УДК 342.951:347.9
DOI: 10.36979/1694-500X-2025-25-11-52-57

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СУДЕБНОЙ СИСТЕМЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Г.М. Бозова

Аннотация. Анализируются законодательство Кыргызской Республики в сфере защиты персональных данных и электронных доказательств, а также нормативные правовые акты, регламентирующие безопасность электронных ресурсов. Подчеркивается потребность совершенствования правового регулирования информационной безопасности судебной системы с учётом развития цифровых технологий и выявления новых киберугроз. Внимание уделяется проблематике соблюдения принципов конфиденциальности и доступности информации в процессе судопроизводства. Делается вывод о необходимости комплексного подхода, основанного на взаимодействии государственных институтов и экспертного сообщества, что позволит обеспечить должный уровень защиты цифровых данных и укрепить доверие к судебной системе. Предлагаются направления совершенствования правоприменительной практики, способствующие формированию стабильной информационной инфраструктуры в отечественной юстиции. Информационная безопасность рассматривается как приоритетный вектор развития судебной системы, требующий постоянного мониторинга технологической среды и оперативного реагирования на возникающие угрозы.

Ключевые слова: информационная безопасность; судебная система; защита персональных данных; цифровизация судопроизводства; гласность судебного разбирательства; электронные доказательства; конфиденциальная информация.

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН СОТ ТУТУМУНДАГЫ МААЛЫМАТТЫК КООПСУЗДУКТУН УКУКТУК АСПЕКТТЕРИ

Г.М. Бозова

Аннотация. Бул илимий макалада Кыргыз Республикасындагы жеке маалыматтарды жана электрондук далилдерди коргоо багытында кабыл алынган мыйзамдар, ошондой эле электрондук ресурстардын коопсуздугун жөнгө салган ченемдик укуктук актылар талданат. Автор санариптик технологиялардын тездик менен өнүгүшү жана жаңы киберкоркунучтардын пайда болушу шартында сот тутумунун маалыматтык коопсуздугун укуктук жактан өркүндөтүү зарылдыгына көңүл бурат. Сот адилеттигин жүзөгө ашырууда купуялуулук жана маалыматтардын жеткиликтүүлүгү принциптерин сактоого байланыштуу көйгөйлөр өзгөчө белгиленет. Макалада мамлекеттик институттар менен эксперттик коомчулуктун өз ара әрекеттенүүсүнө таянган комплекстүү мамиленин маанилүүлүгү баса көрсөтүлөт, анткени ал санаиптик дайындардын коопсуздугун камсыздоого жана сот тутумуна болгон ишенимди жогорулатууга өбөлгө түзөт. Мындан тышкары, мекендеш сот тутумунда туруктуу маалыматтык инфраструктураны калыптандырууга багытталган укук колдонуу практикасында өркүндөтүү чаралары сунушталат. Маалыматтык коопсуздук сот тутумунун приоритеттүү өнүгүү багыты катары каралып, технологиялык чөйрөнү туруктуу мониторинг кылууну жана мүмкүн болуучу коркунучтарга ыкчам жооп берүүнү талап кылат.

Түйүндүү сөздөр: маалыматтык коопсуздук; сот тутуму; жеке маалыматтарды коргоо; сот өндүрүшүн санариптештирүү; сот отурумунун ачык-айкындуулугу; электрондук далилдер; купуя маалымат.

LEGAL ASPECTS OF INFORMATION SECURITY IN THE JUDICIAL SYSTEM OF THE KYRGYZ REPUBLIC

G.M. Bozova

Abstract. This scientific article examines the legislation of the Kyrgyz Republic in the field of personal data protection and electronic evidence, as well as regulatory legal acts governing the security of electronic resources. The author emphasizes the need to improve the legal regulation of information security in the judicial system, taking into account the development of digital technologies and the emergence of new cyber threats. Particular attention is given to issues related to the principles of confidentiality and the availability of information during legal proceedings. The conclusion is drawn that a comprehensive approach, based on collaboration between government institutions and the expert community, is required to ensure an adequate level of digital data protection and to strengthen trust in the judicial system. The article proposes directions for improving law enforcement practices that will help establish a stable information infrastructure in the nation's justice system. Information security is considered a priority vector for the development of the judicial system, necessitating constant monitoring of the technological environment and prompt responses to emerging threats.

Keywords: information security; judicial system; personal data protection; digitalization of judicial proceedings; transparency of court proceedings; electronic evidence; confidential information.

Информационная безопасность в судебной системе Кыргызской Республики занимает ключевое место в обеспечении надлежащего функционирования правосудия и защиты интересов государства, общества и отдельных граждан.

В условиях ускоренной цифровизации процедур судопроизводства, а также с учётом непрерывного роста объёмов обрабатываемых электронных данных, всё более актуальной становится задача системной регламентации и охраны конфиденциальной, служебной и иной защищаемой информации.

Правовое регулирование данной сферы призвано исключить любой несанкционированный доступ к судебным материалам, обеспечить аутентичность электронных доказательств, сохранить тайну информации, освящаемой в совещательной комнате и др. При этом, важна согласованность правовых норм как общего характера, направленных на обеспечение защиты информации, так и специальных нормативно-правовых предписаний, формируемых в рамках судебной системы, чтобы суды могли эффективно использовать инновационные технологии при сохранении высокого уровня защищённости цифровых систем.

Нормативно-правовая база, регулирующая информационную безопасность в судах, базируется прежде всего на Конституции Кыргызской Республики [1], которая закрепляет фундаментальные права граждан на неприкосновенность частной жизни, защиту персональных данных и охрану тайны переписки, переговоров и иной коммуникации.

На уровне конституционных принципов заложена необходимость недопущения нарушения прав и свобод личности при функционировании любых государственных механизмов, в том числе и судебных, что предполагает принятие общих и специальных законов, направленных на детальную регламентацию вопросов информационной безопасности.

Необходимо упомянуть также Закон Кыргызской Республики "Об информации персонального характера" [2], который устанавливает порядок сбора, хранения и обработки персональных данных, а также предусматривает обязанности держателей персональных данных в отношении их конфиденциальности. Его положения распространяются также и на судебную сферу, где при рассмотрении дел суды получают доступ к сведениям, способным идентифицировать участников процесса, их имущественное состояние, медицинские аспекты, либо иную частную информацию.

Данный Закон также закрепляет принципы целевого использования информации, допускает лишь ограниченное хранение и предупреждает о необходимости блокирования, либо уничтожения персональных данных, утративших актуальность. Дополнительные гарантии в этом отношении вносятся Законом Кыргызской

Республики “О праве на доступ к информации” [3], позволяющим обеспечивать принцип гласности судебного разбирательства, но одновременно определяющим границы разглашения данных, имеющих конфиденциальный или секретный характер, чтобы не пострадали права и законные интересы участников судебного спора.

Важным элементом правового поля, связанным с безопасностью информационной среды судопроизводства, выступает Закон “О защите государственных секретов Кыргызской Республики” [4], обязывающий соблюдать режим секретности при рассмотрении дел, затрагивающих сведения, отнесённые к государственной тайне, а также устанавливающий ограничения на их использование в судебной деятельности и хранение в электронных ресурсах. Суды в таких случаях обязаны применять специальные меры, предотвращающие несанкционированный доступ к материалам дела, а также соблюдать строжайшие правила по работе с системами электронного документооборота, где присутствуют секретные компоненты.

Необходимо отметить, что в условиях цифровой трансформации всё больше дел рассматриваются судами с использованием электронных доказательств, видеоконференцсвязи и иных инновационных технологий. Закон Кыргызской Республики “Об электронном управлении” [5] определяет правовые основы для развития и применения в судах электронных инструментов, в том числе электронного документооборота и цифровых подписей, а также устанавливает требования к созданию и эксплуатации информационных систем в государственных органах. Однако его положения носят во многом общий характер, не учитывая полностью узкую специфику судебной власти. По этой причине возникает необходимость в разработке подзаконных нормативных правовых актов и инструкций, которые могли бы содержать более чёткие требования к защите цифровых данных в судах, к формату их хранения, а также к процедурам доступа к электронным материалам дел и к системам распределения судей.

Связи норм о персональных данных и законодательства о государственной и коммерческой тайне дополняются положениями Закона Кыргызской Республики “О кибербезопасности Кыргызской Республики” [6], устанавливающего механизмы категорирования объектов информационной инфраструктуры (более многоаспектно регламентированные Положением “О порядке категорирования объектов критической информационной инфраструктуры Кыргызской Республики [7]), требованиями к проведению аудита кибербезопасности и реагированию на киберинциденты. Данному Закону отводится роль базиса для защиты систем судопроизводства, которые могут быть признаны частью критической информационной инфраструктуры. В частности, если государственный орган, ответственный за кибербезопасность, относит судебные информационные системы к объектам с высоким уровнем значимости, то суды и судебный департамент вынуждены исполнять требования о регулярном проведении проверок, настройке систем обнаружения угроз и соблюдении особых мер мониторинга. Реализация таких мер осложняется отсутствием в Законе прямых упоминаний о судебной специфике, но предполагается, что адаптированные инструкции, утверждённые уполномоченными органами и согласованные с судебным ведомством, позволят преодолеть имеющиеся пробелы.

Важными аспектами информационной безопасности судов Кыргызской Республики выступают вопросы обеспечения конфиденциальности и целостности электронных доказательств. В современных реалиях, когда стороны производят обмен документами, аудио- и видеоматериалами, используют электронные переписки, мессенджеры и прочие формы коммуникаций, суд сталкивается с опасностью появления поддельных или искажённых электронных доказательств. Следовательно, требуется чётко сформулированный регламент, описывающий порядок верификации источника, криптографических подписей, хранения медиаматериалов, а также установления ответственности за манипуляции с электронными документами.

Суд должен иметь технические возможности для идентификации владельцев электронных сообщений, для проверки метаданных файлов, что должно реализовываться на законодательном

уровне и через организационные меры судебного департамента.

Следующий немаловажный правовой аспект состоит в необходимости недопущения несанкционированного вмешательства в деятельность судов путём взлома информационных систем, кражи данных или саботажа серверов, содержащих судебные архивы. Подобные атаки могут привести к утере или изменению сведений по конкретным делам, а также к дискредитации и потере доверия к суду. Поскольку законодательство Кыргызской Республики о национальной безопасности и кибербезопасности уже предусматривает общий порядок реагирования на киберинциденты, суды должны иметь внутренние протоколы на случай угрозы, в том числе порядок резервного копирования, должны осуществлять немедленное уведомление компетентных органов, информирование участников процесса о возможности задержек в рассмотрении дел и восстановлении данных. В противном случае, каждый инцидент может перерасти в системный коллапс и привести к катастрофическим последствиям для системы правосудия.

В рамках защиты персональных данных сторон по делу, свидетелей, экспертов, а также судей и аппарата суда необходимо строго соблюдать Закон Кыргызской Республики "Об информации персонального характера" [8], но практика показывает, что зачастую суды публикуют в открытых источниках судебные акты с указанием персональных данных граждан, их адресов или номеров телефонов, что создаёт предпосылки для злоупотреблений. Хотя открытость и гласность судебного разбирательства – это основополагающий принцип, следует делать поправку на сохранение тайны личной и семейной жизни, а также не допускать раскрытия частных данных в сети Интернет.

В данном случае предполагается внедрение механизмов обезличивания при публикации судебных решений, использования специальных алгоритмов, позволяющих скрывать или шифровать фамилии и иные сведения при идентификации лиц. Таким образом, при подготовке судебных актов к публикации или размещении их на официальном сайте суда необходимо встраивать автоматизированные инструменты маскировки или исключения "чувствительной информации". Здесь важно обеспечивать баланс между принципом информационной открытости и необходимостью защиты конфиденциальных данных.

Ещё одной проблемой, встречающейся в судебной системе, является защита совещательной комнаты, которая теперь может существовать и в виртуальной форме, когда судьи ведут совещание по защищённым каналам видеосвязи. Необходимо законодательно закрепить правила такой удалённой работы судей, исключив любую возможность перехвата аудио- или видеосигнала. Подобная технология должна отвечать повышенным стандартам шифрования, а все аппараты и программное обеспечение, используемые для совещательной комнаты, должны быть сертифицированы в соответствии с национальными требованиями. Кроме того, при закрытых судебных заседаниях должна быть особая организация видеоконференцсвязи, исключающая какое бы то ни было присутствие посторонних лиц и несанкционированное копирование материалов заседания. Должный уровень защиты невозможен без соответствующих кадров. Судьи, работники канцелярий, IT-специалисты, сетевые администраторы судов обязаны иметь достаточный уровень знаний о механизмах и средствах защиты информации.

Актуальна проблема отсутствия в большинстве судов Кыргызской Республики сертифицированных специалистов в сфере кибербезопасности. Следовательно, государство должно обеспечивать образовательные курсы, семинары и стажировки, где бы судей и их помощников обучали правилам безопасного электронного документооборота, работе с электронными подписями, анализу надежности входящей корреспонденции, принципам фиксации киберинцидентов. Без такой практической компоненты, даже при существовании детально регламентированного законодательства, останутся уязвимости, связанные с человеческим фактором, поскольку простое игнорирование пароля или подключение подозрительного носителя информации в компьютер суда может привести к компрометации всего информационного массива.

Важным направлением совершенствования законодательства Кыргызской Республики становится трансграничный обмен данными. Когда суды рассматривают международные споры, либо направляют ходатайства в судебные органы других государств, актуализируются нормы о трансграничной передаче персональных данных и конфиденциальной информации, которые содержатся в Законе "Об информации персонального характера" [2] и Законе "О кибербезопасности Кыргызской Республики" [6]. В идеале необходим детализированный порядок, предусматривающий обязательство заключать соглашения либо пользоваться стандартными правовыми инструментами, гарантирующими высокий уровень защиты, чтобы не допустить незаконное распространение судебных материалов. Это может означать необходимость проверить, что государство или организация, получающая материалы, располагает механизмами, совместимыми с принципами защиты, установленными законодательством Кыргызской Республики.

Особый интерес представляют вопросы аудита кибербезопасности судебных учреждений. Закон "О кибербезопасности Кыргызской Республики" [6] вводит понятие обязательного аудита для критической инфраструктуры, что может распространяться на суды, если они будут отнесены к категории значимых объектов. Такой аудит должен производиться по утверждённым стандартам, с последующей выработкой рекомендаций и устранением выявленных уязвимостей.

Практика показала, что основными уязвимостями судов обычно становятся незащищённые сегменты сетей, плохой контроль прав доступа, использование устаревших программных продуктов без обновлений, отсутствие резервирования и шифрования каналов связи, а также хранилищ данных. В связи с этим требуется более тесное сотрудничество судебного департамента, уполномоченного органа по кибербезопасности и профильных органов государственной власти, ответственных за мониторинг и реагирование на кибератаки.

Рассматривая тему информационной безопасности в судах, нельзя обойти вопрос развития электронных доказательств. Различные цифровые документы, аудио-, видеозаписи, записи мессенджеров и социальных сетей уже играют важную роль в гражданских и уголовных делах. Закон должен регламентировать порядок изъятия, копирования и хранения таких доказательств, а также предусматривать процедуру проверки их достоверности и неизменности. Это может включать использование специальных программных средств, протоколов хеширования и электронной подписи, чтобы можно было убедиться, что файл, предоставленный стороной, не был подделан.

Кроме того, важно определить, в каких случаях можно ограничиваться онлайн-проверкой, а в каких необходимо назначение цифровой экспертизы с привлечением специалистов в области информационной безопасности. Одна из перспективных инициатив – создание централизованного банка цифровых доказательств, управляемого судебным департаментом или независимым специализированным государственным учреждением, который бы помогал сводить к минимуму риски утраты или модификации файлов, предоставлял защищённый доступ судей и сторон по делу.

Важное значение для практики защиты информации имеет взаимодействие с международными организациями и зарубежными коллегами. Многие государства сталкиваются с аналогичными вызовами цифровизации правосудия, и можно использовать опыт, основанный на положениях международных договоров, рекомендательных актов Совета Европы (например, Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера [9]). Отдельные аспекты, в частности в сфере трансграничных электронных доказательств, могут быть согласованы на уровне двусторонних соглашений. Желательно инициировать гармонизацию подходов стран ЕАЭС в плане передачи судебных актов, а также взаимодействия в рамках делегированных запросов.

Таким образом, законодательная база Кыргызской Республики в целом позволяет обеспечивать информационную безопасность в судебной системе, но нуждается в дальнейшей детализации и унификации. Следует в том числе совершенствовать правовую регламентацию

электронного правосудия, ориентируясь на передовые международные стандарты защиты данных. Важно также внедрить специальные ведомственные регламенты, где прописывались бы технические и организационные требования к электронным системам судов, порядок управления доступом и разграничением прав, алгоритмы реагирования на кибератаки и киберинциденты, а также стандарты обезличивания информации при её обнародовании.

В качестве первоочередных мер целесообразно в том числе разработать и принять единую инструкцию для всех уровней судебной системы Кыргызской Республики по защите информации при электронном документообороте, а также создать совместно с уполномоченным органом по кибербезопасности и правоохранительными структурами постоянный консультационный орган, осуществляющий мониторинг и координацию действий на случай выявления и нейтрализации компьютерных угроз.

Не менее актуально решение проблемы подготовки квалифицированных кадров. Необходимо провести повсеместные обучающие программы для судей и сотрудников судов, охватывающие правила цифровой гигиены, методы защиты электронных документов, механизмы документирования факта несанкционированных вторжений. Только при комплексном подходе – внесении изменений в действующие законы, издании подробных подзаконных нормативных правовых актов, расширении штата специалистов по IT-безопасности в судебной системе и повышении компетенции работников судов и органов правопорядка – возможно обеспечить надлежащий уровень информационной безопасности. Это позволит повысить эффективность правосудия, сформировать доверие граждан к электронному судопроизводству, исключить утечки конфиденциальной информации и сохранить гарантию прав всех участников судебного процесса.

Поступила: 25.09.2025;
рецензирована: 09.10.2025; принята: 13.10.2025.

Литература

1. Конституция Кыргызской Республики от 5 мая 2021 года (Принята референдумом (всенародным голосованием) 11 апреля 2021 года). URL: https://cbd.minjust.gov.kg/1-2/edition/1202952/ru (дата обращения: 11.03.2025).
2. Закон Кыргызской Республики “Об информации персонального характера” от 14 апреля 2008 года № 58. URL: https://cbd.minjust.gov.kg/202269/edition/1239270/ru (дата обращения: 12.03.2025).
3. Закон Кыргызской Республики “О праве на доступ к информации” от 29 декабря 2023 года № 217. URL: https://cbd.minjust.gov.kg/4-5355/edition/11754/ru (дата обращения: 17.03.2025).
4. Закон Кыргызской Республики “О защите государственных секретов Кыргызской Республики” от 15 декабря 2017 года № 210 (15). URL: https://cbd.minjust.gov.kg/111719/edition/1229912/ru (дата обращения: 15.03.2025).
5. Закон Кыргызской Республики “Об электронном управлении” от 19 июля 2017 года № 127. URL: https://cbd.minjust.gov.kg/4-2445/edition/1119212/ru (дата обращения: 15.03.2025).
6. Закон Кыргызской Республики “О кибербезопасности Кыргызской Республики” от 17 июля 2024 года № 121. URL: https://cbd.minjust.gov.kg/4-5371/edition/13381/ru (дата обращения: 17.03.2025).
7. Положение “О порядке категорирования объектов критической информационной инфраструктуры Кыргызской Республики” (Утверждено постановлением Кабинета Министров Кыргызской Республики от 29 ноября 2024 года № 716). URL: https://cbd.minjust.gov.kg/230018570/edition/22227/ru (дата обращения: 22.03.2025).
8. Закон Кыргызской Республики “Об информации персонального характера” от 14 апреля 2008 года № 58. URL: https://cbd.minjust.gov.kg/202269/edition/1239270/ru (дата обращения: 19.03.2025).
9. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 года. URL: https://rm.coe.int/1680078c46 (дата обращения: 24.03.2025).