КИБЕРПРЕСТУПЛЕНИЯ ВОЕННОСЛУЖАЩИХ: НОВАЯ КАТЕГОРИЯ ВОИНСКИХ ПРЕСТУПЛЕНИЙ

К.З. Шоранов, *магистрант*
Научный руководитель: *А.С. Сидоров, старший преподаватель, полковник юстиции в отставке*
Российский государственный университет правосудия имени В.М. Лебедева (Россия, г. Москва)

DOI:10.24412/2500-1000-2026-3-2-307-318

Аннотация. *В статье исследуется феномен киберпреступлений, совершаемых военнослужащими, как самостоятельной и качественно новой категории воинских правонарушений. Анализируется действующая система уголовно-правовых норм Российской Федерации и международного права применительно к данной проблематике, выявляются пробелы в регулировании, а также предлагаются направления совершенствования законодательства. Особое внимание уделяется соотношению норм главы 28 и главы 33 УК РФ при квалификации деяний военнослужащих в информационной среде, институту командной ответственности в условиях кибероперациий, а также применению норм международного гуманитарного права к военным действиям в киберпространстве.*

Ключевые слова: *киберпреступления; военнослужащий; воинские преступления; кибероперации; информационное пространство; уголовная ответственность; командная ответственность; международное гуманитарное право; Таллиннское руководство.*

Стремительная цифровизация всех сфер государственного управления и военного дела порождает принципиально новые вызовы для уголовно-правовой науки. Военная служба, веками основанная на физическом присутствии, субординации и применении кинетической силы, неуклонно переходит в цифровое измерение. Современные вооружённые силы оперируют автоматизированными системами управления войсками, беспилотными комплексами, системами спутниковой навигации, криптографическими коммуникациями и разведывательными платформами, каждая из которых представляет собой элемент глобального киберпространства. Как справедливо констатируют исследователи, киберпространство стало «пятым доменом» или «пятой сферой» ведения военных действий – наряду с сушей, морем, воздушным и космическим пространством [1].

Следствием этой трансформации является то, что военнослужащие оказываются одновременно и потенциальными жертвами, и возможными субъектами преступлений в информационном пространстве. При этом если роль военнослужащего как жертвы кибератак очевидна и фиксируется международными институтами, то его роль как субъекта киберпреступлений остаётся недостаточно осмысленной в отечественной уголовно-правовой доктрине. Действующий Уголовный кодекс Российской Федерации содержит специализированную главу 33, посвящённую преступлениям против военной службы, однако в ней отсутствуют составы, специально направленные против противоправных действий военнослужащих с использованием информационных технологий. Это создаёт серьёзный пробел, который не позволяет адекватно реагировать на качественно новые угрозы, возникающие на стыке военного и информационного права [2].

Актуальность обозначенной проблемы подтверждается и на международном уровне: в декабре 2025 года Канцелярия Прокурора Международного уголовного суда опубликовала специальный документ «Политика в отношении киберпреступлений по Римскому статуту», прямо указывающий на намерение расследовать и преследовать киберпреступления наравне с деяниями, совершёнными традиционными средствами. Независимые аналитики Chatham House в январе 2026 года констатировали, что нормы международного уголовного права технологически нейтральны и уже применимы к киберпреступлениям, од-

нако правоприменительная практика значительно отстаёт от этой принципиальной позиции [3, 4].

Настоящая статья ставит целью сформировать концептуальный правовой фундамент для понимания киберпреступлений военнослужащих как самостоятельной категории, определить их место в системе действующего уголовного законодательства, выявить специфику субъекта, объекта и объективной стороны данных деяний, а также наметить пути совершенствования нормативной базы.

1. Понятие и классификация киберпреступлений военнослужащих

Прежде чем перейти к анализу киберпреступлений военнослужащих как особой категории, необходимо установить само понятие данных деяний. В действующем законодательстве Российской Федерации отсутствует легальное определение термина «киберпреступление», тогда как глава 28 УК РФ оперирует более узким понятием «преступления в сфере компьютерной информации». Под компьютерной информацией, в свою очередь, понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В доктрине термин «киберпреступление» используется шире и охватывает не только деяния, предусмотренные главой 28 УК РФ, но и преступления, в которых компьютерные технологии и информационно-коммуникационные сети выступают инструментом совершения иных общественно опасных деяний – хищений, шпионажа, распространения запрещённой информации [5, 6].

Киберпреступления военнослужащих представляют собой умышленные или неосторожные общественно опасные деяния, совершённые лицами, проходящими военную службу по призыву или контракту, а равно гражданами, призванными на военные сборы, с использованием информационно-коммуникационных технологий, компьютерных систем или информационных сетей, причиняющие вред охраняемым законом общественным отношениям. Специфика субъекта – военнослужащего – придаёт таким деяниям дополнительные квалифицирующие признаки, поскольку военная служба неразрывно связана с доступом к сведениям, составляющим государственную и военную тайну, к объектам критической информационной инфраструктуры, а также к системам управления войсками.

С позиций классификации киберпреступления военнослужащих целесообразно разграничить на несколько групп. Первую группу составляют деяния, направленные против установленного порядка прохождения военной службы посредством использования информационных технологий. К ним относятся, в частности, несанкционированный доступ к закрытым военным информационным системам, разглашение военной тайны через интернет-ресурсы и мессенджеры, неправомерное распространение сведений о дислокации воинских частей, личном составе и боевых потерях. Вторую группу образуют общеуголовные киберпреступления, совершаемые военнослужащими с использованием их особого положения или служебного доступа, – например, хищение с использованием банковских карт (ст. 159.3, 159.6 УК РФ), несанкционированный доступ к персональным данным сослуживцев или мирного населения. Третью группу составляют деяния, совершаемые в условиях вооружённого конфликта и квалифицируемые как военные преступления или преступления против мира и безопасности человечества в их «кибернетическом» воплощении [7, 3].

2. Действующая система норм уголовного законодательства и её недостаточность

Анализ действующего российского законодательства обнаруживает принципиальное противоречие: с одной стороны, глава 28 УК РФ содержит достаточно разработанный инструментарий уголовного преследования за компьютерные преступления, с другой – глава 33 УК РФ не предусматривает ни одного специального состава, учитывающего использование информационных технологий в качестве средства или способа совершения воинского преступления.

Согласно ст. 272 УК РФ, неправомерный доступ к охраняемой законом компьютерной информации, повлёкший её уничтожение, блокирование, модификацию либо копирование, наказывается лишением свободы на срок до семи лет с квалифицирующими обстоятельствами, к которым относятся в том числе причинение крупного ущерба и совершение организованной группой. Статья 273 УК РФ

устанавливает ответственность за создание, распространение и использование вредоносных программ с максимальным наказанием до семи лет лишения свободы. Статья 274 УК РФ запрещает нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, а ст. 274.1 УК РФ, введённая позднее, устанавливает специальную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [5, 8-11].

Формально военнослужащий, совершивший деяние по ст. 272 или 273 УК РФ, несёт ответственность на общих основаниях. Принадлежность к вооружённым силам не образует в данных составах ни квалифицирующего признака, ни специального основания для смягчения наказания. Между тем очевидно, что противоправный доступ военнослужащего к засекреченным сетям Министерства обороны или намеренное повреждение программного обеспечения системы управления боевыми дронами представляет собой качественно иной по степени общественной опасности акт по сравнению с аналогичным деянием гражданского лица. Объект посягательства в данном случае выходит далеко за рамки «безопасности компьютерной информации» и охватывает боеспособность вооружённых сил, обороноспособность государства и порядок прохождения военной службы.

Глава 33 УК РФ, в свою очередь, перечисляет составы, ориентированные на традиционные формы воинских правонарушений, – неисполнение приказа (ст. 332), самовольное оставление части (ст. 337), дезертирство (ст. 338), умышленное уничтожение военного имущества (ст. 346), нарушение правил несения боевого дежурства (ст. 340). Ни одна из норм главы 33 прямо не предусматривает санкций за деяния, совершённые посредством компьютерных технологий или в информационном пространстве. Это положение охарактеризовано в современной российской доктрине как пробел, требующий немедленного устранения. Введение новых составов преступлений, связанных с киберугрозами и использованием информационных технологий в военной сфере, указывается как объективная необходимость с учётом развития новых форм вооружённой борьбы и трансформации угроз национальной безопасности [2, 12].

Отдельный блок нормативного регулирования образует ст. 283 УК РФ, устанавливающая ответственность за разглашение государственной тайны. На военнослужащего как субъекта, наделённого специальным правовым статусом в соответствии с Федеральным законом от 27 мая 1998 года № 76-ФЗ «О статусе военнослужащих», возлагается специальная обязанность по сохранности государственной и военной тайны. В условиях цифровизации разглашение военнослужащим секретных сведений через мессенджер или посредством публикации в социальных сетях формально охватывается данной нормой, однако специфика электронного способа распространения тайных данных не нашла отражения в квалифицирующих признаках данного состава [13, 14].

3. Специфика субъекта: военнослужащий как особый субъект киберпреступлений

Военнослужащий занимает в системе уголовного права особое место как специальный субъект. Согласно ст. 331 УК РФ, субъектами преступлений против военной службы признаются военнослужащие, проходящие военную службу по призыву либо по контракту, а также граждане, пребывающие в запасе, во время прохождения ими военных сборов. Постановление Пленума Верховного Суда Российской Федерации от 18 мая 2023 года № 11 дополнительно разъяснило, что к субъектам воинских преступлений относятся и граждане, призванные на военную службу по мобилизации [2, 15-17].

Особый правовой статус военнослужащего приобретает принципиальное значение применительно к киберпреступлениям по ряду оснований. Во-первых, военнослужащий располагает легитимным доступом к сведениям, составляющим государственную тайну, к закрытым информационным системам вооружённых сил и к объектам критической информационной инфраструктуры. Злоупотребление этим доступом порождает деяния, которые технически квалифицируются как «правомерный доступ», однако, по существу, носят преступный характер ввиду нарушения режима информационной безопасности. Во-вторых, военнослужащие, особенно специа-

листы подразделений радиоэлектронной борьбы, информационных операций и связи, обладают значительно более высоким уровнем технической компетентности в сфере кибератак, нежели среднестатистический гражданский нарушитель, что существенно повышает потенциальный вред от их противоправных действий. В-третьих, военнослужащий находится в условиях жёсткой субординации и служебной зависимости, что может создавать как ситуации принуждения к участию в незаконных кибероперациях, так и обстоятельства, при которых приказ командира становится основанием для совершения запрещённых международным правом кибератак [18, 19].

Принципиально важным является и вопрос о разграничении дисциплинарного проступка и уголовного преступления применительно к информационным правонарушениям военнослужащих. Использование служебного компьютера в личных целях, несоблюдение режима работы с электронными документами или нарушение правил использования мобильных устройств в расположении воинской части относятся к дисциплинарным проступкам. Напротив, намеренная установка вредоносного программного обеспечения на боевую вычислительную систему или несанкционированная передача служебной переписки иностранным адресатам образует уголовно наказуемое деяние. Граница между этими категориями не всегда очевидна и требует чёткого законодательного определения [15].

Следует также рассмотреть вопрос о соучастии гражданских лиц в кибернетических воинских преступлениях. Применительно к составам главы 33 УК РФ Пленум Верховного Суда разъяснил, что гражданские лица могут участвовать в воинских преступлениях только в качестве организаторов, подстрекателей и пособников. Применительно к киберпреступлениям это означает, что лицо, не являющееся военнослужащим, но вовлёкшее военнослужащего в несанкционированный доступ к военной информационной системе или распространение военной тайны, несёт ответственность как соучастник воинского преступления со ссылкой на соответствующую часть ст. 33 УК РФ [15].

4. Объект и объективная сторона киберпреступлений военнослужащих.

Определение объекта преступления имеет основополагающее значение для систематизации рассматриваемой категории деяний. В теории отечественного уголовного права объектом преступлений против военной службы выступают охраняемые государством общественные отношения, регулирующие порядок прохождения военной службы, именуемые в совокупности «воинским правопорядком». Нарушение воинского правопорядка определяется как общественно опасное деяние, посягающее на установленный порядок прохождения военной службы, ослабляющее воинскую дисциплину и боевую готовность войск [20].

Применительно к киберпреступлениям военнослужащих объект является сложным по структуре. Родовой объект совпадает с объектом всей главы 33 УК РФ – установленным порядком прохождения военной службы. Однако непосредственный объект существенно дифференцируется в зависимости от конкретного деяния. При несанкционированном доступе военнослужащего к закрытым информационным системам непосредственным объектом выступает режим информационной безопасности в сфере военной службы. При кибератаке военнослужащего на автоматизированные системы управления войсками – боеспособность и боевая готовность вооружённых сил. При разглашении военной тайны посредством электронных коммуникаций – государственная безопасность в информационной сфере. Дополнительным объектом во всех указанных случаях выступают также интересы граждан и организаций, которые могут пострадать вследствие действий военнослужащего.

Объективная сторона данных деяний характеризуется тем, что преступные действия совершаются исключительно в информационном пространстве либо с использованием информационно-коммуникационных технологий в качестве орудия или средства совершения преступления. Это порождает ряд специфических проблем квалификации. Первая из них связана с установлением причинно-следственной связи между действиями военнослужащего в цифровом пространстве и наступившими последствиями в физическом мире. Кибератака на систему управления огнём может повлечь сбой в применении во-

оружений с реальными последствиями для жизни и здоровья людей, однако цепочка причинности при этом значительно сложнее, чем при традиционном насильственном преступлении. Вторая проблема связана с установлением места совершения преступления в условиях трансграничного характера киберпространства [21].

Особого внимания заслуживает проблема бездействия как формы объективной стороны. Военнослужащий, несущий боевое дежурство по обеспечению кибербезопасности и умышленно допустивший вторжение в информационные системы воинской части, формально совершает деяние в форме бездействия. Однако действующая ст. 340 УК РФ, запрещающая нарушение правил несения боевого дежурства, не конкретизирует, что это нарушение может проявляться в форме ненадлежащего обеспечения кибербезопасности. Таким образом, вновь обнаруживается пробел, требующий законодательного восполнения.

5. Отдельные составы киберпреступлений военнослужащих и проблемы их квалификации

Наиболее распространёнными видами киберпреступлений военнослужащих, встречающимися в зарубежной правоприменительной практике, являются несанкционированный доступ к военным компьютерным системам, утечка классифицированных данных через цифровые каналы, использование служебных вычислительных ресурсов в личных или корыстных целях, а также распространение информации о воинских операциях в социальных сетях. Анализ зарубежного опыта показывает, что в системе Единого военного кодекса правосудия США (UCMJ) такие деяния преследуются по ст. 92 (невыполнение приказа или положения) или ст. 134 (общая статья) UCMJ, а нарушение режима работы с военными компьютерными системами влечёт уголовную ответственность, увольнение с военной службы, лишение допуска к секретным сведениям и конфискацию денежного довольствия [18].

В российской практике особую актуальность приобрели случаи разглашения военнослужащими сведений о ходе боевых действий, дислокации подразделений и потерях через мессенджеры и социальные сети. Применительно к подобным деяниям возникает сложная проблема конкуренции норм: деяние может одновременно квалифицироваться по ст. 283 УК РФ (разглашение государственной тайны), по ст. 207.3 УК РФ (дискредитация деятельности вооружённых сил) или по соответствующим статьям главы 33 УК РФ. Такая множественная конкуренция составов свидетельствует о системном недостатке нормативного регулирования, при котором одно и то же деяние охватывается разными уголовно-правовыми нормами с несопоставимыми санкциями [22].

Отдельной разновидностью является использование военнослужащими вредоносного программного обеспечения против систем противника в ходе вооружённого конфликта. Формально такое деяние может охватываться ст. 273 УК РФ, запрещающей создание и распространение вредоносных программ. Однако применение компьютерного оружия в интересах государства в ходе санкционированных боевых операций не только не влечёт уголовной ответственности, но и является частью официально закреплённой военной доктрины. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента от 05 декабря 2016 года № 646, прямо предусматривает «развитие сил и средств информационного противоборства» как направление обеспечения информационной безопасности в области обороны. Это означает, что граница между законной кибервоенной операцией и уголовно наказуемым деянием проходит не по техническим характеристикам действия, а по его правовому основанию и соответствию принципам международного гуманитарного права [11, 23].

6. Институт командной ответственности в контексте кибероопераций

Одной из наиболее сложных проблем в сфере привлечения к уголовной ответственности за кибернетические воинские преступления является вопрос об ответственности командиров. Международное уголовное право закрепляет институт командной ответственности, в рамках которого командир или начальник несёт уголовную ответственность за преступные действия своих подчинённых, если он знал или должен был знать о совершении или намерении совершить преступление и не принял надлежащих мер по его

предотвращению или пресечению. Этот институт кодифицирован в ст. 28 Римского статута Международного уголовного суда [24, 25].

Таллиннское руководство 2.0 по международному праву, применимому к кибероперациям, явившееся результатом работы экспертов НАТО при участии специалистов Международного комитета Красного Креста, прямо распространяет институт индивидуальной и командной ответственности на кибероперации, ограничивая его применение рамками военных преступлений в соответствии со ст. 25 и 28 Римского статута. Помимо этого, Руководство устанавливает ответственность командиров за «приказ о проведении кибератак, составляющих военные преступления» [26, 27].

Российская правовая система традиционно испытывает затруднения с имплементацией концепции командной ответственности. Профессор Г.А. Есаков установил, что в действующем УК РФ 1996 года отсутствует полная схема командной ответственности: ни институт соучастия в Общей части, ни отдельные составы в Особенной части не предусматривают уголовной ответственности командиров за преступления подчинённых в том объёме, который предполагается международным гуманитарным правом. В контексте кибернетических воинских преступлений это означает, что командир, ведомый которого систематически использовал служебные компьютеры для хищения данных или распространения военной тайны, фактически застрахован от уголовного преследования за неисполнение обязанности по надзору [28].

Применительно к Украине, ратифицировавшей Римский статут, предпринимаются законодательные попытки введения командной ответственности в национальное уголовное право: разработан законопроект о введении специальной ст. 31-1 УК, предусматривающей ответственность военных командиров за непредотвращение преступлений подчинённых, включая деяния с использованием информационных технологий. Данный опыт заслуживает изучения с точки зрения возможной имплементации аналогичных норм в российское законодательство [29].

7. Применение норм международного гуманитарного права к кибернетическим воинским преступлениям

Вопрос о применимости международного гуманитарного права к кибернетическим операциям вооружённых сил является центральным в современной международно-правовой науке. Ключевым в этом контексте является то обстоятельство, что факт использования сторонами вооружённого конфликта в ходе военных действий новых технологий никак не влияет на применимость к таким действиям норм МГП. Это подтверждается и позицией Международного комитета Красного Креста, согласно которой кибератаки, осуществляемые в рамках вооружённого конфликта, в полной мере подпадают под действие Женевских конвенций и Дополнительных протоколов к ним [1, 30, 31].

Таллиннское руководство установило, что международный вооружённый конфликт возникает всякий раз, когда между двумя или более государствами происходят военные действия, «которые могут включать кибероперации или ограничиваться ими». Это означает принципиальную возможность существования вооружённого конфликта, ведущегося исключительно посредством кибератак. Вооружённые конфликты в киберпространстве, перетекающие в военные преступления, влекут уголовную ответственность для лиц, которые руководят кибероперациями [1, 32].

С точки зрения международного уголовного права кибератаки могут квалифицироваться как военные преступления, когда их последствия достигают порога, установленного Римским статутом. Исследователи, анализирующие данную проблематику, констатируют, что хотя Римский статут прямо не упоминает киберпреступления, его положения достаточно технологически нейтральны для охвата кибернетических деяний при толковании в свете их гуманитарных последствий. Канцелярия Прокурора МУС в декабре 2025 года подтвердила намерение расследовать и преследовать киберпреступления на основании норм Римского статута на равных основаниях с преступлениями, совершёнными традиционными средствами [7].

Принципиальное значение для квалификации кибератаки как военного преступления имеет вопрос о том, является ли она «нападе-

нием» по смыслу ст. 49 Дополнительного протокола I к Женевским конвенциям. Согласно норме 92 Таллиннского руководства, кибератака представляет собой «наступательную или оборонительную кибероперацию, которая, как разумно ожидается, приведёт к причинению травм или смерти людей, либо к повреждению или разрушению объектов». Следовательно, кибератака, направленная против военных госпиталей, систем водоснабжения или энергетической инфраструктуры, подпадает под запреты МГП, а её осуществление военнослужащим по приказу командования – равно как и вопреки ему – порождает как индивидуальную, так и командную ответственность [1].

Следует также отметить специфическое положение военнослужащих, осуществляющих кибероперации. В отличие от гражданских хакеров, которые в соответствии с МГП теряют защиту и могут подвергнуться нападению, если напрямую участвуют в военных действиях, военнослужащие пользуются особым правовым статусом комбатанта и при захвате в плен – статусом военнопленного. Это фундаментальное различие означает, что государства обязаны чётко идентифицировать своих военных киберспециалистов как членов вооружённых сил, а не позиционировать их как гражданских хакеров-«добровольцев»[33].

Российская Федерация придерживается позиции технологической нейтральности международного гуманитарного права применительно к кибернетическим операциям, признавая принципиальную применимость Женевских конвенций к данной сфере. Вместе с тем Российская Федерация продвигает в ООН и ШОС альтернативный подход к регулированию международной информационной безопасности, более широкий по охвату, нежели западная концепция «кибервойны», и основанный на понятии «информационного пространства». Это означает, что в отечественном правовом дискурсе проблема киберпреступлений военнослужащих должна рассматриваться одновременно в двух измерениях – международно-правовом и национально-уголовно-правовом [34, 35].

8. Проблема атрибуции и доказывания в делах о киберпреступлениях военнослужащих

Проблема атрибуции киберпреступлений применительно к военнослужащим имеет двойное юридическое измерение. На международном уровне атрибуция государству кибератаки, осуществлённой его военными структурами, является необходимым условием для государственной ответственности по международному праву. На внутригосударственном уровне атрибуция конкретному военнослужащему является необходимым условием для уголовного преследования. Обе задачи сопряжены с серьёзными процессуальными и криминалистическими трудностями.

Наглядно проблему атрибуции иллюстрирует дело о предъявлении Министерством юстиции США обвинений семи офицерам Главного разведывательного управления Российской Федерации в 2018 году. Прокуроры объявили, что ГРУ проводило кибератаки в отношении организаций по запрету химического оружия, антидопинговых агентств и американской ядерной компании – однако реальное уголовное преследование в суде стало невозможным ввиду отсутствия механизмов международной выдачи. Этот прецедент ярко демонстрирует разрыв между возможностями установления причастности военнослужащих к кибератакам и возможностями реального привлечения их к уголовной ответственности. МУС при разрешении вопросов атрибуции сталкивается с аналогичной проблемой – субъекты кибератак намеренно скрывают свою деятельность, используя цепочки промежуточных серверов и инфраструктуру третьих государств [27, 36].

Применительно к национальным уголовным делам проблема доказывания осложняется тем, что следователи, обеспечивающие уголовное преследование военнослужащих, зачастую не обладают достаточным уровнем технических компетенций для работы с цифровыми доказательствами. Верховный Суд Российской Федерации и Министерство внутренних дел ориентируют суды на применение комплексного подхода при расследовании дел о киберпреступлениях, сочетающего нормы УК РФ и специального законодательства в сфере информационных технологий. Это требует от органов военного следствия особых компетенций, а от военных судов – специализации, которая в настоящее время остаётся недостаточно развитой [11].

9. Направления совершенствования законодательства

На основании проведённого анализа представляется возможным сформулировать следующие направления совершенствования российского законодательства в сфере ответственности военнослужащих за киберпреступления.

Первым и наиболее очевидным направлением является дополнение главы 33 УК РФ специальными составами воинских преступлений, совершаемых в информационном пространстве. Целесообразно ввести нормы, устанавливающие ответственность за несанкционированное использование военных информационных систем, нарушение режима кибербезопасности военных объектов, несанкционированное раскрытие военной информации через цифровые каналы и ненадлежащее несение обязанностей по кибербезопасности. Системное введение подобных составов позволит преодолеть нынешнюю конкуренцию норм главы 28 и главы 33 УК РФ применительно к деяниям военнослужащих [12].

Вторым направлением является введение в качестве квалифицирующего признака в составы главы 28 УК РФ факта совершения преступления военнослужащим с использованием доступа, предоставленного в связи с прохождением военной службы. Аналогичным образом в главе 33 следует предусмотреть квалифицированные составы деяний, совершённых с использованием информационных технологий, как это закреплено, например, применительно к причинению смерти или тяжкого вреда здоровью в других главах УК.

Третье направление связано с имплементацией принципа командной ответственности применительно к киберпреступлениям. Российское законодательство, как было показано, не содержит полноценного механизма ответственности командиров за преступления подчинённых в сфере кибероперации. Принятие специальной нормы об ответственности командира за непредотвращение кибернетических воинских преступлений подчинённых, осознанно допущенных или ставших возможными ввиду отсутствия надлежащего контроля, отвечало бы как требованиям МГП, так и потребностям национальной безопасности [28].

Четвёртым направлением является создание специализированной методологии квалификации деяний военнослужащих в сфере кибербезопасности. В развитие Постановления Пленума ВС РФ от 18 мая 2023 года № 11 целесообразна разработка специализированного разъяснения, посвящённого вопросам уголовной ответственности военнослужащих в информационном пространстве. Соответствующие разъяснения должны охватывать вопросы разграничения дисциплинарного проступка и уголовного преступления, конкуренции норм, доказывания вины и использования цифровых доказательств.

Пятым направлением является приведение российского законодательства в соответствие с международными стандартами, прежде всего с нормами МГП применительно к кибернетическим операциям. Принятие специального федерального закона о кибернетических операциях вооружённых сил, устанавливающего правовые основания для их проведения и пределы допустимого воздействия на гражданскую инфраструктуру, стало бы важным шагом к систематизации данной сферы. Следует учитывать, что нормы международного права технологически нейтральны – международное преступление остаётся таковым вне зависимости от того, совершено ли оно с применением огнестрельного оружия или компьютерных технологий [3].

Киберпреступления военнослужащих представляют собой качественно новую и самостоятельную категорию воинских правонарушений, которая пока не нашла должного отражения ни в российском уголовном законодательстве, ни в полной мере – в международно-правовых актах. Действующая система норм УК РФ отличается существенными пробелами в части регулирования противоправных деяний военнослужащих в информационном пространстве. Преступления, совершаемые военнослужащими с использованием цифровых технологий, не охватываются специальными составами главы 33 УК РФ, тогда как применение общих норм главы 28 не учитывает специфику военно-служебных отношений и потенциальный масштаб вреда для обороноспособности государства.

На международном уровне формируется устойчивая тенденция к распространению норм МГП и международного уголовного

права на кибернетические операции. Таллинское руководство 2.0 признало применимость к кибернетическим операциям как общих принципов права вооружённых конфликтов, так и специфических институтов командной ответственности. Политика МУС, принятая в декабре 2025 года, закрепила принцип технологической нейтральности международного уголовного права. Эти разработки создают международно-правовой контекст, в котором формирование специального национального уголовно-правового режима для кибернетических воинских преступлений становится не просто научной рекомендацией, но и объективной юридической необходимостью [4, 27].

Перспективными направлениями дальнейших исследований в данной области являются анализ судебной практики по делам о киберпреступлениях военнослужащих в иностранных государствах, разработка модельной нормы для главы 33 УК РФ о «нарушении правил информационной безопасности военной службы», а также исследование процессуальных аспектов доказывания данных преступлений в условиях закрытого судопроизводства военных судов.

Библиографический список

1. Гаркуша-Божко С.Ю. Международное гуманитарное право в киберпространстве: Ratione materiae, ratione temporis и проблема квалификации кибератак / С.Ю. Гаркуша-Божко // Цифровое право. – 2021. – № 2 (1). – С. 64-82. – [Электронный ресурс]. – Режим доступа: https://www.digitallawjournal.org/jour/article/view/42?locale=ru_RU.

2. Глава 33 УК РФ с Комментариями. Преступления против военной службы // Комментарии к УК РФ. – [Электронный ресурс]. – Режим доступа: https://ukodeksrf.ru/ch-2/rzd-11/gl-33.

3. Обеспечение правосудия в отношении международных преступлений, совершенных с использованием кибертехнологий // CHATHAM HOUSE. – [Электронный ресурс]. – Режим доступа: https://www.chathamhouse.org/2026/01/securing-justice-cyber-enabled-international-crimes/02-applying-international-criminal-law.

4. International Criminal Court. On 3 December 2025, the ICC Office of the Prosecutor launched its policy on cyber-enabled crimes // Facebook. – [Электронный ресурс]. – Режим доступа: https://www.facebook.com/InternationalCriminalCourt/videos/on-3-december-2025-the-icc-office-of-the-prosecutor-launched-its-policy-on-cyber/1226103829364982/.

5. Ответственность за совершение преступлений в сфере информационно-коммуникационных технологий // Муниципальный округ Чертаново Южное в городе Москве. – [Электронный ресурс]. – Режим доступа: https://vmo-chu.ru/prokuratura/otvetstvennost_za_sovershenie_prestuplenij_v_sfere_informacionnokommunikacionnyh_tehnologij1/.

6. О преступлениях, совершенных с использованием IT-технологий // Пестречинский муниципальный район. – [Электронный ресурс]. – Режим доступа: https://pestreci.tatarstan.ru/prokuror-razyasnyaet.htm?pub_id=4223924.htm.

7. Жабчик Д., Хедзь В., Бондаренко Е. Новые вызовы для международного уголовного права: как включить киберпреступления, совершенные во время вооруженных конфликтов, в существующую правовую систему // Вышеградский журнал по правам человека. – 2025. – № 3. – С. 17-24. – [Электронный ресурс]. – Режим доступа: https://journals.uran.ua/journal-vjhr/article/view/341725.

8. Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации – Глава 28 Уголовного кодекса Российской Федерации) // Следственное управление Следственного комитета Российской Федерации по Ленинградской области. – [Электронный ресурс]. – Режим доступа: https://lenobl.sledcom.ru/Protivodejstvie-kiberprestupnosti/item/1235055/.

9. Преступления в сфере компьютерной информации – ст. 272 УК РФ // RTM Group. – [Электронный ресурс]. – Режим доступа: https://rtmtech.ru/articles/prestupleniya-v-sfere-kompyuternoj-informatsii-st-272-uk-rf/.

10. Уголовная ответственность за преступления в сфере компьютерной информации // Администрация ГО «Город Калининград». – [Электронный ресурс]. – Режим доступа: https://www.klgd.ru/useful/prokuratura/detail.php?ID=7064793.

11. Танкова, А. Правовые механизмы кибербезопасности: общие принципы и секторальное регулирование // ЭЖ-Юрист. – 2025. – № 14 (1363). – [Электронный ресурс]. – Режим доступа: https://www.eg-online.ru/article/496874/.

12. Савельев, И.Г. Совершенствование регламентации уголовной ответственности военнослужащих и мер профилактики воинских преступлений / И.Г. Савельев, О.В. Филиппова // Вестник Бурятского государственного университета. Юриспруденция. – 2025. – № 3. – С. 19-22. – DOI 10.18101/2658-4409-2025-3-19-22. – EDN SGKLFO.

13. Об уголовной ответственности за разглашение сведений // Социальная защита Республики Татарстан. – [Электронный ресурс]. – Режим доступа: https://sobes.tatarstan.ru/ob-ugolovnoy-otvetstvennosti-za-razglashenie.htm.

14. Об уголовной ответственности за разглашение сведений, составляющих государственную тайну // Организации социального обслуживания населения Республики Татарстан. – [Электронный ресурс]. – Режим доступа: https://sobes.tatarstan.ru/ob-ugolovnoy-otvetstvennosti-za-razglashenie-7804549.htm.

15. Преступления против военной службы: разъяснения Пленума ВС РФ по общим вопросам // ГАРАНТ.РУ. – [Электронный ресурс]. – Режим доступа: https://www.garant.ru/news/1626292/.

16. Постановление Пленума Верховного Суда РФ от 18.05.2023 N 11 «О практике рассмотрения судами уголовных дел о преступлениях против военной службы» // Верховный Суд Российской Федерации. – [Электронный ресурс]. – Режим доступа: https://vsrf.ru/documents/own/32440/.

17. Ермолович Я.Н. Научно-практический комментарий к Главе 33 Уголовного кодекса Российской Федерации (постатейный, с судебной практикой). – ISBN 978-5-6042565-0-3 изд. – М.: Центр правовых коммуникаций, 2018. – 240 с. – [Электронный ресурс]. – Режим доступа: http://www.opklex.com/assets/upload/file/files/isbn.pdf.

18. What Constitutes a Military Computer Crime? // Military Trial Defenders. – [Электронный ресурс]. – Режим доступа: https://militarytrialdefenders.com/blog/cyber-crimes/.

19. Military Criminal Justice: A Guide for the Civilian Prosecutor // Former Prosecutor & Board-Certified Criminal Law Specialist. – [Электронный ресурс]. – Режим доступа: https://knightjustice.com/military-criminal-justice-a-guide-for-the-civilian-prosecutor/.

20. Мальков С.М. Содержание объекта преступления против военной службы и его значение для систематизации главы 33 Уголовного кодекса РФ // Современное право. – 2017. – № 8. – С. 78-83. – [Электронный ресурс]. – Режим доступа: https://sovpravo.press/stati/soderzhanie-obekta-prestupleniya-protiv-voennoj-sluzhby-i-ego-znachenie-dlya-sistematizacii-glavy-33-ugolovnogo-kodeksa-rf/.

21. Мальков С.М. Международное право и война в киберпространстве // Современное право. – 2013. – № 8. – С. 120-126. – [Электронный ресурс]. – Режим доступа: https://goo.su/d8Mj.

22. Уголовная ответственность за дезинформацию о деятельности Вооруженных сил России, а также за дискредитацию их действий по защите страны и поддержанию мира // Администрация г. Нижневартовска. – [Электронный ресурс]. – Режим доступа: https://www.n-vartovsk.ru/inf/legaleducation/clarify/460484.html.

23. Доктрина информационной безопасности Российской Федерации // Совет Безопасности Российской Федерации. – [Электронный ресурс]. – Режим доступа: http://www.scrf.gov.ru/security/information/document5/.

24. Лисаускайте В.В. «Командная ответственность» и военные преступления: вопросы юридической оценки // Вестник Восточно-Сибирского института Министерства внутренних дел России. – 2025. – № 1 (112). – С. 222-229. – [Электронный ресурс]. – Режим доступа: https://sciup.org/komandnaja-otvetstvennost-i-voennye-prestuplenijavoprosy-juridicheskoj-ocenki-143184351.

25. Джейми А. Уильямсон Некоторые размышления об ответственности командования и уголовной ответственности // Международный журнал Красного Креста. – 2008. – № 90 (870). –

С. 131-153. – [Электронный ресурс]. – Режим доступа: https://www.icrc.org/sites/default/files/external/doc/ru/assets/files/other/131-153.pdf.

26. Таллинское руководство // Википедия. – [Электронный ресурс]. – Режим доступа: https://goo.su/vYEux1.

27. Invited Experts on Cyberwarfare Question // ICCforum. – [Электронный ресурс]. – Режим доступа: https://iccforum.com/cyberwar.

28. Есаков Г.А. Ответственность командиров в российском уголовном праве с точки зрения De Lege Lata // Lex russica. – 2017. – № 11 (132). – С. 93-99. – [Электронный ресурс]. – Режим доступа: https://lexrussica.msal.ru/jour/article/download/460/461.

29. В связи с ратификацией Римского статута в УК появится новая статья об ответственности военных командиров // Судебно-юридическая газета. – [Электронный ресурс]. – Режим доступа: https://sud.ua/ru/news/publication/310716-v-svyazi-s-ratifikatsiey-rimskogo-statuta-v-uk-poyavitsya-novaya-statya-ob-otvetstvennosti-voennykh-komandirov.

30. Кибервойна и международное гуманитарное право // Международный комитет красного креста. – [Электронный ресурс]. – Режим доступа: https://www.icrc.org/ru/document/kibervoyna-i-mezhdunarodnoe-gumanitarnoe-pravo.

31. Жизель Л., Роденхойзер Т., Дёрман К. Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперaций во время вооруженных конфликтов // Международный журнал Красного Креста. – 2021. – № 913. – С. 367-425. – [Электронный ресурс]. – Режим доступа: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-12/IRRC_913_pp367-425_Article_by_Gisel_Rodenhauser_Dormann_RU.pdf.

32. О Таллинском руководстве по ведению кибервойн // Around Cyber. – [Электронный ресурс]. – Режим доступа: https://aroundcyber.wordpress.com/2013/05/06/lukatsky-tallin-manual/.

33. 8 rules for “civilian hackers” during war, and 4 obligations for states to restrain them // Humanitarian: law&policy. – [Электронный ресурс]. – Режим доступа: https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.

34. Абрашин Р. По тонкому льду: квалификация кибератак на персональные данные в соответствии с международным гуманитарным правом // Журнал ВШЭ по международному праву. – 2024. – № 4. – С. 36-52. – [Электронный ресурс]. – Режим доступа: https://jil.hse.ru/article/download/24743/20393.

35. Пузырева Ю.В. Международно-правовая квалификация методов и средств ведения войны в информационном пространстве // Московский журнал международного права. – 2024. – № 4. – С. 146-161. – [Электронный ресурс]. – Режим доступа: https://www.mjil.ru/jour/article/view/2833.

36. US charges 7 Russian military agents linked to global cyber hack – BBC News // YOUTUBE. – [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=anTfn7OXGFI.

CYBER CRIMES COMMITTED BY MILITARY PERSONNEL: A NEW CATEGORY OF MILITARY OFFENSES

K.Z. Shoranov, *Graduate Student*
Supervisor: *A.S. Sidorov, Senior Lecturer, Retired Colonel of Justice*
V.M. Lebedev Russian State University of Justice
(Russia, Moscow)

Abstract. *The article examines the phenomenon of cyber crimes committed by military personnel as an independent and qualitatively new category of military offenses. It analyzes the current system of criminal law norms of the Russian Federation and international law in relation to this issue, identifies gaps in regulation, and proposes ways to improve legislation. Special attention is paid to the correlation of the norms of Chapter 28 and Chapter 33 of the Criminal Code of the Russian Federation in the qualification of the acts of military personnel in the information environment, the institution of command responsibility in the context of cyber operations, and the application of international law. humanitarian law in relation to military operations in cyberspace.*

Keywords: *cybercrimes; military personnel; military crimes; cyber operations; information space; criminal liability; command responsibility; international humanitarian law; Tallinn Manual.*