Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

УДК 340.1 https://doi.org/10.33619/2414-2948/124/56

ПРОКУРОРСКИЙ НАДЗОР В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

©***Сматов Ж. С***., *Международный университет Кыргызстана, г. Бишкек, Кыргызстан*

PROSECUTOR'S SUPERVISION IN THE FIELD OF CYBERSECURITY AND INFORMATION SPACE PROTECTION

©***Smatov Zh***., *International University of Kyrgyzstan, Bishkek, Kyrgyzstan*

Аннотация. Рассматриваются особенности прокурорского надзора в сфере кибербезопасности и защиты информационного пространства в условиях цифровизации общественных отношений. Анализируется роль прокуратуры в обеспечении законности при противодействии киберугрозам, распространению экстремистских материалов, незаконному обороту информации и иным правонарушениям в цифровой среде. Особое внимание уделяется нормативно-правовой базе, регламентирующей полномочия прокурора в данной сфере, а также вопросам координации деятельности правоохранительных и контролирующих органов. Обосновывается необходимость развития профилактической и аналитической функции прокурорского надзора с использованием цифровых инструментов мониторинга. Делается вывод о том, что прокурорский надзор в сфере кибербезопасности становится важным элементом государственной политики обеспечения общественной и информационной безопасности.

Abstract. This article examines the specifics of prosecutorial oversight in the area of cybersecurity and information security in the context of the digitalization of public relations. It analyzes the role of the prosecutor's office in ensuring the rule of law when countering cyberthreats, the dissemination of extremist materials, illegal information trafficking, and other offenses in the digital environment. Particular attention is paid to the legal framework governing the prosecutor's powers in this area, as well as to the coordination of law enforcement and regulatory agencies. The need to develop the preventive and analytical functions of prosecutorial oversight using digital monitoring tools is substantiated. It is concluded that prosecutorial oversight in the area of cybersecurity is becoming an important element of state policy for ensuring public and information security.

Ключевые слова: прокуратура, прокурорский надзор, кибербезопасность, информационное пространство, цифровая среда, профилактика правонарушений, экстремистские материалы, государственная безопасность, мониторинг, законность.

Keywords: prosecutor's office, prosecutorial supervision, cybersecurity, information space, digital environment, crime prevention, extremist materials, state security, monitoring, legality.

Актуальность исследования обусловлена тем, что цифровизация общественных отношений привела к формированию новых угроз общественной и государственной безопасности, связанных с распространением экстремистских материалов, киберпреступностью, фейковизацией информационного пространства и нарушением прав граждан в сети Интернет. В этих условиях особое значение приобретает прокурорский надзор

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

как инструмент обеспечения законности в цифровой среде. Прокуратура, обладая надзорными и координационными полномочиями, становится важным субъектом защиты информационного пространства и противодействия киберугрозам [1].

Современные исследования подчеркивают, что прокурорский надзор в сфере кибербезопасности выходит за рамки традиционного контроля за исполнением законов и приобретает профилактическую и аналитическую направленность, связанную с мониторингом интернет-ресурсов, защитой несовершеннолетних в цифровой среде и противодействием распространению недостоверной и противоправной информации [2, 5].

В условиях развития цифровых технологий возрастает значение взаимодействия прокуратуры с органами государственной власти, обеспечивающими кибербезопасность, а также внедрения цифровых инструментов в деятельность прокурора [8].

Целью исследования является анализ теоретико-правовых основ и практических аспектов прокурорского надзора в сфере кибербезопасности и защиты информационного пространства.

Для достижения поставленной цели определены следующие задачи: раскрыть понятие кибербезопасности и защиты информационного пространства; определить место прокуратуры в системе обеспечения информационной безопасности; выявить превентивный потенциал прокурорского надзора в цифровой среде.

Объектом исследования являются общественные отношения, возникающие в процессе обеспечения информационной безопасности и противодействия киберугрозам.

Предметом исследования выступают нормы законодательства, регулирующие деятельность прокуратуры в сфере кибербезопасности, а также практика их применения.

Методологическую основу исследования составляют формально-юридический, системный и сравнительно-правовой методы анализа, а также изучение научных источников, посвящённых вопросам прокурорского надзора и информационной безопасности [4, 7].

Научная новизна работы заключается в комплексном рассмотрении прокурорского надзора в цифровой среде как самостоятельного направления деятельности прокуратуры, обладающего значительным профилактическим потенциалом в системе обеспечения общественной безопасности.

Стремительное развитие цифровых технологий привело к появлению качественно новых форм правонарушений: кибермошенничества, распространения экстремистских материалов в сети Интернет, фейковизации информационного пространства, незаконного оборота персональных данных, вовлечения несовершеннолетних в противоправную деятельность через цифровые платформы. Эти процессы трансформировали не только характер угроз, но и подходы государства к обеспечению законности. Если ранее основное внимание уделялось контролю за традиционными средствами массовой информации и офлайн-пространством, то сегодня ключевая зона правовых рисков переместилась в цифровую среду. В этой связи прокурорский надзор приобретает новое измерение. Он выходит за рамки традиционного контроля за исполнением законов и становится инструментом обеспечения законности в информационном пространстве, где границы юрисдикции размыты, а правонарушения носят транснациональный и технологически сложный характер. Прокуратура, обладая универсальными надзорными полномочиями, способна обеспечивать соблюдение законодательства в деятельности всех субъектов, задействованных в сфере кибербезопасности: органов связи, операторов цифровых платформ, правоохранительных органов, образовательных и социальных учреждений.

Кибербезопасность в современном правовом понимании представляет собой состояние защищённости информационных систем, цифровых ресурсов, персональных данных и

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

пользователей от противоправных посягательств, а также от информационных угроз, способных нанести вред личности, обществу и государству. Это понятие включает не только технические аспекты защиты, но и правовые механизмы регулирования деятельности в цифровой среде. Защита информационного пространства предполагает комплекс мер, направленных на: предотвращение распространения запрещённой информации (экстремистских, террористических материалов, фейков); обеспечение безопасности несовершеннолетних в сети Интернет; защиту персональных данных и частной жизни граждан; регулирование деятельности интернет-ресурсов и цифровых платформ; формирование достоверной информационной среды. В правовом аспекте кибербезопасность охватывает систему норм, регулирующих отношения в сети Интернет, устанавливающих ответственность за киберправонарушения и определяющих полномочия государственных органов в данной сфере [3].

Кибербезопасность является не только технической, но и правовой категорией, в которой ключевую роль играет обеспечение законности. Прокуратура занимает особое место среди субъектов обеспечения информационной безопасности, поскольку осуществляет высший надзор за точным и единообразным исполнением законов всеми органами и должностными лицами. В отличие от органов, непосредственно обеспечивающих кибербезопасность (органы связи, национальной безопасности, внутренних дел), прокуратура не выполняет оперативных функций, а обеспечивает законность их деятельности. Надзорные полномочия позволяют прокурору: контролировать соблюдение законодательства о связи, информации и защите персональных данных; проверять законность блокировки интернет-ресурсов и ограничений доступа к информации; реагировать на распространение экстремистских материалов и фейковой информации; осуществлять надзор за защитой прав несовершеннолетних в цифровой среде [2].

Прокуратура выступает гарантом соблюдения прав граждан при реализации мер кибербезопасности и одновременно субъектом профилактики правонарушений в информационном пространстве. Прокурорский надзор в цифровой среде обладает значительным превентивным потенциалом. Мониторинг интернет-ресурсов, реагирование на выявленные нарушения, взаимодействие с органами, обеспечивающими кибербезопасность, позволяют предупреждать распространение противоправной информации и минимизировать риски киберугроз. Превентивная функция проявляется также в использовании цифровых инструментов анализа и мониторинга правоприменительной практики, что способствует формированию эффективной системы предупреждения правонарушений в информационном пространстве. Эффективность прокурорского надзора в сфере кибербезопасности напрямую зависит от нормативно-правовой базы, регулирующей как деятельность прокуратуры, так и вопросы функционирования информационного пространства. Данная база носит комплексный характер и включает конституционные положения, отраслевое законодательство о прокуратуре, законы, регулирующие сферу связи и информации, а также нормы о противодействии экстремизму и защите прав граждан в цифровой среде.

Конституционные положения, закрепляющие приоритет прав и свобод человека, принцип законности и обязанность государства обеспечивать общественную безопасность, формируют фундамент для деятельности прокуратуры в том числе и в цифровой среде. Поскольку информационное пространство сегодня является частью социальной и правовой реальности, надзор за точным и единообразным исполнением законов объективно распространяется и на сферу интернет-отношений. Конституционный статус прокуратуры как органа высшего надзора позволяет ей реагировать на любые нарушения закона вне зависимости от формы их проявления — в традиционной или цифровой среде. Это означает,

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

что прокурор вправе вмешиваться при выявлении нарушений, связанных с распространением противоправной информации, нарушением прав граждан в сети Интернет, незаконным ограничением доступа к информации или, напротив, бездействием органов, обязанных обеспечивать информационную безопасность. Законодательство о прокуратуре конкретизирует данные конституционные положения, закрепляя право прокурора: проводить проверки исполнения законодательства в сфере информации и связи; вносить акты прокурорского реагирования при выявлении нарушений в деятельности органов и организаций, обеспечивающих кибербезопасность; координировать деятельность правоохранительных органов в части противодействия правонарушениям в цифровой среде; защищать права граждан, нарушенные в информационном пространстве [3].

Именно нормы о прокуратуре создают универсальную правовую основу, позволяющую прокурору осуществлять надзор за законностью в цифровом пространстве, не будучи при этом специализированным органом в сфере информационных технологий.

Ключевым инструментом реализации прокурорского надзора в киберпространстве выступает отраслевое законодательство, регулирующее сферу связи, распространения информации и противодействия экстремистской деятельности. Эти нормативные акты устанавливают правовой режим функционирования интернет-ресурсов, цифровых платформ, операторов связи и средств массовой информации. Данные нормы определяют: требования к размещению и распространению информации в сети Интернет; порядок ограничения доступа к запрещённым ресурсам; обязанности владельцев интернет-платформ по удалению противоправного контента; меры по защите несовершеннолетних от вредной информации; ответственность за распространение экстремистских и фейковых материалов. Прокурор, осуществляя надзор за исполнением этих норм, получает возможность реагировать на факты размещения запрещённой информации, требовать её удаления, инициировать блокировку ресурсов и проверять законность действий органов, уполномоченных в сфере связи и информации [5, 6].

Законодательство о связи, информации и противодействии экстремизму становится для прокуратуры практическим правовым инструментом, позволяющим реализовывать надзорные полномочия в цифровой среде и обеспечивать защиту прав граждан в информационном пространстве. Международные стандарты, выработанные в рамках ООН и других международных организаций, оказывают влияние на формирование национального законодательства в сфере кибербезопасности. Эти стандарты направлены на обеспечение защиты информационного пространства, борьбу с киберпреступностью и соблюдение прав человека в цифровой среде. Прокурорский надзор развивается с учетом данных международных подходов, что способствует гармонизации национального законодательства и практики с международными требованиями в области защиты информационной безопасности [4].

Прокурорский надзор в цифровой среде имеет комплексный характер и реализуется по нескольким приоритетным направлениям, каждое из которых связано с обеспечением законности, защитой прав граждан и предупреждением правонарушений в сети Интернет. В условиях, когда значительная часть общественных отношений переместилась в цифровое пространство, именно эти направления формируют практическое содержание прокурорской деятельности в сфере кибербезопасности. Данные направления охватывают контроль за содержанием распространяемой информации, надзор за деятельностью интернет-ресурсов и цифровых платформ, а также постоянное взаимодействие с государственными органами, обеспечивающими информационную безопасность. Одной из центральных задач прокурорского надзора является выявление и пресечение распространения запрещённой

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

информации в сети Интернет. К такой информации относятся: экстремистские и террористические материалы, призывы к насилию, пропаганда радикальной идеологии, фейковая информация, способная вызвать общественную дестабилизацию, а также контент, наносящий вред несовершеннолетним. Особенность данной деятельности заключается в том, что противоправная информация распространяется с высокой скоростью, может дублироваться на различных платформах и нередко размещается анонимными пользователями. В этих условиях прокурор осуществляет мониторинг информационного пространства, анализирует поступающие сигналы от правоохранительных органов, граждан и организаций, а также использует данные уполномоченных органов. При выявлении нарушений прокурор применяет акты прокурорского реагирования: выносит представления, требования об устранении нарушений, инициирует ограничение доступа к интернет-ресурсам, направляет материалы в уполномоченные органы для блокировки противоправного контента [5, 7].

Такая деятельность носит не только карательный, но и предупредительный характер, поскольку предотвращает дальнейшее распространение вредной информации. Современные цифровые платформы — социальные сети, видеохостинги, мессенджеры, новостные порталы — оказывают значительное влияние на формирование общественного мнения и поведение пользователей. В этой связи прокурорский надзор распространяется на соблюдение ими требований законодательства о распространении информации, защите персональных данных, рекламе, противодействии экстремизму и защите несовершеннолетних. Надзорная деятельность включает: проверку выполнения владельцами интернет-ресурсов обязанностей по удалению запрещённого контента; анализ механизмов модерации информации на цифровых платформах; оценку соблюдения требований по защите персональных данных пользователей; контроль за исполнением мер по защите несовершеннолетних от вредной информации. Особое значение приобретает предотвращение вовлечения несовершеннолетних в противоправную деятельность через интернет, что требует усиленного внимания прокуратуры к деятельности образовательных платформ, социальных сетей и развлекательных ресурсов [1].

Таким образом, прокурорский надзор в отношении интернет-ресурсов и цифровых платформ направлен на формирование безопасной и законной информационной среды, в которой минимизируются риски киберугроз и нарушений прав граждан. Эффективность прокурорского надзора в информационном пространстве во многом зависит от взаимодействия с органами, обеспечивающими кибербезопасность, такими как органы внутренних дел, органы национальной безопасности, органы связи и информационных технологий. Прокурор координирует их деятельность, обеспечивает законность принимаемых мер и участвует в обмене информацией, что позволяет оперативно реагировать на киберугрозы и предупреждать правонарушения в цифровой среде. Несмотря на расширение полномочий прокуратуры в сфере защиты информационного пространства, реализация прокурорского надзора в цифровой среде сталкивается с рядом объективных ограничений. Эти трудности связаны с необходимостью соблюдения прав и свобод человека, динамичным развитием цифровых технологий и спецификой правоприменительной практики. Контроль за информационным пространством неизбежно затрагивает конституционные права граждан — свободу выражения мнения, право на получение и распространение информации, право на неприкосновенность частной жизни. Примеры:

Блокировка интернет-ресурса по требованию прокурора за размещение запрещённого контента может затронуть и законные материалы, размещённые на той же платформе.

Мониторинг социальных сетей и мессенджеров с целью выявления экстремистских материалов может восприниматься как вмешательство в частную переписку пользователей.

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

Ограничение доступа к информации под предлогом борьбы с фейками может вступать в противоречие с принципами свободы слова.

Таким образом, прокурорский надзор требует особой осторожности и строгого соблюдения процессуальных гарантий.

Законодательство зачастую не успевает за развитием цифровых технологий. Появление новых платформ, способов передачи информации, анонимных сервисов и технологий шифрования создает ситуации, когда существующие нормы не дают чётких механизмов реагирования. Примеры: Сложности в правовом регулировании деятельности иностранных интернет-платформ, не имеющих юридического представительства в стране. Отсутствие чётких процедур взаимодействия с администрациями зарубежных социальных сетей при выявлении противоправного контента. Проблемы квалификации новых форм киберпреступности и цифровых правонарушений.

Это затрудняет реализацию прокурорского надзора и требует постоянного обновления нормативной базы. На практике прокуроры сталкиваются с техническими и организационными трудностями при осуществлении надзора в цифровой среде. Недостаточный уровень технической подготовки, ограниченный доступ к специализированным цифровым инструментам и сложность идентификации нарушителей снижают эффективность надзорной деятельности. Примеры: Трудности установления личности лица, распространяющего запрещённую информацию под анонимным аккаунтом. Сложности в сборе и фиксации цифровых доказательств, которые могут быть быстро удалены или изменены. Зависимость от информации, предоставляемой операторами связи и интернет-платформами, что может затягивать процесс реагирования. Прокурорский надзор в цифровой среде требует не только правового, но и технологического обеспечения, а также повышения квалификации сотрудников [3].

Стремительное развитие цифровых технологий и усложнение киберугроз требуют модернизации подходов к прокурорскому надзору в информационном пространстве. В современных условиях прокурор должен обладать не только правовыми, но и технологическими инструментами для эффективной реализации своих полномочий. Развитие данного направления связано с совершенствованием законодательства, внедрением цифровых инструментов мониторинга и усилением профилактической составляющей надзора. Одним из ключевых направлений является адаптация законодательства к реалиям цифровой среды. Необходимо уточнение понятийного аппарата, регламентация процедур взаимодействия с интернет-платформами, установление чётких механизмов блокировки противоправного контента и обеспечения доказательственной базы в киберпространстве. Совершенствование нормативной базы позволит устранить правовые пробелы и обеспечить более эффективную реализацию надзорных полномочий прокуратуры. Цифровые технологии открывают новые возможности для прокурорского надзора. Использование специализированных программ мониторинга интернет-ресурсов, аналитических платформ, автоматизированных баз данных и инструментов цифровой фиксации доказательств позволяет своевременно выявлять противоправный контент и реагировать на него. Внедрение таких инструментов способствует переходу от реактивной модели надзора к проактивной, основанной на постоянном анализе информационного пространства. Прокурорский надзор в сфере кибербезопасности должен быть ориентирован не только на пресечение нарушений, но и на их предупреждение. Это предполагает правовое просвещение пользователей интернета, взаимодействие с образовательными учреждениями, участие в формировании цифровой культуры и безопасного поведения в сети. Усиление профилактической направленности позволит снизить уровень киберправонарушений и укрепить информационную безопасность общества. Проведённое

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

исследование показало, что прокурорский надзор в сфере кибербезопасности и защиты информационного пространства становится самостоятельным и стратегически важным направлением деятельности прокуратуры в условиях цифровизации общественных отношений. Расширение цифровой среды создало новые формы правонарушений и угроз общественной безопасности, что потребовало адаптации надзорной функции прокуратуры к современным реалиям [8].

Анализ свидетельствует о наличии значительного потенциала прокурорского надзора в предупреждении распространения запрещённой информации, защите прав граждан в интернете и координации деятельности органов, обеспечивающих кибербезопасность. В то же время выявлены проблемы, связанные с рисками нарушения прав и свобод человека, недостаточностью правового регулирования цифровой сферы и трудностями практической реализации надзора. Развитие прокурорского надзора в киберпространстве требует совершенствования законодательства, внедрения цифровых инструментов мониторинга и усиления профилактической направленности деятельности прокуратуры. Это позволит обеспечить баланс между защитой информационного пространства и соблюдением прав граждан, а также повысить эффективность государственной политики в сфере кибербезопасности.

Список литературы:

1. Новиков А. И., Юдакова И. Р. Прокурорский надзор за противодействием киберпреступности в информационно-телекоммуникационной сети Интернет // Управление и цифровизация: национальное и региональное измерение: Материалы V научной конференции нац. науч.-практ. конф. с междунар. участием. Брянск, 2025. С. 245.

2. Арабаев Ч. И., Маатов И. С., Суеркулов У. Организация прокурорского надзора за исполнением законов в сфере информационной безопасности несовершеннолетних // Международный журнал гуманитарных и естественных наук. 2025. №2–3 (101). С. 175–180.

3. Мацкевич И. М. Информатизация в современном мире: уголовно-правовые и криминологические аспекты, профилактическая роль прокуратуры // Правопорядок: история, теория, практика. 2024. №3 (42). С. 89–95.

4. Танов Н. Р. Основные проблемы совершенствования правового регулирования взаимодействия органов прокуратуры и органов государственной власти РФ при противодействии преступлениям в киберпространстве, затрагивающим права человека // Legal Bulletin. 2024. Т. 9. №3. С. 98–107.

5. Белоусова Д. С. Об основных способах противодействия фейковизации информационного пространства средствами прокурорского надзора // Вопросы российского и международного права. 2024. Т. 14. №11-1. С. 122–128.

6. Евдокимов К. Н. Особенности прокурорского надзора за исполнением законодательства о противодействии экстремистской деятельности в Российской Федерации // Вестник Восточно-Сибирского института МВД России. 2022. №3. С. 155-169.

7. Степанова М. Н. Информационная безопасность в правовом поле: стратегии правового регулирования и защиты киберпространства // Правопорядок: история, теория, практика. 2024. №1 (40). С. 48–52.

8. Морозов Р. М., Пакова В. М. Цифровизация деятельности прокурора на досудебных стадиях уголовного процесса // Lex criminalis scientiarum. 2025. Т. 2. №4 (6). С. 345–352.

References:

1. Novikov, A. I., & Yudakova, I. R. (2025). Prokurorskii nadzor za protivodeistviem kiberprestupnosti v informatsionno-telekommunikatsionnoi seti Internet. In *Upravlenie i*

tsifrovizatsiya: natsional'noe i regional'noe izmerenie: Materialy V nauchnoi konferentsii nats. nauch.-prakt. konf. s mezhdunar. uchastiem. Bryansk, 245. (in Russian).

2. Arabaev, Ch. I., Maatov, I. S., & Suerkulov, U. (2025). Organizatsiya prokurorskogo nadzora za ispolneniem zakonov v sfere informatsionnoi bezopasnosti nesovershennoletnikh. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk,* (2–3 (101)), 175–180. (in Russian).

3. Matskevich, I. M. (2024). Informatizatsiya v sovremennom mire: ugolovno-pravovye i kriminologicheskie aspekty, profilakticheskaya rol' prokuratury. *Pravoporyadok: istoriya, teoriya, praktika,* (3 (42)), 89–95. (in Russian).

4. Tanov, N. R. (2024). Osnovnye problemy sovershenstvovaniya pravovogo regulirovaniya vzaimodeistviya organov prokuratury i organov gosudarstvennoi vlasti RF pri protivodeistvii prestupleniyam v kiberprostranstve, zatragivayushchim prava cheloveka. *Legal Bulletin, 9*(3), 98–107. (in Russian).

5. Belousova, D. S. (2024). Ob osnovnykh sposobakh protivodeistviya feikovizatsii informatsionnogo prostranstva sredstvami prokurorskogo nadzora. *Voprosy rossiiskogo i mezhdunarodnogo prava, 14*(11-1), 122–128. (in Russian).

6. Evdokimov, K. N. (2022). Osobennosti prokurorskogo nadzora za ispolneniem zakonodatel'stva o protivodeistvii ekstremistskoi deyatel'nosti v Rossiiskoi Federatsii. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii,* (3), 155-169. (in Russian).

7. Stepanova, M. N. (2024). Informatsionnaya bezopasnost' v pravovom pole: strategii pravovogo regulirovaniya i zashchity kiberprostranstva. *Pravoporyadok: istoriya, teoriya, praktika,* (1 (40)), 48–52. (in Russian).

8. Morozov, R. M., & Pakova, V. M. (2025). Tsifrovizatsiya deyatel'nosti prokurora na dosudebnykh stadiyakh ugolovnogo protsessa. *Lex criminalis scientiarum, 2*(4 (6)), 345–352. (in Russian).

Поступила в редакцию
25.01.2026 г.

Принята к публикации
01.02.2026 г.

Ссылка для цитирования:

Сматов Ж. С. Прокурорский надзор в сфере кибербезопасности и защиты информационного пространства // Бюллетень науки и практики. 2026. Т. 12. №3. С. 492-499. https://doi.org/10.33619/2414-2948/124/56

Cite as (APA):

Smatov, Zh. (2026). Prosecutor’s Supervision in the Field of Cybersecurity and Information Space Protection. *Bulletin of Science and Practice, 12*(3), 492-499. (in Russian). https://doi.org/10.33619/2414-2948/124/56