства находится практически в непрерывном реформировании. К динамике вносимых изменений можно относиться как положительно, так и отрицательно, однако вызвана она вполне конкретными причинами, к которым относятся, например: развитие регулируемых общественных отношений, коррекция выявленных судебно-следственной практикой недостатков, внутриполитическими и внешнеполитическими реалиями.

Положения об ответственности за совершение компьютерных преступлений в данном контексте исключением не являются. В первоначальной редакции УК РФ и на протяжение множества лет после его принятия глава 28 содержала всего 3 статьи, которые охватывали наиболее типичные преступления. Однако научно-технический прогресс привел к повсеместному распространению технологий и переосмыслению отношения к ним в обществе. Новые угрозы обусловили появление новых правовых средств защиты. По объективным причинам была установлена ответственность за посягательства на критическую информационную инфраструктуру, за нарушение ряда правил, связанных с установкой и модернизацией технических средств противодействия угрозам функциональности сети «Интернет», за незаконный оборот персональных данных. 2025 год стал примечательным в контексте введения в УК РФ сразу нескольких статей, регулирующих ответственность за нарушения в сфере связи. Таким образом, некогда небольшая по количеству составов преступлений глава 28 УК РФ существенно расширилась. Исследование настоящей темы базируется на гипотезе о несоответствии названия главы 28 УК РФ как видовому объекту посягательств, закрепленных в ст. 272-274.5 УК РФ, так и содержанию данных статей. Научное предположение построено в том числе на встречающихся в научной литературе доводах о некорректном названии, расположении главы в структуре уголовного закона и выделении самостоятельного раздела о компьютерных преступлениях.

Основная часть

Соотношение названия главы 28 УК РФ с объектом преступления

Сущность объекта преступления не является предметом данного исследования, поэтому в ходе анализа научной литературы были отобраны источники, авторы которых придерживаются как ценностной концепции, так и концепции общественных отношений. В доктрине принято полагать, что основой систематизации Особенной части УК РФ послужили родовой и видовой объекты посягательств [3, с. 41]. Исходя из этого сформулированы названия разделов и глав, определена последовательность статей. Обычно законодатель прямо указывает на объект посредством словесной конструкции «преступления против». Таким образом в законе отражены, например, общественные отношения, охраняющие жизнь и здоровье, обеспечивающие правосудие и другие. Однако избранный законодателем подход содержит исключения. К ним относятся главы 22, 26 и 28 УК РФ, в заголовках которых словесная конструкция «преступления против» не используется. Возможно, отчасти из-за указанной выше особенности названия в науке уголовного права не сложилось однозначного понимания видового объекта рассматриваемых в настоящем исследовании преступлений. Большинство авторов так или иначе связывают видовой объект с компьютерной информацией, а именно с интересами в области безопасности ее создания, использования и распространения. Такой вывод по итогам анализа ряда теоретических трудов сделал К. Н. Евдокимов [5, с. 305]. В пользу состояния защищенности (иными словами, в пользу безопасности) компьютерной информации и нормального функционирования средств автоматизированной обработки приводит аргументы Е. А. Русскевич [10, с. 216]. В учебных пособиях по дисци-

плине «Уголовное право» под видовым объектом, как правило, понимают общественные отношения в сфере безопасности компьютерной информации или нечто схожее по смыслу [13; 14].

Представляется, что авторы формулировали подходы к определению видового объекта в значительной мере исходя из названия главы 28 УК РФ и толкования воли законодателя. С одной стороны, структурные части уголовного закона и их названия являются достаточно стабильными. С другой стороны, сфера компьютерной информации, в отличие от других сфер, включающих интересы личности, экономические отношения, защиту государства, является достаточно новой и слабо изученной. Название «Преступления в сфере компьютерной информации» глава 28 УК РФ получила в период, характеризующийся качественно и количественно иным состоянием киберпреступности. С тех пор изменились не только виды преступлений и распространенность информации в электронном виде, но также охраняемые общественные отношения и восприятие обществом технологий. Кроме персональных компьютеров информация теперь обращается повсеместно: в смартфонах, часах, электрочайниках, электровесах и других гаджетах. В обиход прочно вошел термин «цифровизация», а не «компьютеризация», что нашло отражение даже в наименовании Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. В уголовном праве такая терминология не используется, хотя изменение подхода к пониманию сущности технологий наблюдается: более десяти лет назад из составов преступления исключили признаки «ЭВМ», «система ЭВМ» и «программа для ЭВМ» как несоответствующие новым реалиям.

В гражданском праве, как наиболее гибкой отрасли, прямо закреплены такие категории, как «цифровые права» и «цифровая форма». Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» оперирует понятием «цифровой рубль» [20]. Стоит отметить также наличие Федерального закона от 31.07.2020 № 258-ФЗ, который носит название «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» [21]. Трудовое законодательство предусматривает ведение электронного документооборота на цифровой платформе «Работа в России» [12]. Антимонопольное законодательство запрещает отдельные действия, совершаемые хозяйствующим субъектом, который владеет цифровой платформой [19]. Перечисленные нормативные правовые источники наглядно характеризуют наметившуюся тенденцию в использовании терминологии, хотя существует и множество других.

Таким образом, в современной юридической технике наблюдается переход к термину «цифровой» вместо термина «компьютерный» и, как представляется, такой переход должен быть осуществлен в уголовном праве, поскольку это предоставит возможность наилучшим образом описать объект посягательств и признаки отдельных составов преступлений. В литературе необходимость перехода уже обсуждалась, сформулированы аргументированные доводы в его пользу. Так, И. Р. Бегишев и И. И. Бикеев убедительно доказывают целесообразность изменения названия главы 28 УК РФ на «Преступления в сфере обращения цифровой информации», что позволит учесть сущность цифровой формы информации и дополнительно охватить ряд составов преступлений. Метко отмечается, что с позиций русского языка, «если обращаемая в компьютере информация является компьютерной, то обращаемая информация в принтере будет называться принтерной, в сканере – сканерной», и такой подход, естественно, был бы неточным [9, с. 33]. Несмотря на высокую значимость проведенного исследования, следует отметить, что проводилось оно на нормативной базе, содержание которой существенно изменилось. Появились новые статьи, регулирующие ответственность за совершение преступлений против безопасности связи, что не полностью укладывается в рамки категории «цифровая информация». Поскольку законодатель расширил круг объектов, на которые посягают сгруппированные в главе 28 УК РФ преступления, возникла необходимость скорректировать название, распространив его на новые охраняемые общественные отношения – в области безопасности связи.

Не вполне удачным в названии главы видится указание именно на сферу. «Сфера» – это область или пределы распространения чего-нибудь [11]. Таким образом, законодатель скорее указывает на место совершения преступления (компьютерная среда, виртуальная среда, киберпространство), чем на объект, которому причиняется вред. В действительности же любого потерпевшего значительно больше волнует не сама сохранность компьютерной информации, а последствия, которые могут наступить вследствие ее нарушения: утрата недописанной книги, памятных фотографий, ухудшение работы организации, дисциплинарное взыскание и т.п. Такие последствия не обязательно наступают из-за совершения предусмотренных главой 28 УК РФ преступлений, но существует их риск, ставящий под угрозу безопасность, как более комплексное явление.

Указание на сферу компьютерной информации в целом малоинформативно в силу возможности чрезмерно расширительного толкования и соотношения с преступлениями, которые могут в ней совершаться. Компьютерную составляющую имеют, например, доведение до самоубийства (ст. 110 УК РФ), торговля людьми (ст. 127.1 УК РФ) и сбыт наркотических средств (ст. 228.1 УК РФ). Все указанные деяния имеют и «реальную» составляющую – их исполнение подразумевает действия за пределами сети «Интернет». Однако круг деликтов, совершаемых исключительно в киберпространстве, остается крайне широким. В частности, азартные игры часто проводятся с использованием информационно-телекоммуникационных сетей и электронных денежных средств (ст. 171.2 УК РФ). Осуществление неправомерных операций с использованием электронного средства платежа (ч. 4 и ч. 6 ст. 187 УК РФ) происходит, как правило, в ходе использования программ дистанционного банковского обслуживания. Кроме перечисленных, существуют и другие преступления, совершение которых возможно исключительно в пределах киберпространства. Законодатель довольно логично разместил описание соответствующих составов в других статьях, исходя из непосредственного объекта посягательства: порядка проведения азартных игр, собственности, порядка безналичных расчетов и иных. Киберпространство в таких преступлениях выступает в роли места или, грубо говоря, способа, но безопасности компьютерной информации вред не причиняется или причиняется факультативно. Таким образом, статьи главы 28 УК РФ охватывают преступления не в силу особой сферы их осуществления, а в силу их посягательства на схожие объекты, которые связаны с общественной безопасностью и общественным порядком, если исходить из расположения статей в соответствующем разделе IX. Следовательно, логичным было бы указать в названии главы на нарушение безопасности компьютерной (цифровой) информации, поскольку без нее общественная безопасность в современных условиях не существует.

Представители науки уголовного права аргументировали несколько отличающихся друг от друга позиций, суть которых заключается в признании безопасности в качестве объекта киберпреступлений. В частности, С.Э. Ахъядов утверждает, что анализ статей 272-274.2 УК РФ позволяет сделать вывод об информационной безопасности как основном объекте и общественных отношениях в области информации и компьютерных технологий как родовом (видовом) объекте [2, с. 472]. Зарубежный опыт регулирования, особенно в странах постсоветского пространства, говорит о поддержке данной позиции. Например, согласно Уголовному кодексу Республики Беларусь, раздел XII и глава 31 именуются одинаковым образом – «Преступления против компьютерной безопасности» [16]. Причем сам круг преступлений весьма схож с отечественным. Среди объектов охраны компьютерную, информационную или иную разновидность безопасности называют уголовные законы Республики Таджикистан [17], Республики Армения [15]. Хотя зарубежный опыт заслуживает внимания и анализа на предмет возможного заимствования в отечественное законодательство, для полноценного вывода об изменении названия недостаточно изучить только объект посягательства. Необходимо также остановиться на содержании главы с учетом последних дополнений.

Соотношение названия главы 28 УК РФ с ее содержанием

Как уже отмечалось ранее, в последние годы глава 28 УК РФ претерпела ряд изменений. По поводу введения ст. 274.1 УК РФ Д. С. Мирный справедливо отмечает факт постановки под охрану принципиально нового объекта, выходящего за рамки компьютерной информации. Текущая редакция ст. 274.1 УК РФ запрещает посягательства не только на безопасность цифровых данных, содержащихся в критической информационной инфраструктуре, но и «на нормальное функционирование систем» [7].

Введение в УК РФ ст. 272.1 УК РФ было обусловлено необходимостью защиты персональных данных, неосторожные и умышлен-

ные утечки которых все чаще стали иметь место в условиях цифровизации. Однако поскольку при незаконном обороте таких данных всегда нарушаются права и свободы конкретных физических лиц, а не общества в целом или даже значительной ее части, А. А. Шутова задается вопросом, каким образом возникает угроза общественной безопасности, которая является родовым объектом? Автор приходит к выводу о необходимости выделения в самостоятельный раздел положений, содержащих запреты уголовно наказуемых деяний в сфере компьютерной информации [22, с. 123].

Изменение подхода к безопасности информационной сферы привело к внедрению технических средств противодействия различным угрозам. За нарушение правил их установки, эксплуатации и модернизации, а также за нарушение требований к пропуску трафика предусмотрена административная (статьи 13.42 и 13.42.1 КоАП РФ) и уголовная (ст. 274.2 УК РФ) ответственность. Данные преступления не протекают полностью в сфере компьютерной информации и не всегда посягают на ее безопасность, поскольку, во-первых, запрещают ненадлежащие действия или бездействие должностных лиц или индивидуальных предпринимателей по поводу правил централизованного управления техническими средствами, а во-вторых, касаются также трансляции телеканалов и (или) радиоканалов в части взаимодействия с сетями связи общего пользования. Так, например, к административной ответственности по ч. 3 ст. 13.42 КоАП РФ (что является одним из условий для дальнейшего привлечения к уголовной ответственности) было привлечено ООО «СпецТелеком-Юг». Мировым судьей было установлено, что ООО «СпецТелеком-Юг» при оказании телематических услуги связи, вопреки установленным правилам, после получения обращения из радиочастотной службы не направило в службу заявление о необходимом для установки количестве технических средств контроля. ООО «СпецТелеком-Юг» было признано виновным в совершении правонарушения, предусмотренного ч. 3 ст. 13.42 КоАП РФ с назначением штрафа в размере 300000 рублей [8].

В июле 2025 года глава 28 УК РФ пополнилась сразу 3 статьями, направленными на противодействие массовым звонкам, незаконному обороту абонентских номеров, а также данных (логинов, паролей), используемых для регистрации и авторизации пользователей. Меры по совершенствованию закона были призваны усилить кибербезопасность и ликвидировать отдельные правовые пробелы. Особенно это справедливо для области авторизации на информационных ресурсах сети «Интернет», так как оборот личных данных опасен сам по себе, а если такие данные позволяют войти в учетную запись другого человека с целью совершения преступления, то характер и степень общественной опасности возрастают. Однако в меньшей степени к сфере компьютерной информации относится уголовно-правовой запрет деятельности по передаче абонентских номеров (ст. 274.4 УК РФ). Основным нормативным актом, к которому отсылает диспозиция бланкетного характера, является Федеральный закон от 07.07.2003 № 126-ФЗ «О связи», регулирующий деятельность операторов, особенности оказания услуг, основания передачи абонентского номера третьим лицам. Верным видится замечание М. В. Ульянова о том, что принятие последних изменений говорит об осознании законодателем нарастания угроз информационной безопасности и нацеленности норм, закрепленных в гл. 28 УК РФ, на обеспечение уголовно-правовой охраны информационной среды, средств коммуникации и связи [18, с. 105]. Думается, что безопасность связи при криминализации имела более высокий приоритет, нежели безопасность компьютерной информации в целом. Расположение новой ст. 274.4 в УК РФ вполне логично, но лишь при условии расширения названия главы 28 УК РФ и, соответственно, правильного указания на круг общественных отношений, подлежащих охране.

При корректировке уголовного закона целесообразно учитывать не только текущее содержание и текущий уровень развития общества – следует дать реалистичный прогноз о будущих угрозах. Как отмечает Н. Ш. Козаев, содержания главы 28 УК РФ недостаточно для охвата всего спектра противоправных деяний, связанных с использованием информационно-телекоммуникационных технологий, поэтому целесообразно закрепить в законе новые составы преступлений, отражающие современные реалии [6, с. 147]. Отдельные исследователи доказывают, что обвинительные приговоры по уголовным делам о преступлениях, совершенных с использованием искусственного интеллекта, перестали быть редкими [4, с. 104]. Анализ научных статей, посвященных противодействию высокотехнологичным преступлениям, позволяет говорить о высоковероятной криминализации в будущем общественно опасных деяний, связанных с искусственным интеллектом. Нейронные сети стремительно ворвались в привычный уклад жизни общества, а их интеграция произошла в медицине, транспортной, развлекательной и других сферах. К сожалению, интеллектуальные системы широко используются в криминальных целях. По соответствующему запросу программы генерируют порнографический, клеветнический и дискредитирующий контент, отстаивают интересы государств, участвующих в вооруженных конфликтах против России. Зарубежные исследователи сообщают о значительном росте числа фишинговых рассылок с использованием искусственного интеллекта, который позволяет создать убедительные персонализированные атаки, создавать копии известных сайтов [25, с. 47]. Полицейская служба Европейского союза выявила организованную группу, специализирующуюся на отмывании денежных средств, добытых преступным путем. Соучастники использовали интеллектуальную систему, которая дробила и структурировала финансовые операции, осуществляла их в нескольких юрисдикциях, чтобы избежать обнаружения органами власти [24, с. 249].

Современные нейросети, внедренные в различные процессы деятельности, не полностью автономны, поэтому не исключается ошибка человека при принятии какого-либо вредоносного решения. Однако не существует и гарантий безошибочного обучения полностью автономных программ в будущем, а ведь такие ошибки способны привести к неверной постановке диагнозов, авариям, гибели людей. Упущения в защите искусственного интеллекта могут повлечь нанесение ущерба со стороны третьих лиц. Так, уязвимость в работе одной из программ позволила виновным лицам получить несанкционированный доступ к личной информации. Искусственный интеллект по запросу составлял сводки переписок с доступом к личным сообщениям. Взломщики использовали технику под названием «инъекция с подсказкой», обманули программу, и заставили ее отразить информацию из сообщений других граждан [25, с. 48]. Изложенное позволяет говорить о будущем потенциале криминализации не только умышленных, но и неосторожных деяний, связанных с использованием искусственного интеллекта, но это будет зависеть от распространенности внедрения программ и риска наступления вредных последствий.

Кроме того, в настоящее время в противоправных целях на системы искусственного интеллекта осуществляются атаки, не отвечающие признакам, описанным в статьях 272 или 273 УК РФ. Используя уязвимости нейронных сетей, отдельные лица внедряют ложную информацию разными способами, то есть обманывают программы (такие атаки, получившие название «состязательные», внедряют поврежденные сегменты в процесс обучения программы, что приводит к принятию неверных, ошибочных или общественно опасных решений) [23]. В России подобные уязвимости неоднократно выявлялись «Лабораторией Касперского» [1]. Использование несовершенств и уязвимостей искусственного интеллекта создает риск причинения вреда жизни и здоровью человека, собственности, экономической деятельности, общественной безопасности, деятельности государства. В то же время некоторые виновные лица иногда преследуют цель причинить ущерб именно системе, руководствуясь мотивами ненависти и вражды. Иными словами, объектом посягательств в их представлении являются роботы и их программное обеспечение [26, с. 4]. Таким образом, уголовно-правовая охрана искусственного интеллекта и робототехники с соответствующим расширением главы 28 УК РФ – вопрос не столь отдаленного времени.

Выводы

Думается, название главы 28 УК РФ частично устарело и не соответствует требованию языковой стандартизированности закона. Последние изменения в других отраслях нормативно-правового регулирования указывают на термин «цифровая информация», как наиболее предпочтительный и точный. Указание на сферу компьютерной информации в значительной мере относится к месту совершения преступления и специфике, но не к объекту посягательства, который обычно выделяется посредством употребления словесной конструкции «преступления против».

Не соответствует действующее название главы 28 УК РФ и ее содержанию, которое существенно расширилось после введения

статей 274.2-274.6 УК РФ, посвященных противодействию преступлениям не столько против безопасности цифровой информации, сколько против связи. Многие из правоведов прогнозируют дальнейшую криминализацию общественно опасных деяний, связанных с искусственным интеллектом. Последний играет в жизни людей столь важную роль, что нарушение его функционирования способно породить тяжкие последствия. Таким образом, название главы 28 УК РФ предлагается скорректировать. Оптимальная формулировка, думается, выглядит следующим образом: «Преступления против безопасности цифровой информации, искусственного интеллекта и связи». Предложенное название позволит надлежаще учесть объекты посягательств, а также охватить содержание статей, как текущих, так и прогнозируемых в обозримом будущем.

Литература

1. «Лаборатория Касперского» помогла устранить критические уязвимости в менеджере паролей для бизнеса // URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-pomogla-ustranit-kriticheskie-uyazvimosti-v-menedzhere-parolej-dlya-biznesa (дата обращения 14.08.2026).
2. Ахъядов Э. С. М. Основные характеристики преступлений, совершаемых в сфере обращения цифровой информации // Право и государство: теория и практика. 2025. №. 1. С. 471-474.
3. Безверхов А. Г., Голенко Д. В. О соотношении Общей и Особенной частей Уголовного кодекса Российской Федерации // Вестник Университета имени ОЕ Кутафина. 2024. №. 4 (117). С. 39-48.
4. Евдокимов К. Н. К вопросу совершенствования российского уголовного законодательства в контексте противодействия криминальному использованию технологий искусственного интеллекта // Вестник Университета прокуратуры Российской Федерации. 2024. № 6 (104). С. 102-108.
5. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика : дис. … д-ра юрид. наук. М., 2021. 557 с.
6. Козаев Н. Ш. Киберпреступность в современном мире: тенденции, вызовы и стратегии противодействия // Гуманитарные, социально-экономические и общественные науки. 2024. №. 11. С. 146-153.
7. Мирный Д. С. О соотношении объекта преступлений, предусмотренных ст. 274.1 УК РФ, и объекта охраны законодательства в сфере безопасности критической информационной инфраструктуры // Государственная служба и кадры. 2024. №. 3. С. 193-197.
8. Постановление по делу об административном правонарушении Мирового судьи судебного участка № 409 Красносельского района гор. Москвы от 09.09.2021 г. по делу № 5-760/2021// URL: https://mos-sud.ru/409 (дата обращения 14.08.2026).
9. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев. – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. 300 с.
10. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. 521 с.
11. Толковый словарь Ожегова // URL: https://slovarozhegova.ru/word.php?wordid=31156 (дата обращения 14.08.2026).
12. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 3.
13. Уголовное право России. Особенная часть: учебник для бакалавров / под ред. Н. В. Иванцовой. – Йошкар-ола: Марийский гос.ун-т, 2024. 1068 с.
14. Уголовное право России. Части Общая и Особенная: учебник / под ред. А. И. Рарога. – 8-е изд., перераб. и доп. – М.: Проспект, 2014. 784 с.
15. Уголовный кодекс Республики Армения от 27.05.2021 № ЗР-199 // Официальные ведомости Республики Армения». 2021.
16. Уголовный кодекс Республики Беларусь от 09.07.1999 № 275 З // Ведамасці Нацыянальнага сходу Рэспублікі Беларусь. 1999. № 24. Ст. 420.
17. Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574 // Ахбори Маджлиси оли Республики Таджикистан. 1998 г. № 9. Ст. 68–70.
18. Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // Правопорядок: история, теория, практика. 2022. №. 4 (35). С. 102-108.
19. Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3434.
20. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Собрание законодательства РФ. 2011. №. 27. Ст. 3872.
21. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (часть 1). Ст. 5017.
22. Шутова А. А. Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных // Ученые записки Казанского университета. Серия Гуманитарные науки. 2024. Т. 166. №. 6. С. 122-134.
23. Blauth T. F., Gstrein O. J., Zwitter A. Artificial intelligence crime: An overview of malicious use and abuse of AI // Ieee Access. 2022. Vol. 10. P. 77110-77122.
24. Hasan Z., Marisna D. S. Artificial Intelligence: Making crime easier in the world of finance? // AL-ARBAH: Journal of Islamic Finance and Banking. 2024. Vol. 6. I. 2. P. 223-256.
25. Jain B. AI: A New Terror Unleashed // LawFoyer International Journal of Doctrinal Legal Research. 2025. Vol. 3. P. 47-68.
26. Oravec J. A. Rage against robots: Emotional and motivational dimensions of anti-robot attacks, robot sabotage, and robot bullying // Technological Forecasting and Social Change. 2023. Vol. 189. P. 1-8.

On improving the title of chapter 28 of the criminal code of the russian federation

Mosechkin Il.N.
Vyatka State University

This article analyzes the title of Chapter 28 of the Russian Criminal Code in terms of its correspondence to the generic and specific objects of offenses, as well as the content of the articles included within it. The verbal construction "crimes against" is most typical for the structural elements of criminal law, but Chapter 28 of the Russian Criminal Code is one of the few exceptions. The author argues that the reference to the field of computer information better characterizes the specifics of the relevant crimes and the location of their commission than the object. The article also argues that the category "computer information" is outdated and less precise than the category "digital information." The current title of Chapter 28 of the Russian Criminal Code is inconsistent with its content, which was significantly expanded following the introduction of Articles 272.3-272.4 of the Russian Criminal Code, which address crimes against not only the security of digital information but also communications. Numerous scholarly studies predict the further criminalization of socially dangerous acts, including those related to artificial intelligence. Based on the research conducted, the author proposes changing the title of Chapter 28 of the Criminal Code of the Russian Federation, "Crimes against the security of digital information, artificial intelligence, and communications."

Keywords: computer information; digital information; security; artificial intelligence; communication; name; computer.

References

1. Kaspersky Lab helped fix critical vulnerabilities in a business password manager // URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-pomogla-ustranit-kriticheskie-uyazvimosti-v-menedzhere-parolej-dlya-biznesa (accessed 14.08.2026). (in Russ.).
2. Akhyadov E. S. M. Key characteristics of crimes committed in the field of digital information circulation // Law and State: Theory and Practice. 2025. No 1. P. 471-474. (in Russ.).
3. Bezverkhov A. G., Golenko D. V. (2024). On the relationship between the General and Special Parts of the Criminal Code of the Russian Federation // Courier of Kutafin Moscow State Law University (MSAL). 2024. No 4. P. 39-48. (in Russ.).
4. Evdokimov K. N. On the issue of improving Russian criminal legislation in the context of countering the criminal use of artificial intelligence technologies // Bulletin of the University of the Prosecutor's Office of the Russian Federation. 2024. No 6. P. 102-108. (in Russ.).
5. Evdokimov K. N. Combating Computer Crime: Theory, Legislation, and Practice. Doctor of Juridical Sciences Thesis. Moscow, 2021. 557 p. (in Russ.).
6. Kozaev N. Sh. Cybercrime in the modern world: trends, challenges and counteraction strategies // Humanities, socio-economic and social sciences. 2024. No 11. P. 146-153. (in Russ.).
7. Mirnyy D. S. On the relationship of the object of crimes provided for in article 274.1 of the RF criminal code and the object of protection of legislation in the field of security of critical information infrastructure // Civil Service and Personnel. 2024. No 3. P. 193-197 (in Russ.).
8. Resolution on the case of an administrative offense of the Justice of the Peace of Judicial District No. 409 of the Krasnoselsky District of Moscow dated September 9, 2021, in case No. 5-760/2021 // URL: https://mos-sud.ru/409 (accessed 14.08.2026).
9. Begishev I. R., Bikeev I. I. Crimes in the field of digital information circulation. Kazan, 2020. (in Russ.).

10. Russkevich Ye. A. Differentiation of responsibility for crimes committed using information and communication technologies and problems of their qualification Doctor of Juridical Sciences Thesis. Moscow, 2020. 521 p. (in Russ.).
11. Ozhegov's Explanatory Dictionary // URL: https://slovarozhegova.ru/word.php?wordid=31156 (accessed 14.08.2026). (in Russ.).
12. Labor Code of the Russian Federation of December 30, 2001 No. 197-FZ // Collection of Legislation of the Russian Federation. 2002. No 1 (Ch. 1). Art. 3. (in Russ.).
13. Ivancova N. V. Criminal Law of Russia. Special Section: A Textbook for Bachelor's Degrees. Yoshkar-Ola, 2024. (in Russ.).
14. Rarog A. I. Criminal Law of Russia. General and Special Parts: textbook. Moscow, 2014. (in Russ.).
15. Ulyanov M. V. (2022). Crimes in the sphere of computer information: possibilities of criminal legal impact and prevention // LEGAL ORDER: History, Theory, Practice. 2022. No 4 (35). P. 102-108. (in Russ.).
16. Criminal Code of the Republic of Armenia dated May 27, 2021 No. 3P-199 // Official Gazette of the Republic of Armenia. 2021.
17. Criminal Code of the Republic of Belarus dated 07/09/1999 No. 275 Z // Vedamastsi Natsyyanalnaga immediately of the Republic of Belarus. 1999. No 24. Art. 420.
18. Criminal Code of the Republic of Tajikistan dated May 21, 1998 No. 574 // Akhbori Majlisi Oli of the Republic of Tajikistan. 1998 r. No 9. Art. 68–70.
19. Shutova A. A. Novelties in Russian Criminal Law on Liability for Personal Data Breaches // Uchenye Zapiski Kazanskogo Universiteta. Seriya Gumanitarnye Nauki. 2024. Vol. 166. No 6. P. 122-134. (in Russ.).
20. Federal Law of July 26, 2006 No. 135-FZ "On the Protection of Competition" // Collection of Legislation of the Russian Federation. 2006. No 31 (Ch. 1). Art. 3434. (in Russ.).
21. Federal Law of June 27, 2011 No. 161-FZ "On the National Payment System" // Collection of Legislation РФ. 2011. No. 27. Art. 3872. (in Russ.).
22. Federal Law of July 31, 2020 No. 258-FZ "On Experimental Legal Regimes in the Sphere of Digital and Technological Innovations in the Russian Federation" // Collected Legislation of the Russian Federation. 2020. No 31 (Ch. 1). Art. 5017. (in Russ.).
23. Blauth T. F., Gstrein O. J., Zwitter A. Artificial intelligence crime: An overview of malicious use and abuse of AI // Ieee Access. 2022. No 10. P. 77110-77122.
24. Hasan Z., Marisna D. S. Artificial Intelligence: Making crime easier in the world of finance? // AL-ARBAH: Journal of Islamic Finance and Banking. 2024. Vol. 6. No 2. P. 223-256.
25. Jain B. AI: A New Terror Unleashed // LawFoyer International Journal of Doctrinal Legal Research. 2025. No 3. P. 47-68.
26. Oravec J. A. Rage against robots: Emotional and motivational dimensions of anti-robot attacks, robot sabotage, and robot bullying // Technological Forecasting and Social Change. 2023. No 189. P. 1-8.