

ПОТЕНЦИАЛ ВНЕДРЕНИЯ КАМЕРЫ ХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Смушкин Александр Борисович¹,

канд. юрид. наук, доцент,
e-mail: skif32@yandex.ru

Вехов Виталий Борисович^{2,3},

д-р юрид. наук, профессор, академик РАН, Заслуженный деятель науки и образования РАН,
e-mail: v-vehov@mail.ru

¹Федеральное государственное бюджетное образовательное учреждение высшего образования
Саратовская государственная юридическая академия, г. Саратов, Россия,

²Московский государственный технический университет имени Н.Э. Баумана (НИУ), г. Москва, Россия

³Московский университет МВД России имени В.Я. Кикотя, г. Москва, Россия

Статья посвящена критической необходимости создания специализированного помещения для долгосрочного хранения и верификации электронных доказательств. Рассматривается переход от «физического» понимания вещественных доказательств к «логическому». Цель данной статьи – всесторонне обосновать необходимость внедрения камер хранения электронных доказательств, описать их ключевые функции и требования, нормативно-правовой и технический контексты. Кроме того, в статье описываются ключевые требования по обеспечению безопасности хранения электронных доказательств и подходы к построению соответствующих систем, а также практические рекомендации по внедрению и интеграции в существующие процессы. Без обеспечения надлежащих условий и безопасности для хранения доказательств риск их утраты, повреждения, подмены или нелегального доступа существенно возрастает. В условиях, когда цифровая трансформация становится главным трендом государственного управления, наличие камер хранения электронных доказательств превращается в показатель цифровой обеспеченности и технологической состоятельности правоохранительной и судебной системы. Подчеркивается, что внедрение камеры хранения электронных доказательств в перспективе будет являться неотъемлемым элементом электронного правосудия.

По тексту статьи Российская Федерация сокращенно указывается – РФ.

Ключевые слова: электронные доказательства, электронная цифровая информация, камера хранения электронных доказательств, кибербезопасность, электронное правосудие, условия хранения электронных доказательств, Единый репозиторий электронных доказательств

THE POTENTIAL FOR INTRODUCING AN ELECTRONIC EVIDENCE STORAGE CHAMBER

Smushkin A.B.¹,

Candidate of Legal Sciences, Associate Professor,
e-mail: skif32@yandex.ru

Vekhov V.B.^{2,3},

Doctor of Legal Sciences, Professor, Academician of the Russian Academy of Natural Sciences (RAE),
Honored Worker of Science and Education of the RAE,
e-mail: v-vehov@mail.ru

¹Federal State Budgetary Educational Institution of Higher Education Saratov State Law Academy, Saratov, Russia

²Bauman Moscow State Technical University (national research university), Moscow, Russia

³The Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia

The article addresses the critical need to create a specialized facility for the long-term storage and verification of electronic evidence. The author examines the transition from a “physical” understanding of material

evidence to a “logical” one. This article aims to comprehensively substantiate the need to implement electronic evidence storage chambers, to describe their key functions and requirements, along with the regulatory and technical contexts. In addition, the article describes the key requirements for ensuring the security of electronic evidence storage and approaches to creating the relevant systems, and offers practical recommendations for implementation and integration into existing processes. Without ensuring proper conditions and security for the storage of evidence, the risk of its loss, damage, substitution, or illegal access increases significantly. As digital transformation becomes the main trend in public administration, the presence of electronic evidence storage chambers becomes an indicator of the digital readiness and technological sophistication of the law enforcement and judicial systems. The article emphasizes that the introduction of electronic evidence storage chambers will be an integral element of electronic justice.

In the text of the article, the Russian Federation is abbreviated as RF.

Keywords: electronic evidence, digital information, electronic evidence storage chamber, cybersecurity, electronic justice, electronic evidence storage conditions, Unified Repository of Electronic Evidence

Введение

Современный мир становится все более гибридным – аналогово-цифровым. Объемы информации, курсирующей в киберпространстве, растут по экспоненте. Цифровая трансформация всех сфер общественной жизни привела к тому, что значительная часть преступной активности оставляет электронные следы: от переписок в мессенджерах и логов серверов до данных устройств интернета вещей и облачных сервисов. В сфере уголовного судопроизводства также все большую роль начинают играть доказательства, полученные с помощью информационно-технологических устройств или извлеченные из них. Не вдаваясь в дискуссию, отметим лишь, что мы полагаем наименование «электронные доказательства» оптимальным для данных информационных объектов.

Основная часть

Неотъемлемым элементом жизненного цикла любых доказательств (последовательности этапов, через которые проходит доказательство с момента возникновения в виде следов в киберпространстве до момента их использования и уничтожения) является их хранение. По общему принципу, предусмотренному ч. 1 ст. 82 УПК РФ, вещественные доказательства должны храниться при уголовном деле до вступления приговора в законную силу либо до истечения срока обжалования постановления или определения о прекращении уголовного дела и передаваться вместе с уголовным делом, за исключением случаев, предусмотренных настоящей статьей. В случае, когда спор о праве на имущество, являющееся вещественным доказательством, подлежит разрешению в порядке гражданского судопроизводства, вещественное доказательство хранится до вступления в силу решения суда.

Электронное доказательство требует определённого режима хранения. При этом следует учитывать сложившийся в российской процессуальной парадигме примат изъятия электронных носителей информации перед копированием самой информации – в первую очередь нормативное регулирование направлено на изъятие носителей, а не информации. Согласно ч. 5 ст. 82 УПК РФ электронные носители информации а) хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации; б) возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания.

Возможность возврата электронных носителей информации или копирования информации для ее возврата владельцу определяется следователем по смыслу рассматриваемой нормы. Таким образом, при необходимости, электронная информация, которая может послужить доказательством по делу, размещенная на материальном объекте – носителе, может храниться и на более поздних этапах.

В настоящее время электронные доказательства хранятся в обычных комнатах хранения вещественных доказательств, что защищает их практически только от физического повреждения и похищения. Это может быть оправдано в ситуации примата носителя информации над самой информацией, но при повышении значимости электронной доказательственной информации необходимо обращать внимание на особые условия её хранения. Традиционные подходы к хранению доказательств, приспособленные под физические предметы, не всегда удовлетворяют требованиям цифрового века.

Нам представляется, что надлежащие условия хранения электронной цифровой информации может обеспечить концепция камеры хранения электронных доказательств. Концепция камеры хранения цифровых доказательств предполагает создание выделенного пространства для хранения и управления цифровыми объектами, сопровождаемого механизмами контроля целостности (хеши, цепочки несменяемости), электронной подписью и аудиторной логикой. Камера хранения электронных доказательств – это целостная система, объединяющая физическую защиту, криптографическую защиту данных, контроль доступа, журналирование, автоматизацию процессов получения, сохранения и последующего использования доказательств.

В первую очередь, для реализации концепции камеры хранения электронных доказательств нужны безопасные помещения с контролем доступа и физической защитой (турникетами, идентификацией пользователей, видеонаблюдением и т.д.), а также защищенная зона хранения носителей и устройств на которой непосредственно размещается Единый репозиторий электронных доказательств: централизованный (или распределенный) цифровой архив с поддержкой хранения в виде копий-образов, версионирования и подписи.

Программный уровень камеры хранения электронных доказательств должен включать:

- систему приёма и регистрации;
- систему безопасного хранения;
- систему контроля целостности;
- систему разграничения доступа;
- систему выдачи.

Для хранения электронных доказательств предъявляются требования, касающиеся, во-первых, специфических условий материального плана для обеспечения безопасности носителя и информации на нём, а во-вторых, специфические требования кибербезопасности.

В материальную безопасность входит обеспечение физической неприкосновенности доказательств и климат-контроля: обеспечение соответствующей температурной обстановки, невысокого уровня влажности воздуха, а также обеспечение электромагнитной безопасности и отсутствие опасности от перепадов напряжения электричества в сети. Камеры хранения электронных вещественных доказательств должны быть оборудованы сетевыми фильтрами и источниками бесперебойного питания. Если для обеспечения оптимальных влажности и температуры в помещении никаких дополнительных условий не предъявляется, носители могут храниться в обычных камерах хранения вещественных доказательств, то для повышения безопасности от скачков напряжения хранение осуществляется в выключенном упакованном состоянии. Хранение особо важных носителей может осуществляться в запечатанных сейфах, сертифицированных по стандартам прочности и пожаробезопасности.

В целях же электромагнитной безопасности необходимо ставить вопрос об экранировании помещения от возможного скачка магнитного поля. Данный метод может использоваться злоумышленниками путем создания мощного электромагнитного импульса поблизости от камеры хранения вещественных доказательств. Для экранирования необходимо использование материала аналогичного применяемому в мешке Фарадея для транспортировки электронных вещественных доказательств. Указанный метод будет также способствовать пресечению попыток дистанционной модификации или стирания информации на включенном электронном устройстве.

В некоторых случаях, как предлагает Х.Х. Рамалданов, может возникнуть необходимость организации дистанционного доступа к электронным доказательствам (к информации). В этой ситуации копия информационного объекта (образ) должны храниться на устройстве, подключённом к сети. По схеме, предлагаемой Х.Х. Рамалдановым, «файлы будут отправлены на сервер ЦИТТУ¹ (как, впрочем, и любого другого

¹ Центральное информационно-техническое таможенное управление.

органа дознания или следствия – *прим. А.С.*). С момента сохранения файлов на сервере они официально приобретут статус цифровых доказательств. Каждому файлу автоматически будет присвоен уникальный номер. Этот номер и будет индивидуальным идентификатором цифрового доказательства, по этому номеру, как по интернет-ссылке, можно будет переходить на сервер ЦИТТУ и обращаться к конкретному файлу» [1, с. 180]. Кроме того, при реализации предлагаемой нами концепции единой экосистемы уголовного судопроизводства [2] при необходимости изучения и ознакомления с данными доказательствами надзирающий прокурор и судебные органы также могут получить оперативный доступ к информации.

В целях обеспечения кибербезопасности, как мы уже отмечали, используется ряд методов типа брандмауэра, антивирусных программных комплексов и т.д. Исследования также показывают эффективность применения нейросетевых технологий для борьбы со зловредными программами. Как верно отметил Д.В. Бахтеев: «Работа искусственной нейронной сети основана на интеллектуальном эвристическом анализе данных, который гораздо более эффективен, чем методы математической статистики, используемые в большинстве криминалистических программных комплексов. В этом отношении искусственные нейронные сети гораздо ближе к человеческому мозгу, поскольку способны выявлять скрытые, неочевидные связи и закономерности» [3, с. 49].

Некоторые учёные настаивают на необходимости активизации LLM систем в области кибербезопасности. Так, например, в некоторых зарубежных публикациях предлагается «использовать систему HuntGPT, которая интегрирует методы машинного обучения для обнаружения аномалий и LLM для поиска угроз» [4].

К аппаратно-программным средствам относятся:

- аппаратная защита и специализированные шлюзы;
- сертификаты электронной подписи;
- средства идентификации и аутентификации пользователей;
- межсетевые экраны-брандмауэры;
- системы обнаружения вторжений;
- средства резервного копирования;
- логическое разделение сети на сегменты и построение изолированных сетей для обращения конфиденциальной информации;
- криптографические средства защиты информации;
- использование новых технологий блокчейна или квантовых технологий;
- многие другие, а также их вариации и комбинации².

Как мы уже отмечали ранее, «к основным мерам обеспечения кибербезопасности относятся: надежные сложные пароли, двухфакторная аутентификация, регулярная проверка учетной записи, своевременное обновление программных средств защиты, мониторинг сетевой активности, обучение и самообразование, регулярное резервное копирование, шифрование данных, безопасность при онлайн-покупках и посещении подозрительных сайтов, осторожность при использовании общественных Wi-Fi сетей, разработки использования стратегий ограничения доступа и контроля за доступом, проверка используемых электронных носителей информации, сотрудничество с организациями, созданными для противодействия и расследования компьютерных инцидентов» [5, с. 120].

Непосредственно к современным техническим мерам обеспечения кибербезопасности можно отнести следующие интеллектуальные методы:

- методы интеллектуальной идентификации пользователей;
- предотвращения вирусных и других атак;
- выявления атак и проникновений;
- ситуационного анализа состояния информационной безопасности;
- новые методы криптографической защиты, основанные на нейросетевых технологиях [6, с. 26].

Важно обеспечить единый интерфейс загрузки файлов, проверки целостности после попадания в систему и возможности повторной проверки материалов до их окончательного признания в рамках дела. Образы хранятся в изолированной от сети системе.

² Анна Видулина. Защита систем электронного документооборота // WiseAdvice. IC интегратор [Электронный ресурс]. – URL: <https://wiseadvice-it.ru/o-kompanii/blog/articles/zashhita-sistem-edo/?ysclid=lxir3lvif950544027> (дата обращения 17.01.2026).

Кроме того, высокий уровень безопасности позволит обеспечить использование облачных и блокчейн-технологий.

При использовании облачных технологий, информация дробится на отдельные элементы, каждый из которых хранится на отдельном устройстве, входящем в состав облачного сервиса, что будет требовать повышенных усилий для взлома всей цепочки облачных серверов, на которых хранится информация, поскольку получение отдельных изолированных частей информации не даст возможности изучить даже содержимое этой отдельной части.

Следует также поднять вопрос об организации ведомственного облачного провайдера, поскольку ведомственные программы рекомендуют перенесение части информации в облачный режим в облачные сервисы. Как отметил Х.Х. Рамалданов, «применяя миграцию файлов и их дублирование на серверах правоохранительных органов в качестве одного из наиболее действенных способов повышения устойчивости информации можно получить автономию цифровых доказательств от внешних факторов, негативно влияющих на их устойчивость» [7, с. 107].

Использование блокчейн-технологий связано с тем, что каждый новый элемент цепочки содержит в себе информацию о предыдущих элементах и всех транзакциях. Блокчейн считается практически невозможным к взлому извне. Даже при проникновении злоумышленника каким-то образом внутрь цепочки, например с помощью коррумпированного сотрудника, без обладания влиянием на 51 % узлов цепочки любая модификация информации будет невозможной.

Аналогичное мнение о необходимости применения технологий блокчейн высказывал и Л.В. Бертовский, уточняя, что: «К записям могут получить доступ только следователь, у которого есть один закрытый ключ, и руководитель, у которого есть другой. Затем к этой информации получают доступ только те, кому один из этих пользователей предоставит свой закрытый ключ. Например, судебно-экспертному учреждению, в случае назначения экспертизы, или, если судебная экспертиза производится в порядке ч. 4 ст. 199 УПК РФ вне экспертного учреждения, эксперту, или суду, в случае возникновения необходимости в осуществлении судебно-контрольных действий в стадии предварительного расследования, а также прокурору, при осуществлении надзора, или адвокату (которому предоставлено право знакомиться с протоколами следственных действий, проводимых с участием его подзащитного) в процессе осуществления защиты подозреваемого или обвиняемого, или другим участникам уголовного процесса. Вышеуказанные управомоченные (кому предоставлено право работать с файлами) лица видят все содержимое папки с уголовным делом (никаких скрытых файлов), ее можно быстро просмотреть: кто, когда и в какие подпапки загружал документы. Но при этом у всех разный уровень доступа к данным файлам» [8, с. 229].

Кроме того, необходимо задаться вопросом объёма хранилищ. Если для хранения обычных вещественных доказательств можно предположить потребные материальные объёмы помещения, то хранение электронных вещественных доказательств будет требовать соответствующих виртуальных объёмов электронных носителей. В настоящее время средний домашний компьютер по ёмкости носителей может достигать 1 ТБ и более. Используемые в коммерческой деятельности информационно-технологические устройства могут существенно превышать этот показатель. С учётом того, что проведённое нами исследование показало использование принципа изъятия всего устройства или копирования всей информации, представляется, что в комнате хранения электронных вещественных доказательств носители должны быть кратно больших объёмов. Для повышения безопасности эффективности и быстрого действия рекомендуется использовать RAID-массивы для хранения информации. При этом непосредственная архитектура RAID-массива при одних конфигурациях может способствовать обеспечению сохранности информации путем ее дублирования, а при других – физически расширять емкость логического диска.

Заключение

Таким образом, представляется, что использование камеры хранения электронных доказательств может существенно повысить их безопасность и эффективность использования. Камера хранения элек-

тронных доказательств – это специализированная информационно-техническая и организационная система, предназначенная для приёма, безопасного хранения, мониторинга, управления доступом и выдачей электронных доказательств с обеспечением их юридической пригодности, объединяющая технические средства, процессы и кадровые практики, и направленная на обеспечение законной и надёжной работы с цифровыми артефактами.

Для материальных носителей электронной цифровой информации наиболее важным аспектом является обеспечение физической сохранности. Для самой информации – возможность ее использования. Представляется, что сети (репозитории, озера данных и т.д.) хранения электронной доказательственной информации должны быть изолированы от сети Интернет. При этом важна возможность интеграции предлагаемой камеры хранения электронных доказательств с существующими цифровыми платформами правоохранительных органов, а также перспективными экосистемами предварительного расследования.

Для оптимизации процесса внедрения камер хранения электронных доказательств возможна их пилотная пробация в конкретном ведомстве (например, ФТС) или в ключевых подразделениях (например, в центральном аппарате СКР).

На стратегическом уровне камеры хранения электронных доказательств – это инфраструктурный проект, формирующий основу для следующего шага: «электронного уголовного дела», где весь материал, от протокола осмотра места происшествия до приговора, будет существовать в едином защищённом цифровом контуре. Это путь к прозрачности, эффективности и технологическому суверенитету правовой системы.

Список литературы

1. Рамалданов, Х.Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений: дис. ... канд. юрид. наук: специальность: 5.1.4 «Уголовно-правовые науки» / Х.Х. Рамалданов; АНО ВО «Российский новый университет». – Москва, 2024. – 244 с.
2. Вехов, В.Б. К вопросу о создании единой цифровой экосистемы уголовного судопроизводства / В.Б. Вехов, М.В. Савельева, А.Б. Смушкин // Расследование преступлений: проблемы и пути их решения. – 2025. – № 2(48). – С. 82–94.
3. Бахтеев, Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования / Д.В. Бахтеев // Российское право: образование, практика, наука. – 2018. – №2 (104). – С. 43–49.
4. Kulkarni, M.S. A Proactive Approach to Advanced Cyber Threat Hunting / M.S. Kulkarni, A.D. Hegadi, C.C. Narayan // Proceedings of the 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS). – 2023. – P. 1–6.
5. Смушкин, А.Б. Кибербезопасность: понятие, структура, механизм правового обеспечения / А.Б. Смушкин // Правоприменение. – 2025. – Т. 9, №. 3. – С. 114–123.
6. Безкоровайный, М.М. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 22–27.
7. Рамалданов, Х.Х. Проблемы использования и хранения цифровых доказательств в доказывании в уголовном процессе / Х.Х. Рамалданов // Вестник Казанского юридического института МВД России. – 2023. – № 2. – С. 105–111.
8. Бертовский, Л.В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства / Л.В. Бертовский // Проблемы экономики и юридической практики. – 2017. – № 6. – С. 226–230.

References

1. Ramaldanov, H.H. The process of proving criminal cases in the context of total digitalization of public relations: Dissertation ... Candidate of Law: Specialty: 5.1.4 “Criminal Law Sciences” / H.H. Ramaldanov; ANO HE “Russian New University”. – Moscow, 2024. – 244 p.
2. Vekhov, V.B. On the issue of creating a unified digital ecosystem of criminal proceedings / V.B. Vekhov, M.V. Saveleyeva, A.B. Smushkin // Investigation of crimes: problems and solutions. – 2025. – No. 2 (48). – P. 82–94.
3. Bakhteev, D.V. Artificial intelligence in criminalistics: state and prospects of use / D.V. Bakhteev // Russian law: education, practice, science. – 2018. – No. 2 (104). – P. 43–49.

4. *Kulkarni, M.S.* A Proactive Approach to Advanced Cyber Threat Hunting / M.S. Kulkarni, A.D. Hegadi, C.C. Narayan // Proceedings of the 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS). – 2023. – P. 1–6.
5. *Smushkin, A.B.* Cybersecurity: concept, structure, mechanism legal support / A.B. Smushkin // Law enforcement. – 2025. – Vol. 9, No. 3. – P. 114–123.
6. *Bezkorovayny, M.M.* Cybersecurity – approaches to the definition of the concept / M.M. Bezkorovayny, A.L. Tatuzov // Cybersecurity issues. – 2014. – No. 1 (2). – P. 22–27.
7. *Ramaldanov, H.H.* Problems of using and storing digital evidence in proving in criminal proceedings / H.H. Ramaldanov // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. – 2023. – No. 2. – P. 105–111.
8. *Bertovsky, L.V.* Blockchain technology in criminal proceedings as an element of digital legal proceedings / L.V. Bertovsky // Problems of economics and legal practice. – 2017. – No. 6. – P. 226–230.

Статья поступила в редакцию: 20.01.2026

Received: 20.01.2026

Статья принята к публикации: 01.06.2026

Accepted: 01.06.2026