DOI: 10.17803/1994-1471.2025.173.4.146-156

А. Б. Смушкин*

Информационная безопасность электронного документооборота в уголовном судопроизводстве

Аннотация. В статье анализируются состояние и перспективы обеспечения безопасности электронного документооборота в рамках уголовного судопроизводства в контексте цифровой трансформации правоохранительных органов. В первую очередь охарактеризованы угрозы безопасности информации. Определены нормативные основы обеспечения безопасности, уделено внимание организационным вопросам. Констатируется, что организационные средства обеспечения безопасности включают определение и нормативное закрепление круга лиц, допущенных к работе с электронным документооборотом, недопущение воздействия на информацию иных лиц и явлений. Подробно рассматриваются технические средства обеспечения безопасности электронного документооборота, включая аппаратно-программные, аппаратные и криптографические средства защиты. В качестве перспектив ближайшего времени выделены: более активное использование облачных сервисов и технологии блокчейн для сохранности информации, а также перспективных квантовых технологий криптографии и квантовой передачи информации. Автор приходит к выводу, что только в системе все меры обеспечения безопасности электронного документооборота в уголовном судопроизводстве могут дать синергетический эффект, гарантирующий безопасность информации.

Ключевые слова: электронное правосудие; электронный документооборот; защита электронной информации; уголовное судопроизводство; технические методы защиты информации; идентификация пользователя; аутентификация пользователя; верификация информации; блокчейн; облачные сервисы; квантовые методы защиты информации; ГАС «Правосудие».

Для цитирования: *Смушкин А. Б.* Информационная безопасность электронного документооборота в уголовном судопроизводстве // Актуальные проблемы российского права. — 2025. — Т. 20. — № 4. — С. 146–156. — DOI: 10.17803/1994-1471.2025.173.4.146-156.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/.

Information Security of Electronic Document Flow in Criminal Proceedings

Alexander B. Smushkin, Leading Researcher, Project Office of Scientific Programs and Research, Associate Professor, Department of Criminalistics, Saratov State Law Academy, Saratov, Russian Federation
skif32@yandex.ru

Abstract. The paper examines the state and prospects of ensuring the security of electronic document flow in criminal proceedings in the context of the digital transformation of law enforcement agencies. First, threats to

* *Смушкин Александр Борисович*, ведущий научный сотрудник проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии Чернышевского ул., д. 104, г. Саратов, Российская Федерация, 410028
skif32@yandex.ru

information security are characterized. The regulatory framework for ensuring safety has been defined, and attention has been given to organizational issues. It is stated that organizational means of ensuring security include the definition and regulatory consolidation of the circle of persons allowed to work with electronic document flow, as well as the prevention of the impact on information by other persons and phenomena. The technical means of ensuring the security of electronic document management are examined in detail, including hardware and software, hardware and cryptographic means of protection. The following are highlighted as prospects for the near future: more active use of cloud services and blockchain technology for information security, as well as promising quantum technologies of cryptography and quantum information transfer. As a conclusion, it is stated that only in the system all measures to ensure the security of electronic document flow in criminal proceedings can provide a synergistic effect that guarantees the security of information.
Keywords: electronic justice; electronic document flow; protection of electronic information; criminal proceedings; technical methods of information protection; user identification; user authentication; information verification; blockchain; cloud services; quantum methods of information protection; GAS «Pravosudie».
***Cite* as:** Smushkin AB. Information Security of Electronic Document Flow in Criminal Proceedings. *Aktual'nye problemy rossijskogo prava*. 2025;20(4):146-156. (In Russ.). DOI: 10.17803/1994-1471.2025.173.4.146-156.

Acknowledgements. The study was supported by the Russian Science Foundation, grant No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

Введение

В условиях активной цифровой трансформации органов уголовного судопроизводства особое значение приобретает обеспечение информационной безопасности электронного документооборота в уголовном судопроизводстве. В процессе расследования и осуществления правосудия в системы электронного документооборота попадает большой объем информации, составляющей тайну следствия, тайну личной жизни участников уголовного судопроизводства и иные охраняемые законом тайны. Цифровизации уголовного судопроизводства и вопросам электронного документооборота в уголовном судопроизводстве посвящено большое количество научных трудов. Однако результативность электронного документооборота обуславливается в значительной мере его информационной безопасностью.

Президент РФ обозначил информационную безопасность в качестве задачи, необходимой для достижения национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы»[1].

Угрозы информационной безопасности

В наиболее общем виде среди угроз электронному документообороту в уголовном судопроизводстве можно выделить внешние и внутренние.

К внешним угрозам относятся естественные и искусственные угрозы, а к внутренним — умышленные или неумышленные. Естественные угрозы практически не зависят от пользователей (пожар, наводнение, землетрясение, приведшие к уничтожению или сильному повреждению электронных носителей информации). Искусственные угрозы — прямые хакерские атаки, взломы, вирусы.

Внутренние угрозы возникают вследствие действий (бездействия) сотрудников правоохранительного органа. Умышленными угрозами являются прямая преднамеренная передача информации, полное или частичное снятие защит-

[1] П. «л» ч. 8 Указа Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Официальный сайт Президента РФ. URL: http://www.kremlin.ru/events/president/news/63728 (дата обращения: 27.05.2024).

ных мер. Неумышленные возникают вследствие халатного отношения к своим обязанностям или режиму защиты информации, недостатка знаний об использовании мер безопасности или неосторожности.

А. Г. Анацкая выделяет следующие угрозы информационной безопасности для используемых в уголовном судопроизводстве систем документооборота:

— «угроза целостности;
— угроза конфиденциальности;
— угроза доступности;
— угроза работоспособности системы;
— невозможность доказательства авторства»[2].

Правовая основа обеспечения информационной безопасности

В первую очередь необходимо отметить Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3], который в качестве целей защиты указывает триаду: защита информации, обеспечение ее конфиденциальности и обеспечение доступа к ней. Достижение этих целей возможно с помощью комплекса правовых, организационных и технических мер.

Однако как же реализуются данные меры в уголовном судопроизводстве? К правовым мерам обеспечения информационной безопасности электронного документооборота в уголовном судопроизводстве относятся нормативные акты, регламентирующие уголовную, дисциплинарную, административную или гражданско-правовую ответственность, а также использование инструментов защиты информации.

С 1 января 2017 г. в УПК РФ действует статья 474.1 «Порядок использования электронных документов в уголовном судопроизводстве»[4]. Данной нормой установлены ситуации подписания электронных документов в уголовном судопроизводстве разными видами электронной подписи. Использование электронных документов на досудебном этапе уголовного судопроизводства началось с 2024 г.[5]

Усиленная квалифицированная электронная подпись предусмотрена для наиболее важных документов, влияющих на осуществление судопроизводства. Простой электронной подписью подписываются менее важные документы.

Использование электронной подписи в рамках уголовного судопроизводства осуществляется в рамках соответствующих указанных выше норм УПК РФ, а также Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»[6]. Электронная подпись — одна из важнейших криптографических мер защиты информации в уголовном судопроизводстве (подробнее характеристики различных видов электронной подписи рассмотрим далее).

Важным элементом обеспечения безопасности электронной информации в рамках уголовного судопроизводства является защита критической информационной инфраструктуры. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[7] раскрывает механизм обнаружения, преду-

[2] *Анацкая А. Г.* Защита электронного документооборота : учеб. пособие. Омск : СибАДИ, 2019. Сходной позиции придерживаются и некоторые другие авторы. См., например: *Ушаков Н. О., Сибикина И. В., Космачева И. М.* Информационная безопасность в системах электронного документооборота // Техническая эксплуатация водного транспорта: проблемы и пути развития. 2021. № 1. С. 70–71.

[3] СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[4] Федеральный закон от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» // СЗ РФ. 2016. № 26 (ч. I). Ст. 3889.

[5] Федеральный закон от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СЗ РФ. 2024. № 1 (ч. I). Ст. 53.

[6] СЗ РФ. 2011. № 15. Ст. 2036.

[7] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

преждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты с критической информационной инфраструктурой, а также закрепляет создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Обработка персональных данных в ходе электронного документооборота в рамках уголовного судопроизводства регулируется в том числе и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»[8]. Закон подробно рассматривает меры обеспечения безопасности персональных данных.

В настоящее время обеспечением безопасности государственных информационных систем занимается Центр информационной безопасности Федеральной службы безопасности. Нормативными актами ФСБ регламентированы некоторые вопросы в данной сфере. Так, приказом ФСБ РФ от 09.02.2005 № 66 утверждено Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации[9]. Требования к средствам электронной подписи и Требования к средствам удостоверяющего центра утверждены приказом ФСБ РФ от 27.12.2011 № 796[10].

Организационные средства обеспечения безопасности электронного документооборота в уголовном судопроизводстве

Организационные средства обеспечения безопасности включают определение и нормативное закрепление круга лиц, допущенных к работе с электронным документооборотом, а также недопущение воздействия на информацию иных лиц и явлений.

Среди организационных средств можно выделить:

— надлежащий учет и хранение ключей шифрования и электронной подписи;

— эксплуатацию компетентными обученными сотрудниками ключей шифрования и электронной подписи в соответствии с разработанным порядком;

— разграничение прав доступа;

— ведение строгого учета доступа сотрудников к информации ограниченного распространения;

— тщательную идентификацию и аутентификацию пользователей, осуществляемую в дистанционном режиме, а также верификацию информации;

— ограничение физического доступа посторонних в помещение, в котором расположено компьютерное оборудование, предназначенное для обеспечения функционирования электронного документооборота и хранения информации;

— обеспечение отказоустойчивости и помехоустойчивости оборудования, бесперебойного электроснабжения, экранирования электромагнитных и иных воздействий;

— контроль подрядчиков, занимающихся обеспечением функционирования и обновления, технической поддержкой электронного документооборота в уголовном судопроизводстве;

— импортозамещение и «приземление» персональной информации.

Современные системы электронного документооборота позволяют отслеживать маршрут любого документа и действия любого должностного лица, а также ограничивать доступ к

[8] Ч. 2 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 06.02.2023) // Российская газета. 2006. 29 июля. № 165.

[9] Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» // Российская газета. 2005. 19 марта. № 55.

[10] Приказ ФСБ РФ от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2012. 16 апреля. № 16.

документам. Право на доступ к данным могут получать на различных этапах судопроизводства разные лица в разном объеме. Так, уже достаточно широко распространены варианты ознакомления обвиняемого с обвинительным заключением в электронном виде.

И. Иванов отмечает, что для электронного правосудия оптимальным может быть следующее: «1) децентрализация; 2) одноранговая структура; 3) асимметричный способ шифрования; 4) обязательное государственное регулирование и контроль»[11].

Аппаратно-программные и иные технические средства обеспечения безопасности электронного документооборота

Технические средства обеспечения безопасности электронного документооборота можно условно разделить на аппаратные, аппаратно-программные, криптографические и иные технические.

Как отмечает А. О. Калашников, «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»[12].

А. Викулина дополнила перечень, указав следующие меры:

— «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 комбинации»[13].

Аппаратные средства защиты представляют собой различные электронные, электромеханические, технические средства, которые аппаратным путем решают вопросы защиты информации. К таковым можно условно отнести источники бесперебойного питания, сетевые фильтры и иное оборудование, встроенные программные средства защиты.

В целях обеспечения безопасности данных в электронном документообороте используется отечественное лицензионное антивирусное программное обеспечение.

Установление личности участника судопроизводства, его аутентификация и верификация в дистанционном режиме вполне возможны. Для идентификации участника судопроизводства существует несколько вариантов:

1) использование учетных записей лиц на ведомственных порталах и цифровых платформах;

2) идентификация и аутентификация лиц через учетные записи портала «Госуслуги»;

3) разработка единой экосистемы уголовного судопроизводства с объединением действующих ведомственных платформ и иных банков данных в модульной архитектуре либо путем соединения шлюзами.

Как отметили О. А. Зайцев и П. С. Пастухов, «при проведении… следственных действий потребуются не только комплекс мер, указанных в законе, но и информационно-технологические средства, обеспечивающие идентификацию лица без его личного присутствия (единая система идентификации и аутентификации; единая информационная система персональных дан-

[11] *Иванов И.* Оптимизация делопроизводства в суде с учетом внедрения электронного правосудия // Закон.ру. URL: https://zakon.ru/blog/2021/11/10/optimizaciya_deloproizvodstva_v_sude_s_uchyotom_vnedreniya_elektronnogo_pravosudiya#footnote10back (дата обращения: 08.07.2024).

[12] *Калашников А. О.* Модели и методы организационного управления информационными рисками корпораций : дис. … д-ра техн. наук. М., 2011. С. 37.

[13] *Викулина А.* Защита систем электронного документооборота // WiseAdvice. Интегратор 1С. URL: https://wiseadvice-it.ru/o-kompanii/blog/articles/zashhita-sistem-edo/?ysclid=lxir3lvif950544027 (дата обращения: 08.07.2024).

ных, обеспечивающая обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным)»[14].

Оптимальным представляется использование многофакторной идентификации и аутентификации лица, в том числе с распознаванием по биометрическим показателям, а также применение разработок в области идентификации лица по клавиатурному почерку[15].

Д. А. Степаненко и А. А. Рудых в своей публикации достаточно подробно разработали цифровые решения вопросов идентификации и аутентификации пользователей[16].

Межсетевые экраны — это аппаратно-программные средства, осуществляющие фильтрацию трафика сетевых пакетов. При этом параметры фильтрации могут быть установлены администратором сети заранее.

Системы предотвращения вторжений предназначены для обнаружения, блокирования и предотвращения попыток несанкционированного доступа.

Криптографические системы дифференцируются:

— на симметричные, в которых для шифрования и дешифровки используется один и тот же ключ;

— криптосистемы с открытым ключом: для шифрования используется ключ, находящийся в открытом доступе, а для дешифровки — ключ, известный только получателю сообщения;

— управление ключами — процесс обработки информации, включающий составление и распределение ключей между пользователями;

— электронную подпись.

Использование электронных подписей в различных сферах, включая уголовное судопроизводство, определено Законом «Об электронной подписи». Согласно п. 1 ст. 2 данного Закона, электронная подпись — это «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию». Электронная подпись может быть простой и усиленной. Усиленная, в свою очередь, бывает неквалифицированной и квалифицированной.

Простая подпись в уголовном судопроизводстве используется в строго установленных законом случаях для подписания документов, не влияющих кардинально на процесс расследования и осуществления судопроизводства на судебной стадии (ст. 474.1–474.2 УПК РФ). Простая электронная подпись заключается в подтверждении факта формирования подписи простой парольной системой.

Остальные электронные документы в уголовном судопроизводстве должны быть подписаны

---

[14] *Зайцев О. А.*, *Пастухов П. С.* Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 304.

Аналогичной позиции придерживается и М. А. Юркевич. См.: *Юркевич М. А.* Применение судом видеотехнологий в уголовном судопроизводстве : дис. … канд. юрид. наук. М., 2021. С. 167.

[15] Криминалистическое значение индивидуально-психологических особенностей личности на характеристики изготовления электронного документа / Е. С. Гольдшмидт, Р. Г. Драпезо, В. Н. Шелестюков [и др.] // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 6 (14). С. 65–72 ; *Перегудов А. В.* Анализ клавиатурного почерка. Способы его применения // Интерактивная наука. 2018. № 6 (28). С. 59–60 ; *Протасевич А. А.*, *Фойгель Е. И.* О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 471–480.

[16] *Степаненко Д. А.*, *Рудых А. А.* К вопросу об использовании механизма удаленной идентификации и аутентификации в правоохранительной деятельности // Технологии XXI века в юриспруденции : материалы Третьей международной научно-практической конференции (Екатеринбург, 21 мая 2021 г.) / под ред. Д. В. Бахтеева. Екатеринбург : Уральский государственный юридический университет, 2021. С. 318–326.

усиленной квалифицированной электронной подписью.

Согласно ч. 3–5 ст. 5 Закона «Об электронной подписи», усиленной квалифицированной электронной подписью является электронная подпись, которая удовлетворяет следующим требованиям:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи;

5) ключ проверки электронной подписи указан в квалифицированном сертификате;

6) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Законом.

При использовании усиленной квалифицированной электронной подписи изменение информации невозможно без нарушения целостности системы, что обеспечивает неизменность информации в подписанных электронных документах и безопасность самого электронного документооборота в уголовном судопроизводстве.

Отдельно сто́ит сказать об использовании хеш-сумм для верификации информации. Хеш-сумма представляет собой формулу, основанную на определенном алгоритме. При этом разные файлы различаются по данным контрольным суммам, а контрольные суммы оригинального файла идентичны, что дает возможность дифференциации разных файлов и, соответственно, идентификации конкретного. Существует много алгоритмов расчета контрольной суммы: MD5, CRC32, SHA-1, SHA-2, GOST, GOST-GRYPTO и др. Следовательно, указание контрольной суммы файла с электронным документом, особенно нескольких вариантов, вычисленных по разным алгоритмам расчета, дает возможность сравнения с изучаемым документом для гарантии неизменности первоначального содержания электронного документа.

Перспективы обеспечения безопасности электронного документооборота в уголовном судопроизводстве

Относительно ближайших перспектив обеспечения безопасности информации в электронном документообороте следует отметить использование облачных сервисов, блокчкейна и квантовых технологий.

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, утвержденная распоряжением Правительства РФ от 01.11.2013 № 2036-р[17], в рамках приоритетных с точки зрения информационной безопасности направлений исследований и разработок в области информационных технологий называет стимулирование циркуляции данных облачных сервисов внутри страны. Облачные сервисы в основном используют принцип распределенного хранения информации. Информационный объект дробится на некоторое количество частей, хранится на разных облачных серверах и собирается в единый объект только по запросу. При этом возможно использование облачных серверов не только как дистанционных хранилищ информации, но и в иных форматах. Облачные сервисы в следственной деятельности могут использоваться как в качестве удаленного хранилища информации, доступ к которому возможен из любого места при наличии доступа к электронному устройству, подключенному к сети Интернет, так и в виде иных предлагаемых вариантов: «Инфраструктура как услуга» (Infrastructure as a Service, IaaS — предоставление фактически дистанционного хранилища информации или возможности дистанционного использования компьютера); «Платформа как услуга» (Platform as a Service, PaaS — предоставление целиком платформы для работы с

[17] СЗ РФ. 2013. № 46. Ст. 5954.

операционной системой, специализированным программным обеспечением, СУБД и т.д.); «Программное обеспечение как услуга» (Software as a Service, SaaS — предоставление конкретного программного продукта). Использование облачных сервисов обеспечит защиту от физического повреждения носителей электронной информации (иногда даже за счет избыточного дублирования восстановит потерянные сегменты), предоставит дополнительные объемы и мощности для электронного документооборота в уголовном судопроизводстве.

Первоначально термин «блокчейн» относился только к криптовалютам и осуществлению транзакций. Именно в таком значении он и знаком большинству пользователей. Однако по своей сути блокчейн — это реплицированная распределенная база (реестр) данных, надежность которой поддерживается всеми узлами сети путем подтверждения контрольных сумм. Впоследствии технология цепочек блоков была распространена и на иные взаимосвязанные информационные блоки[18].

При использовании блокчейн-технологии будут отсутствовать единый депозитарий и единая база, размещенная на определенных серверах. Информация будет распределена, а у каждого пользователя будет реестр информации. Каждая новая транзакция, произведенная с информацией, отражается во всей цепочке блоков. Посредством блокчейна информация через распределенные записи децентрализуется, последовательно хешируется (от англ. hashing — перемешивание, преобразование) и зашифровывается, что делает практически невозможным для злоумышленников ее выявление и осмысление[19]. На сегодняшний день блокчейн считается одной из самых устойчивых к взлому технологий. Поэтому представляется возможным использование ее для реализации электронного уголовного дела. Каждый документ (изначально существующий в электронном либо отсканированном виде) в рамках такого уголовного дела будет представлять собой отдельный блок в цепочке, выстроенной в определенном хронологическом порядке. Внешнее воздействие, взлом, несанкционированное изменение содержания блока будут практически полностью исключены. Пользователям может быть предоставлен доступ к отдельным документам, а также определен технически различный уровень доступа (ознакомление либо изменение). Аналогичное мнение о необходимости применения блокчейн-технологий 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 получат доступ только те, кому один из этих пользователей предоставит свой закрытый ключ. <…> …Управомоченные (кому предоставлено право работать с файлами) лица видят всё 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»[20].

Кроме того, направляемые участниками судопроизводства документы в рамках такого уголовного дела получат свое отражение в блоке, как и принятое по обращению решение с обязательной мотивировкой, что будет способствовать обеспечению соблюдения прав участников судопроизводства и препятствовать злоупотреблению правами следователя и суда.

Квантовые технологии защиты информации используют квантовое состояние фотонов для передачи информации с криптографической защитой, основанной не на математических методах, а на физике передачи информации в вакууме, волоконно-оптической связи или естественной среде. Риск перехвата квантовой информации нивелируется невозможностью измерить квантовую систему, не нарушив ее состояние.

---

[18] *Генкин А. С., Михеев А. А.* Блокчейн. Как это работает и что ждет нас завтра. М. : Альпина Паблишер, 2017.

[19] *Luff C.* Cybersecurity and the future of blockchain technology // URL: http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm (дата обращения: 08.07.2024).

[20] *Бертовский Л. В.* Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 229.

В плане уже применяемых систем обеспечения безопасности электронного документооборота в рамках уголовного судопроизводства можно привести в пример государственную автоматизированную систему «Правосудие». В рамках целей подсистемы информационной безопасности, являющейся элементом системы ГАС «Правосудие», можно назвать: обеспечение безопасности внутриведомственного взаимодействия; обеспечение безопасности доступа к электронной библиотеке, действующему законодательству, базам судебных решений и иной правоохранительной практики; предотвращение ущерба при использовании ГАС «Правосудие»; обеспечение безопасного использования и безопасного решения некоторых служебных задач в автоматизированном режиме.

ГАС «Правосудие» предусматривает три контура обращения информации: публичный (открытый) контур, ведомственный (закрытый) контур и защищенный контур, предназначенный для передачи информации, защищенной грифом «Секретно». При размещении информации в открытом контуре в целях обеспечения безопасности участников судопроизводства из актов удаляются персональные сведения и некоторые иные положения, которые содержат данные, составляющие государственную или другую охраняемую законом тайну.

Выводы

Подводя итог исследованию, можно отметить, что цифровизация уголовного судопроизводства в Российской Федерации достигла достаточно высокого уровня. При этом в рамках основных задач обеспечения надлежащего функционирования электронного правосудия и реализации концепции электронного уголовного дела выделяется обеспечение безопасности курсирования информации на различных стадиях уголовного судопроизводства. Именно безопасность информации в пределах цифровых платформ, электронного уголовного дела и электронного межведомственного взаимодействия служит гарантией реализации права граждан на судебную защиту. В настоящий момент обеспечение безопасности электронного документооборота имеет свойства системы, когда синергетический эффект надлежащей реализации всех мер защиты дает больше простой суммы элементов. При этом нельзя забывать о постоянном ускорении научно-технического прогресса и активном принятии криминальными структурами на вооружение любых новинок, способствующих достижению криминальных целей. Поэтому разработка мер защиты информации обязательно должна носить опережающий характер.

БИБЛИОГРАФИЯ

1. *Анацкая А. Г.* Защита электронного документооборота : учеб. пособие. — Омск : СибАДИ, 2019. — 87 с.
2. *Бертовский Л. В.* Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. — 2017. — № 6. — С. 226–230.
3. *Викулина А.* Защита систем электронного документооборота // WiseAdvice. Интегратор 1С. — URL: https://wiseadvice-it.ru/o-kompanii/blog/articles/zashhita-sistem-edo/?ysclid=lxir3lvif950544027 (дата обращения: 08.07.2024).
4. *Генкин А. С., Михеев А. А.* Блокчейн. Как это работает и что ждет нас завтра. — М. : Альпина Паблишер, 2017. — 592 с.
5. *Зайцев О. А.*, *Пастухов П. С.* Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. — 2022. — № 56. — С. 281–308.
6. *Иванов И.* Оптимизация делопроизводства в суде с учетом внедрения электронного правосудия // Закон.ру. — URL: https://zakon.ru/blog/2021/11/10/optimizaciya_deloproizvodstva_v_sude_s_uchyotom_vnedreniya_elektronnogo_pravosudiya#footnote10back (дата обращения: 08.07.2024).

7. *Калашников А. О.* Модели и методы организационного управления информационными рисками корпораций : дис. … д-ра техн. наук. — М., 2011. — 362 с.
8. Криминалистическое значение индивидуально-психологических особенностей личности на характеристики изготовления электронного документа / Е. С. Гольдшмидт, Р. Г. Драпезо, В. Н. Шелестюков [и др.] // Сибирские уголовно-процессуальные и криминалистические чтения. — 2016. — № 6 (14). — С. 65–72.
9. *Перегудов А. В.* Анализ клавиатурного почерка. Способы его применения // Интерактивная наука. — 2018. — № 6 (28). — С. 59–60.
10. *Протасевич А. А.*, *Фойгель Е. И.* О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 3. — С. 471–480.
11. *Степаненко Д. А.*, *Рудых А. А.* К вопросу об использовании механизма удаленной идентификации и аутентификации в правоохранительной деятельности // Технологии XXI века в юриспруденции : материалы Третьей международной научно-практической конференции (Екатеринбург, 21 мая 2021 г.) / под ред. Д. В. Бахтеева. — Екатеринбург : Уральский государственный юридический университет. — 2021. — С. 318–326.
12. *Ушаков Н. О.*, *Сибикина И. В.*, *Космачева И. М.* Информационная безопасность в системах электронного документооборота // Техническая эксплуатация водного транспорта: проблемы и пути развития. — 2021. — № 1. — С. 70–74.
13. *Юркевич М. А.* Применение судом видеотехнологий в уголовном судопроизводстве : дис. … канд. юрид. наук. — М., 2021.
14. *Luff C.* Cybersecurity and the future of blockchain technology // URL: http://www.gingermaypr.com/cybersecurity-blockchain-technology.html (дата обращения: 08.07.2024).

Материал поступил в редакцию 8 июля 2024 г.

REFERENCES (TRANSLITERATION)

1. Anatskaya A. G. Zashchita elektronnogo dokumentooborota: ucheb. posobie. — Omsk: SibADI, 2019. — 87 s.
2. Bertovskiy L. V. Tekhnologiya blokcheyna v ugolovnom protsesse kak element tsifrovogo sudoproizvodstva // Problemy ekonomiki i yuridicheskoy praktiki. — 2017. — № 6. — S. 226–230.
3. Vikulina A. Zashchita sistem elektronnogo dokumentooborota // WiseAdvice. Integrator 1S. — URL: https://wiseadvice-it.ru/o-kompanii/blog/articles/zashhita-sistem-edo/?ysclid=lxir3lvif950544027 (data obrashcheniya: 08.07.2024).
4. Genkin A. S., Mikheev A. A. Blokcheyn. Kak eto rabotaet i chto zhdet nas zavtra. — M.: Alpina Pablisher, 2017. — 592 s.
5. Zaytsev O. A., Pastukhov P. S. Tsifrovoy profil litsa kak element informatsionno-tekhnologicheskoy strategii rassledovaniya prestupleniy // Vestnik Permskogo universiteta. Yuridicheskie nauki. — 2022. — № 56. — S. 281–308.
6. Ivanov I. Optimizatsiya deloproizvodstva v sude s uchetom vnedreniya elektronnogo pravosudiya // Zakon.ru. — URL: https://zakon.ru/blog/2021/11/10/optimizaciya_deloproizvodstva_v_sude_s_uchyotom_vnedreniya_elektronnogo_pravosudiya#footnote10back (data obrashcheniya: 08.07.2024).
7. Kalashnikov A. O. Modeli i metody organizatsionnogo upravleniya informatsionnymi riskami korporatsiy: dis. … d-ra tekhn. nauk. — M., 2011. — 362 s.
8. Kriminalisticheskoe znachenie individualno-psikhologicheskikh osobennostey lichnosti na kharakteristiki izgotovleniya elektronnogo dokumenta / E. S. Goldshmidt, R. G. Drapezo, V. N. Shelestyukov [i dr.] // Sibirskie ugolovno-protsessualnye i kriminalisticheskie chteniya. — 2016. — № 6 (14). — S. 65–72.

9. Peregudov A. V. Analiz klaviaturnogo pocherka. Sposoby ego primeneniya // Interaktivnaya nauka. — 2018. — № 6 (28). — S. 59–60.
10. Protasevich A. A., Foygel E. I. O vozmozhnostyakh kriminalisticheskoy gabitoskopii pri realizatsii mer protivodeystviya sovremennoy kiberprestupnosti // Vserossiyskiy kriminologicheskiy zhurnal. — 2020. — T. 14. — № 3. — S. 471–480.
11. Stepanenko D. A., Rudykh A. A. K voprosu ob ispolzovanii mekhanizma udalennoy identifikatsii i autentifikatsii v pravookhranitelnoy deyatelnosti // Tekhnologii XXI veka v yurisprudentsii: materialy Tretey mezhdunarodnoy nauchno-prakticheskoy konferentsii (Ekaterinburg, 21 maya 2021 g.) / pod red. D. V. Bakhteeva. — Ekaterinburg: Uralskiy gosudarstvennyy yuridicheskiy universitet. — 2021. — S. 318–326.
12. Ushakov N. O., Sibikina I. V., Kosmacheva I. M. Informatsionnaya bezopasnost v sistemakh elektronnogo dokumentooborota // Tekhnicheskaya ekspluatatsiya vodnogo transporta: problemy i puti razvitiya. — 2021. — № 1. — S. 70–74.
13. Yurkevich M. A. Primenenie sudom videotekhnologiy v ugolovnom sudoproizvodstve: dis. … kand. yurid. nauk. — M., 2021.
14. Luff C. Cybersecurity and the future of blockchain technology // URL: http://www.gingermaypr.com/cybersecurity-blockchain-technology.html (data obrashcheniya: 08.07.2024).