УДК 343.163 URL: https://ptsj.bmstu.ru/catalog/jur/crim/1133.html

ПРОКУРОРСКИЙ НАДЗОР ЗА ИСПОЛНЕНИЕМ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ: ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ, ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ

А.Р. Нигматуллин[1] adel.railevich@yandex.ru
SPIN-код: 4485-1950

Д.А. Печёнов[2] danilpechenov@gmail.com
SPIN-код: 2998-6946

[1] *Саратовская государственная юридическая академия, Саратов, Российская Федерация*

[2] *МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

Статья посвящена теоретическим и прикладным вопросам прокурорского надзора за исполнением законодательства в сфере противодействия киберугрозам. Актуальность обращения к заявленной проблематике обусловлена ростом числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, расширением круга объектов цифровой инфраструктуры и усложнением нормативных требований к обеспечению их безопасности. На основе изучения законодательства, научной доктрины и материалов прокурорской практики раскрыто юридическое содержание киберугрозы, систематизированы типичные нарушения, связанные с категорированием объектов критической информационной инфраструктуры, защитой информации, учетом компьютерных инцидентов и восстановлением нарушенных прав граждан. Научная новизна заключается в обосновании риск-ориентированной модели организации прокурорского надзора, предполагающей формирование цифрового профиля поднадзорного объекта, межведомственный обмен сведениями и оценку результативности мер реагирования по фактическому снижению угроз охраняемым законом интересам. Сформулированные положения могут быть использованы при совершенствовании организационно-распорядительных документов Генеральной прокуратуры Российской Федерации и методического обеспечения надзорной деятельности.

Ключевые слова: прокурорский надзор, киберугрозы, кибербезопасность, информационная безопасность, критическая информационная инфраструктура, цифровые права, компьютерные инциденты, прокурорское реагирование, цифровая трансформация

Введение. Расширение цифровой среды изменило представление о безопасности публичных и частных отношений. Государственное управление, финансовые операции, медицинская помощь, связь, транспорт и энергетика сегодня зависят от устойчивости информационных систем. Нарушение их работы может одновременно повлечь прекращение оказания социально значимых услуг, утрату имущества, распространение персональных данных

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

и дезорганизацию деятельности органов власти. Киберинцидент уже нельзя рассматривать только как техническую неисправность или как один из способов совершения преступления. Он способен затронуть несколько охраняемых законом интересов, причем последствия нередко выходят за пределы организации, в которой первоначально возникла уязвимость.

Такая трансформация закономерно влияет на содержание прокурорской деятельности. Обязанности по обеспечению информационной безопасности распределены между федеральными органами исполнительной власти, субъектами критической информационной инфраструктуры, операторами связи, обладателями информационных систем, организациями финансового рынка и иными участниками цифровых отношений. Исполнение этих обязанностей служит предметом прокурорской оценки постольку, поскольку их несоблюдение нарушает закон либо создает реальную угрозу правам граждан, общественным и государственным интересам.

Терминологическая неопределенность осложняет формирование единообразной практики. Российское законодательство использует категории «информационная угроза», «компьютерная атака», «компьютерный инцидент», «безопасность критической информационной инфраструктуры», однако универсального определения киберугрозы не содержит. А.А. Карцхия и Г.И. Макаренко рассматривают кибербезопасность как сложную совокупность публично-правовых и частноправовых отношений, возникающих по поводу защиты цифровой среды, а киберпреступность — как одну из форм посягательства на нее [1, с. 60–62]. Подобный подход позволяет не сводить работу прокуратуры исключительно к надзору за расследованием преступлений, совершенных с применением информационно-телекоммуникационных технологий.

Разграничение информационной и кибербезопасности, предложенное А.Б. Смушкиным, также имеет прикладное значение. Первая охватывает защиту любой информации независимо от формы ее существования, тогда как вторая связана преимущественно с цифровыми данными, сетями, программным обеспечением, информационными системами и подключенными устройствами [2, с. 117–118]. При такой трактовке к угрозам относятся не только вредоносное программное обеспечение, фишинг, социальная инженерия, DDOS-атаки и неправомерный доступ, но и утечки данных, уязвимости цифровых сервисов, дефекты организации защиты, несвоевременное реагирование на инциденты [2, с. 120–121].

Для прокурорской деятельности киберугрозу предлагается понимать как обусловленную противоправными действиями, технологической уязвимостью либо организационным упущением возможность причинения вреда

 © МГТУ им. Н.Э. Баумана, 2026

охраняемым законом интересам посредством воздействия на информацию, информационные системы, сети связи или цифровые сервисы. В этом определении намеренно соединены техническое и юридическое начала. Прокурор не оценивает надежность программного кода как таковую, но вправе установить, исполнена ли предусмотренная законом обязанность по защите системы, регистрации инцидента, передаче сведений уполномоченному органу и устранению последствий атаки.

Цель статьи состоит в уточнении правовой природы рассматриваемого направления надзора, определении его предметных границ, выявлении наиболее заметных правоприменительных затруднений и разработке предложений по их преодолению. Особое внимание уделено соотношению прокурорской и технической оценки цифровых рисков, поскольку именно здесь наиболее вероятны неоправданное сужение компетенции прокуратуры и подмена органов специального контроля.

Киберугроза как юридически значимый риск в предмете прокурорского надзора. Киберпространство не образует обособленной от права реальности. Каждая информационная система принадлежит определенному субъекту, используется для конкретной деятельности и подчиняется установленному правовому режиму. Поэтому цифровой риск приобретает значение для прокурора не вследствие своей технической сложности, а при наличии обязанности, которая не была исполнена вовсе либо исполнена ненадлежащим образом.

Между угрозой и мерой реагирования должна существовать последовательная юридическая связь: источник риска — правовая обязанность по его предупреждению — действие или бездействие поднадзорного субъекта — возможный либо наступивший вред. Например, обнаруженная уязвимость программного обеспечения сама по себе не всегда свидетельствует о нарушении закона. Иная оценка требуется, если организация знала о ней, была обязана установить обновление, провести тестирование или уведомить уполномоченный орган, но не сделала этого. Такой подход удерживает прокурорскую проверку в правовых пределах и препятствует ее превращению в технический аудит.

Д.Ю. Данилов и Н.Д. Бут связывают надзор в сфере критической информационной инфраструктуры (КИИ) с необходимостью обеспечить устойчивое и бесперебойное функционирование информационных ресурсов, имеющих критическое значение для обороны, экономики, здравоохранения, транспорта, энергетики и финансовой системы [3, с. 46–47]. Повреждение таких объектов отличается от обычного сбоя масштабом возможных последствий. Вместе с тем повышенная общественная значимость не отменяет требования о точном установлении предмета проверки. Принадлежность орга-

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

низации к субъектам КИИ не дает оснований для неопределенного вмешательства во все аспекты ее хозяйственной и технологической деятельности.

С учетом характера охраняемых интересов юридически значимые угрозы целесообразно подразделить на пять групп. Первую составляют инфраструктурные риски, связанные с нарушением устойчивости информационных систем и сетей, обеспечивающих деятельность критически важных отраслей. Ко второй относятся угрозы конфиденциальности, целостности и доступности персональных, банковских, служебных и иных охраняемых сведений. Третья группа охватывает коммуникационные посягательства: подмену абонентских номеров, использование сим-боксов, незаконный пропуск трафика, распространение вредоносных сообщений. В четвертую входят контентно-технологические риски — фишинговые сайты, цифровые финансовые пирамиды, ресурсы с инструкциями по совершению преступлений, вредоносные приложения. Пятую группу образуют новые угрозы, возникающие при использовании искусственного интеллекта, автоматизированного принятия решений и обработки больших массивов данных.

Предлагаемая классификация отличается от технической систематизации компьютерных атак. Ее основанием служит правовой режим объекта, на который направлено воздействие. Для каждой группы характерны собственный круг поднадзорных субъектов, нормативная база и набор возможных мер реагирования. При проверке безопасности КИИ центральное значение имеют категорирование, создание системы защиты и взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак. При оценке деятельности оператора персональных данных внимание переносят на правомерность обработки сведений, локализацию баз данных, управление доступом и уведомление об утечке. В отношении оператора связи проверяют исполнение обязанностей по идентификации абонентов, прекращению подменного трафика и противодействию мошенническим вызовам.

О.В. Кипкаев и И.В. Горошко выделяют несколько устойчивых направлений прокурорской работы: надзор за созданием и эксплуатацией информационных систем, безопасностью КИИ, защитой данных, деятельностью операторов связи, реализацией цифровых государственных программ и распространением информации в сети Интернет [4, с. 65–67]. Перечисленные направления позволяют говорить о формировании особой надзорной специализации. Она не становится самостоятельной отраслью в традиционном понимании, поскольку по-прежнему основывается на положениях статей 21 и 26 Федерального закона от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации». Однако объем специального регулирова-

 © МГТУ им. Н.Э. Баумана, 2026

ния, характер объектов и потребность в технических знаниях придают ей организационную самостоятельность.

Киберугрозы шире киберпреступности. Преступное посягательство представляет наиболее опасную, но не единственную форму реализации цифрового риска. Несоздание комиссии по категорированию, отсутствие плана реагирования, назначение неподготовленного ответственного работника или использование несертифицированного средства защиты могут не содержать признаков преступления. При этом подобные нарушения создают условия, при которых атака причинит более значительный вред. И.М. Мацкевич обоснованно связывает профилактическую роль прокуратуры с выявлением факторов, способствующих противоправному использованию цифровых технологий, а также с мониторингом интернет-пространства и своевременным ограничением доступа к опасным ресурсам [5, с. 92–94].

Предупредительный потенциал надзора имеет объективные пределы. Ю.О. Карпышева замечает, что отсутствие закрепленных в федеральном законодательстве обязанностей и компетентного контрольного субъекта заметно сужает возможности прокурора по раннему предупреждению нарушений, связанных с применением новых технологий [6, с. 395–397]. Прокурор не вправе создавать правило поведения вместо законодателя. Пробел может стать основанием для правотворческой инициативы, информационного письма либо обращения к уполномоченному органу, но не для возложения на организацию обязанности, которой закон еще не предусматривает.

Особенно заметен этот предел в отношениях, связанных с искусственным интеллектом. Алгоритмические системы уже используются для автоматизированной подготовки фишинговых сообщений, генерации вредоносного кода, имитации голоса и изображения, поиска уязвимостей. Одновременно такие технологии применяются для обнаружения подозрительных операций, анализа сетевого трафика и прогнозирования инцидентов. И.А. Соколов связывает участие прокуратуры в обеспечении информационной безопасности с необходимостью оценивать не саму технологию, а законность порядка ее разработки и применения, распределение обязанностей между участниками и достаточность государственного контроля [7, с. 104–106]. Подобная позиция помогает избежать упрощенного отношения к искусственному интеллекту исключительно как к источнику опасности.

Правозащитный аспект не должен растворяться в инфраструктурной проблематике. Цифровая безопасность личности включает защиту частной жизни, персональных данных, имущества, репутации, доступа к государственным и социальным услугам. А.А. Матушкина подчеркивает, что роль прокуратуры в этой сфере предполагает сочетание надзорных полномочий

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

с судебной защитой и мерами, направленными на реальное восстановление прав граждан [8, с. 220–222]. Поэтому устранение технического нарушения не всегда означает достижение конечного результата. Если вследствие утечки данных гражданину причинен ущерб, требуется оценка действий оператора, контролирующего органа, правоохранительных подразделений и доступных способов компенсации.

Предмет, пределы и организация надзорной деятельности в цифровой среде. Нормативную основу рассматриваемого направления образуют федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и № 152-ФЗ «О персональных данных», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», от 7 июля 2003 г. № 126-ФЗ «О связи», законодательство о банковской деятельности, государственной тайне и защите прав потребителей. Существенное значение имеют указы Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» и от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», постановления Правительства РФ, акты ФСТЭК России и ФСБ России. По оценке О.В. Кипкаева и И.В. Горошко, система регулирования информационных технологий и защиты сведений насчитывает свыше двухсот документов [4, с. 64–65].

Такой массив порождает практический вопрос: входит ли соблюдение технических требований подзаконных актов в предмет прокурорской проверки, если статья 21 Федерального закона от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» говорит об исполнении законов? Представляется, что правовая оценка должна строиться через норму законодательного уровня. Если федеральный закон возлагает на субъект обязанность создать систему безопасности, провести категорирование или выполнить требования уполномоченного органа, прокурор вправе оценить исполнение конкретизирующего нормативного акта. Ссылка только на ведомственное предписание без установления его законодательного основания недостаточна.

К объектам надзорного внимания относятся органы государственной власти и местного самоуправления, органы контроля, субъекты КИИ, операторы персональных данных, организации связи, владельцы информационных систем, кредитные и медицинские организации. Их круг нельзя считать раз и навсегда определенным. Цифровые отношения быстро меняются, возникают операторы платформ, биометрических систем, сервисов искусственного интеллекта и посредники по обработке информации. Основным критерием

 © МГТУ им. Н.Э. Баумана, 2026

остается наличие возложенной законом обязанности, затрагивающей охраняемые интересы.

Содержание надзора можно раскрыть через четыре уровня исполнения законодательства. Первый охватывает предупреждение инцидентов: учет информационных ресурсов, категорирование объектов, моделирование угроз, применение средств защиты, назначение ответственных работников. Второй связан с обнаружением и фиксацией атаки, сохранением электронных следов и передачей сведений компетентным органам. Третий включает локализацию последствий, восстановление работы систем и устранение уязвимости. На четвертом уровне решаются вопросы ответственности, возмещения ущерба и предупреждения повторных нарушений. Подобная структура ориентирует проверку не на наличие отдельных документов, а на весь цикл управления цифровым риском.

Предметные границы зависят от функции прокуратуры. При надзоре за исполнением законов проверяют деятельность организаций, операторов связи и органов контроля. Нарушения, допущенные подразделениями дознания, следствия или органами, осуществляющими оперативно-розыскную деятельность, оценивают с учетом правил соответствующих отраслей надзора. Координация борьбы с киберпреступностью вообще не является надзором, хотя тесно с ним связана. Смешение этих направлений затрудняет выбор полномочий и порождает спорные требования.

Отдельной осторожности требует ограничение доступа к интернет-ресурсам. Скорость распространения вредоносной информации оправдывает оперативное реагирование, но не отменяет необходимости проверять законность, соразмерность и точность блокировки. Ограничение доступа к целому сайту из-за отдельного материала может затронуть добросовестный контент и права неопределенного круга пользователей. Поэтому требование прокурора должно содержать ясное описание противоправной информации, правовое основание запрета и сведения, позволяющие индивидуализировать ресурс.

Информационно-аналитическое обеспечение остается слабым звеном. Сведения об объектах КИИ, компьютерных инцидентах, утечках данных, подменном трафике и результатах проверок находятся у разных ведомств. Их несопоставимость вынуждает прокурора собирать информацию вручную, а решение о проверке нередко принимается после поступления обращения или сообщения о причиненном вреде. П.В. Широкова связывает повышение качества прокурорской аналитики с развитием государственных информационных систем и обеспечением полноты аккумулируемых сведений [9, с. 198–199]. Электронный документооборот сам по себе не решает проблему, если он лишь воспроизводит разрозненный бумажный обмен.

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

Заслуживает внимания идея о цифровом профиле риска поднадзорного объекта. Такой профиль мог бы включать сведения о его правовом статусе, категории значимости, зарегистрированных инцидентах, ранее выявленных нарушениях, сроках исполнения представлений и результатах контрольных мероприятий. Алгоритмическое ранжирование помогло бы выделять организации, в которых одновременно присутствуют несколько неблагоприятных факторов. Окончательное решение о проверке должно сохраняться за прокурором: автоматическая оценка не учитывает качество исходных данных, специфику объекта и юридическую значимость предполагаемого нарушения.

Необходима и кадровая специализация. По мнению О.В. Кипкаева и И.В. Горошко, современный прокурор в этой сфере должен сочетать юридические знания с пониманием принципов функционирования информационных систем, программного обеспечения и менеджмента информационной безопасности [4, с. 74–75]. Речь не идет о превращении прокурорского работника в инженера. Однако без представления о категорировании КИИ, резервном копировании, цифровых следах и порядке реагирования на атаку невозможно сформулировать вопросы специалисту, оценить материалы контроля и выбрать адекватную меру реагирования.

Проблемы правоприменения и направления совершенствования прокурорского надзора. Первая системная проблема заключается в преобладании реактивного подхода. Поводом для проверки часто становится уже произошедшая атака, массовая утечка либо обращение потерпевшего. Между тем организационные недостатки могут существовать месяцами. При риск-ориентированной модели внимание должно смещаться к признакам возможного инцидента: непроведению категорирования, отсутствию резервного копирования, неисполнению предписаний контролирующих органов, кадровой необеспеченности и повторяемости однотипных сбоев.

Масштаб проблемы подтверждает официальная статистика. В 2025 г. в Российской Федерации зарегистрировано 675,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 11,8 % меньше, чем в 2024 г. Их удельный вес в общем числе зарегистрированных преступлений составил 38,1 %. Более половины таких деяний (352,2 тыс.) относились к категориям тяжких или особо тяжких; 63,5 % совершены путем кражи или мошенничества, 17,4 % — с целью незаконного производства, сбыта или пересылки наркотических средств [10]. Эти показатели характеризуют не весь массив цифровых угроз, а только зарегистрированную преступность. За их пределами остаются административные нарушения, технические инциденты без установленного злоумышленника и события, о которых организация не сообщила.

Состояние расследования также сохраняет проблемный характер. По итогам 2025 г. раскрываемость преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, составила 26,6 % против 23,2 % годом ранее; нераскрытыми остались 494,3 тыс. таких деяний, хотя их количество сократилось на 13,5 % [10]. В январе–августе 2026 г. число зарегистрированных преступлений рассматриваемой категории уменьшилось на 32 % по сравнению с аналогичным периодом 2025 г.; количество преступлений в сфере компьютерной информации снизилось на 40,4 %, дистанционных краж — на 19,7 %, ИТТ-мошенничеств — на 29 % [11]. Положительная динамика не устраняет необходимости своевременно получать сведения от банков и операторов связи, сохранять цифровые следы, полно исследовать движение денежных средств и использовать специальные знания.

Вторая проблема связана с формализацией проверок. Наличие утвержденного положения, приказа о назначении ответственного лица или акта категорирования еще не гарантирует готовности организации к атаке. Документы могут существовать только на бумаге, не пересматриваться после изменения конфигурации системы и не подтверждаться практическими тренировками. В то же время отсутствие документа иногда непосредственно создает угрозу жизни и здоровью людей.

Показателен пример Ловозерского района Мурманской области. В медицинском учреждении более 300 дней не разрабатывался план реагирования на компьютерные инциденты и ликвидации последствий атак. Нарушение угрожало устойчивой работе медицинской информационной системы и автоматизированного управления наркозно-дыхательными аппаратами. После вмешательства прокуратуры внесено представление и возбуждены три дела по части 2 статьи 13.12.1 КоАП РФ [12]. Здесь юридическая обязанность имеет вполне осязаемое содержание: от готовности персонала и системы зависит непрерывность медицинской помощи.

Третья проблема состоит в неполноте межведомственного обмена. ФСТЭК России располагает сведениями о категорировании и нарушениях требований защиты, ФСБ России — информацией о взаимодействии с ГосСОПКА, Роскомнадзор — данными об утечках и операторах персональных данных, Банк России — сведениями о подозрительных операциях, МВД России — материалами о преступлениях. Отсутствие общего аналитического контура приводит к тому, что один и тот же субъект оценивается фрагментарно. Между тем сочетание нескольких сигналов — повторных утечек, неисполненного предписания и инцидента с приостановлением работы — может свидетельствовать о системном характере нарушений.

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

Целесообразно установить регулярный автоматизированный обмен юридически значимыми сведениями между Генеральной прокуратурой РФ, ФСТЭК России, ФСБ России, Роскомнадзором, Банком России, Минцифры России и МВД России. Передаваться должны не массивы технической информации, а данные, необходимые для определения состояния законности: факт инцидента, категория объекта, нарушенная обязанность, срок устранения, принятое контрольное решение и сведения о повторности.

Четвертая проблема касается критериев эффективности. Количество представлений, исков и административных производств отражает интенсивность работы, но не позволяет судить, снизился ли риск. Более содержательными показателями могли бы стать число объектов, приведенных в соответствие с требованиями безопасности, продолжительность устранения критического нарушения, объем возвращенных потерпевшим средств, доля повторных инцидентов и количество восстановленных цифровых услуг.

Практика Волгоградской области подтверждает возможность совмещения различных результатов. В первом полугодии 2025 г. после прокурорского вмешательства нарушения устранены более чем на 30 объектах КИИ, ограничен доступ к 270 интернет-ресурсам. В защиту имущественных интересов потерпевших от IT-преступлений предъявлено 507 исков почти на 170 млн руб. [13]. Здесь надзор не ограничился пресечением формальных нарушений: использованы инфраструктурные, информационные и гражданско-правовые способы защиты.

Пятая проблема связана с выбором меры реагирования. Однотипное представление не всегда соответствует характеру угрозы. Если нарушение можно устранить безотлагательно, оправдано требование о принятии конкретных организационных мер. При уклонении от категорирования или непредставлении сведений возникает основание для административного производства. Когда бездействие создает продолжающуюся угрозу неопределенному кругу лиц, более результативным может быть обращение в суд. При наличии признаков преступления материалы подлежат направлению в орган предварительного расследования для решения вопроса об уголовном преследовании.

Предупреждение повторных нарушений требует анализа причин. Неисполнение требований часто объясняется не только недобросовестностью, но и нехваткой специалистов, сложностью закупки российских средств защиты, неоднозначностью отнесения организации к субъектам КИИ, частыми изменениями нормативных требований. Такая причина не освобождает от ответственности, однако влияет на содержание представления. Общая формула «устранить нарушения закона» здесь малополезна; прокурорский акт должен указывать, какие управленческие решения позволят восстановить законность.

 © МГТУ им. Н.Э. Баумана, 2026

Для упорядочения практики представляется оправданным принятие специального организационно-распорядительного акта генерального прокурора РФ. В нем целесообразно закрепить предмет и пределы надзора, типовые источники информации, порядок взаимодействия с органами специальной компетенции, основания привлечения специалистов, особенности оценки подзаконных технических требований и критерии выбора мер реагирования. Отдельный раздел может быть посвящен защите прав граждан при утечках персональных данных, дистанционном мошенничестве и неправомерном ограничении доступа к информации.

Повышение квалификации прокурорских работников должно строиться на разборе реальных инцидентов. Теоретического ознакомления с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» недостаточно. Необходимы практические модули по чтению актов категорирования, оценке планов реагирования, сохранению цифровых доказательств, взаимодействию с техническими специалистами и выявлению фиктивного исполнения требований. Подобная подготовка позволит прокурору точнее отделять нарушение закона от технологического спора и сосредоточиваться на рисках, способных причинить существенный вред.

Заключение. Прокурорский надзор за исполнением законодательства в сфере противодействия киберугрозам развивается как комплексное направление, соединяющее защиту КИИ, персональных данных, цифровых прав граждан, законность деятельности операторов связи и контрольных органов. Его содержание нельзя сводить ни к технической проверке информационных систем, ни к надзору за расследованием киберпреступлений. В центре внимания находится юридически значимый цифровой риск, которому соответствует конкретная обязанность поднадзорного субъекта.

Предметные границы определяются через связь между источником угрозы, нормой закона, поведением организации и возможным вредом. Такая конструкция препятствует подмене специальных контролирующих органов и одновременно не позволяет им прикрывать бездействие технической сложностью регулируемых отношений. Прокурор оценивает не качество программного продукта как инженер, а полноту исполнения обязанностей по предупреждению, обнаружению, локализации инцидента и восстановлению нарушенных прав.

Дальнейшее развитие рассматриваемого направления связано с переходом к риск-ориентированному планированию, межведомственному обмену данными, созданию цифровых профилей поднадзорных объектов, углублением специализации работников и изменением критериев результативности.

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

В качестве основного показателя следует рассматривать не численность актов реагирования, а фактическое снижение уязвимости, восстановление законности и предупреждение повторного причинения вреда.

Согласованная реализация этих мер позволит сохранить правовую природу прокурорского надзора и одновременно приспособить его к отношениям, в которых промедление измеряется уже не месяцами и неделями, а временем распространения вредоносного кода, вывода денежных средств или остановки работы цифрового сервиса.

Литература

[1] Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности. *Вопросы кибербезопасности*, 2023, № 1 (53), с. 58–74. https://doi.org/10.21681/2311-3456-2023-1-58-74

[2] Смушкин А.Б. Кибербезопасность: понятие, структура, механизм правового обеспечения. *Правоприменение*, 2025, т. 9, № 3, с. 114–123. https://doi.org/10.52468/2542-1514.2025.9(3).114-123

[3] Данилов Д.Ю., Бут Н.Д. Защита критической информационной инфраструктуры средствами прокурорского надзора как важная составляющая национальной безопасности. *Вестник Университета прокуратуры Российской Федерации*, 2024, № 2 (100), с. 45–52.

[4] Кипкаев О.В., Горошко И.В. Первоосновы прокурорского надзора за исполнением законодательства в сфере информационных технологий и защиты информации. *Вестник Университета прокуратуры Российской Федерации*, 2025, № 5 (109), с. 63–76.

[5] 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. https://doi.org/10.47475/2311-696X-2024-42-3-89-95

[6] Карпышева Ю.О. Профилактика прокурором нарушений законов об искусственном интеллекте: постановка проблемы. *Всероссийский криминологический журнал*, 2022, т. 16, № 3, с. 392–399. https://doi.org/10.17150/2500-4255.2022.16(3).392-399

[7] Соколов И.А. Теоретические и практические аспекты участия прокурора в обеспечении информационной безопасности государства в сфере использования искусственного интеллекта. *Вестник Университета имени О.Е. Кутафина (МГЮА)*, 2024, № 6 (118), с. 101–108.

[8] Матушкина А.А. Роль органов прокуратуры по обеспечению цифровой безопасности личности. *Вестник Саратовской государственной юридической академии*, 2026, № 2 (169), с. 217–223.

 © МГТУ им. Н.Э. Баумана, 2026

[9] Широкова П.В. К вопросу о применении информационных систем в деятельности прокурора. *Вестник Костромского государственного университета*, 2023, т. 29, № 1, с. 196–200. https://doi.org/10.34216/1998-0817-2023-29-1-196-200

[10] *Состояние преступности в России за январь–декабрь 2025 года*. URL: https://мвд.рф/reports/item/77848182/ (дата обращения 26.10.2026).

[11] *МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за январь–август 2026 года*. URL: https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskuyu-informatsiyu-o-sostoyanii-prestupnosti/ (дата обращения 26.10.2026).

[12] *Прокуратурой Ловозерского района выявлены нарушения требований законодательства в области обеспечения информационной безопасности*. URL: https://epp.genproc.gov.ru/ru/proc_51/mass-media/news/regional/e8298168 (дата обращения 30.07.2026).

[13] *На коллегии в прокуратуре Волгоградской области подведены итоги работы регионального надзорного ведомства за первое полугодие 2025 года*. URL: https://epp.genproc.gov.ru/web/proc_34/mass-media/news?item=106772182 (дата обращения 30.07.2026).

Поступила в редакцию 22.10.2026

Нигматуллин Адель Раилевич — ассистент кафедры прокурорского надзора и криминологии Саратовской государственной юридической академии, Саратов, Российская Федерация.

Печёнов Данила Александрович — студент кафедры «Безопасность в цифровом мире» МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Нигматуллин А.Р., Печёнов Д.А. Прокурорский надзор за исполнением законодательства в сфере противодействия киберугрозам: теоретико-правовые основы, проблемы правоприменения и направления совершенствования. *Политехнический молодежный журнал*, 2026, № 5 (106). URL: https://ptsj.bmstu.ru/catalog/jur/crim/1133.html

© МГТУ им. Н.Э. Баумана, 2026 ISSN 2541-8009

PROSECUTORIAL SUPERVISION OVER ENFORCEMENT OF LEGISLATION IN COUNTERING CYBER THREATS: THEORETICAL AND LEGAL FOUNDATIONS, LAW ENFORCEMENT PROBLEMS AND AREAS FOR IMPROVEMENT

A.R. Nigmatullin1 adel.railevich@yandex.ru
SPIN-code: 4485-1950

D.A. Pechenov2 danilpechenov@gmail.com
SPIN-code: 2998-6946

[1] *Saratov State Law Academy, Saratov, Russian Federation*

[2] *Bauman Moscow State Technical University, Moscow, Russian Federation*

The article examines theoretical and applied issues of prosecutorial supervision over compliance with legislation in the field of countering cyber threats. The relevance of the study is determined by the growth in the number of crimes committed using information and telecommunication technologies, the expansion of digital infrastructure, and the increasing complexity of regulatory requirements for its security. Based on legislation, legal doctrine, and prosecutorial practice, the legal content of a cyber threat is clarified and typical violations related to categorization of critical information infrastructure facilities, information protection, recording of computer incidents, and restoration of violated rights are systematized. The scientific novelty lies in substantiating a risk-oriented model of prosecutorial supervision that includes creation of a digital risk profile of a supervised entity, interagency exchange of information, and assessment of the effectiveness of prosecutorial measures by the actual reduction of threats to legally protected interests. The proposed provisions may be used to improve organizational and administrative acts of the Prosecutor General's Office of the Russian Federation and methodological support for prosecutorial supervision.

Keywords: prosecutorial supervision, cyber threats, cybersecurity, information security, critical information infrastructure, digital rights, computer incidents, prosecutorial response, digital transformation

References

[1] Kartskhiya A.A., Makarenko G.I. Pravovye aspekty sovremennoy kiberbezopasnosti i protivodeystviya kiberprestupnosti [Legal aspects of modern cybersecurity and countering cybercrime]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2023, no. 1 (53), pp. 58–74. (In Russ.). https://doi.org/10.21681/2311-3456-2023-1-58-74

[2] Smushkin A.B. Kiberbezopasnost: ponyatie, struktura, mekhanizm pravovogo obespecheniya [Cybersecurity: concept, structure and legal support mechanism]. *Pravoprimenenie* [Law Enforcement Review], 2025, vol. 9, no. 3, pp. 114–123. (In Russ.). https://doi.org/10.52468/2542-1514.2025.9(3).114-123

 © BMSTU, 2026

[3] Danilov D.Yu., But N.D. Zashchita kriticheskoy informatsionnoy infrastruktury sredstvami prokurorskogo nadzora kak vazhnaya sostavlyayushchaya natsionalnoy bezopasnosti [Protection of critical information infrastructure by means of prosecutorial supervision as an important component of national security]. *Vestnik Universiteta prokuratury Rossiyskoy Federatsii* [Bulletin of the University of the Prosecutor's Office of the Russian Federation], 2024, no. 2 (100), pp. 45–52. (In Russ.).

[4] Kipkaev O.V., Goroshko I.V. Pervoosnovy prokurorskogo nadzora za ispolneniem zakonodatelstva v sfere informatsionnykh tekhnologiy i zashchity informatsii [Fundamentals of prosecutorial supervision over enforcement of legislation in information technology and information protection]. *Vestnik Universiteta prokuratury Rossiyskoy Federatsii* [Bulletin of the University of the Prosecutor's Office of the Russian Federation], 2025, no. 5 (109), pp. 63–76. (In Russ.).

[5] Matskevich I.M. Informatizatsiya v sovremennom mire: ugolovno-pravovye i kriminologicheskie aspekty, profilakticheskaya rol prokuratury [Informatization in the modern world: criminal-law and criminological aspects, preventive role of the prosecutor's office]. *Pravoporyadok: istoriya, teoriya, praktika* [Legal Order: History, Theory, Practice], 2024, no. 3 (42), pp. 89–95. (In Russ.). https://doi.org/10.47475/2311-696X-2024-42-3-89-95

[6] Karpysheva Yu.O. Profilaktika prokurorom narusheniy zakonov ob iskusstvennom intellekte: postanovka problemy [Prosecutor's prevention of violations of legislation regulating artificial intelligence: problem statement]. *Vserossiyskiy kriminologicheskiy zhurnal* [Russian Journal of Criminology], 2022, vol. 16, no. 3, pp. 392–399. (In Russ.). https://doi.org/10.17150/2500-4255.2022.16(3).392-399

[7] Sokolov I.A. Teoreticheskie i prakticheskie aspekty uchastiya prokurora v obespechenii informatsionnoy bezopasnosti gosudarstva v sfere ispolzovaniya iskusstvennogo intellekta [Theoretical and practical aspects of prosecutor participation in ensuring state information security in the use of artificial intelligence]. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)* [Courier of Kutafin Moscow State Law University (MSAL)], 2024, no. 6 (118), pp. 101–108. (In Russ.).

[8] Matushkina A.A. Rol organov prokuratury po obespecheniyu tsifrovoy bezopasnosti lichnosti [The role of prosecution bodies in ensuring an individual's digital security]. *Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii* [Bulletin of Saratov State Law Academy], 2026, no. 2 (169), pp. 217–223. (In Russ.).

[9] Shirokova P.V. K voprosu o primenenii informatsionnykh sistem v deyatelnosti prokurora [On the use of information systems in prosecutorial activities]. *Vestnik Kostromskogo gosudarstvennogo universiteta* [Vestnik of Kostroma State University], 2023, vol. 29, no. 1, pp. 196–200. (In Russ.). https://doi.org/10.34216/1998-0817-2023-29-1-196-200

[10] *Sostoyanie prestupnosti v Rossii za yanvar'–dekabr' 2025 goda* [The state of crime in Russia for January–December 2025]. Available at: https://мвд.рф/reports/item/77848182/ (accessed October 26, 2026). (In Russ.).

© BMSTU, 2026 ISSN 2541-8009

[11] *MVD Rossii publikuet statisticheskuyu informatsiyu o sostoyanii prestupnosti v Rossiyskoy Federatsii za yanvar'–avgust 2026 goda* [The Ministry of Internal Affairs of Russia publishes statistical information on the state of crime in the Russian Federation for January–August 2026]. URL: https://mvdmedia.ru/news/official/mvd-rossii-publikuet-statisticheskuyu-informatsiyu-o-sostoyanii-prestupnosti/ (accessed October 26, 2026). (In Russ.).

[12] *Prokuraturoy Lovozerskogo rayona vyyavleny narusheniya trebovaniy zakonodatelstva v oblasti obespecheniya informatsionnoy bezopasnosti* [The Lovozersky District Prosecutor's Office identified violations of information security legislation]. Available at: https://epp.genproc.gov.ru/ru/proc_51/mass-media/news/regional/e8298168 (accessed July 30, 2026). (In Russ.).

[13] *Na kollegii v prokurature Volgogradskoy oblasti podvedeny itogi raboty regionalnogo nadzornogo vedomstva za pervoe polugodie 2025 goda* [The Volgograd Region Prosecutor's Office summarized the work of the regional supervisory authority for the first half of 2025]. Available at: https://epp.genproc.gov.ru/web/proc_34/mass-media/news?item=106772182 (accessed July 30, 2026). (In Russ.).

Received 22.10.2026

Nigmatullin A.R. — Assistant, Department of Prosecutorial Supervision and Criminology, Saratov State Law Academy, Saratov, Russian Federation.

Pechenov D.A. — Student, Department of Security in the Digital World, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Nigmatullin A.R., Pechenov D.A. Prosecutorial Supervision over Enforcement of Legislation in Countering Cyber Threats: Theoretical and Legal Foundations, Law Enforcement Problems and Areas for Improvement. *Politekhnicheskiy molodezhnyy zhurnal*, 2026, no. 5 (106). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/jur/crim/1133.html

 © BMSTU, 2026