Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.5:347.91/.95:340.134

КИБЕРБЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ. АКТУАЛЬНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИС В СУДЕБНОЙ СИСТЕМЕ

Рытова Екатерина Ивановна,
Казанский инновационный университет им. В.Г. Тимирясова, г. Казань,
Факультет менеджмента и инженерного бизнеса,
Магистрант 3 курса,
Rytowa.catya@yandex.ru

Аннотация

Цифровизация судебной системы коренным образом изменила способы хранения, обработки, передачи юридически значимой информации. Ускорение процессов документооборота и расширение доступа граждан к электронным сервисам сопровождались ростом уязвимостей, которые способны подорвать доверие к правосудию, поставить под сомнение легитимность решений. Этим обусловливается актуальность обсуждаемой темы — устойчивость государственных информационных систем становится как техническим, так и социально-правовым вопросом. Цель в рамках статьи заключается в выявлении рисков киберугроз, характерных для судебных инфо-платформ, и формулировании перспективных направлений усовершенствования механизмов их защиты. Материал будет полезен юристам, разработчикам государственных сервисов, исследователям цифровой трансформации правосудия.

Ключевые слова: безопасность данных, государственные информационные системы, киберугрозы, правовое регулирование, судебная система, уязвимости, цифровые доказательства

CYBERSECURITY OF GOVERNMENT INFORMATION SYSTEMS: CURRENT SECURITY CHALLENGES IN THE JUDICIAL SYSTEM

Rytova Ekaterina Ivanovna,
Kazan Innovative University named after V.G. Timiryasov, Kazan,
Faculty of Management and Engineering Business,
3rd year Master's student,
Rytowa.catya@yandex.ru

ABSTRACT

The digital transformation of the judiciary has fundamentally reshaped the ways legally significant information is stored, processed, and transmitted. The acceleration of document workflows and the expansion of citizens' access to electronic services have been accompanied by

a rise in vulnerabilities that may undermine public trust in justice and cast doubt on the legitimacy of court rulings. This underscores the relevance of the topic: the resilience of government information systems has become not only a technical challenge but also a socio-legal issue. The purpose of the article is to identify the cybersecurity risks inherent in judicial information platforms and to outline promising directions for strengthening protection mechanisms. The material will be of value to legal practitioners, developers of government services, and scholars studying the digital transformation of justice.

Keywords: cybersecurity threats, data protection, digital evidence, government information systems, judicial system, legal regulation, vulnerabilities

Введение. Государственные информационные системы (ГИС) выступают в качестве ключевого инструмента функционирования публичной власти и обеспечивают управление значимыми общественными процессами. Их уязвимость в цифровой среде напрямую влияет на национальную безопасность, правовую стабильность, доверие граждан к институтам государства.

Особое место в рассматриваемой сфере занимает судебная система, где электронные сервисы используются для хранения процессуальных документов, обработки персональных данных участников процессов, взаимодействия между различными инстанциями. Одна из наиболее острых проблем состоит в том, что рост объёмов информации, переход к digital-каналам коммуникации, весомое усложнение технологий порождают новые формы угроз, с которыми традиционные подходы к защите зачастую не справляются.

В увязке с отмеченным выше очень важно рассмотреть специфику рисков, которые связаны с эксплуатацией информационных систем судов, выявить слабые места в действующих механизмах обеспечения киберустойчивости, а также предложить направления усовершенствования защиты.

Методы. В работе над статьёй применялось сочетание междисциплинарного анализа и приёмов научного изложения, позволяющих показать тему целостно, аргументированно. В первую очередь, использовалась системная перспектива (судебные информационные системы рассматривались не как изолированные технические решения, а как часть правового, социального контекста, что дало возможность выявить не только технические, но и организационные, нормативные аспекты проблемы). Важным шагом стало структурирование материала по логическим блокам — от постановки проблемы и описания функций систем до анализа угроз, перспектив развития. Такой подход обеспечил связность рассуждений.

При характеристике уязвимостей и направлений защиты применялись элементы сравнительного анализа (сопоставлялись внутренние и внешние факторы риска, указывалось на противоречия между требованием открытости судебной информации и необходимостью её конфиденциальности). Это дало возможность показать напряжённость внутри самой системы.

Завершающий раздел строился на обобщении выявленных тенденций и формулировании выводов с практической значимостью.

Результаты и обсуждение. Цифровизация правосудия опирается на внедрение таких платформ, как электронные архивы дел, системы удалённого участия в заседаниях, онлайн-порталы для подачи заявлений и т. д. Благодаря этому ускоряются процедуры документооборота, повышается доступность правосудия. Помимо этого, снижаются издержки. Однако столь интенсивная интеграция технологий создает условия, при которых сбой в одном элементе способен парализовать работу целой подсистемы.

Важно подчеркнуть, что судебные информационные системы выполняют как техническую, так и социально-правовую функцию. Они аккумулируют конфиденциальные сведения, в том числе:

- медицинские данные;
- сведения о финансовом положении граждан;
- корпоративную тайну [2, 5].

Следовательно, любая несанкционированная утечка подрывает принцип тайны судопроизводства и ставит под сомнение законность принятых решений.

Далее целесообразно перейти к конкретизированному рассмотрению угроз судебных информационных систем. Уместно выделить следующие уровни (таблица 1):

Таблица 1 – Характеристика уровней уязвимостей
(составлено на основе [1, 4, 5])

Уровень	Описание
Технические риски	Внедрение вредоносного программного обеспечения, взлом каналов связи, атаки типа DDoS, направленные на блокировку доступа к системам.
Организационные проблемы	Недостаток квалификации у сотрудников, человеческие ошибки, слабая регламентация распределения прав доступа.
Правовые пробелы	Несовершенство нормативной базы, отставание механизмов регулирования от скорости технологических изменений.
Социальные вызовы	Недостаток доверия к цифровизации, что выражается в сомнении сторон судебного процесса в корректности электронных доказательств.

Нужно отметить, что наиболее опасным сценарием становится не только внешнее вмешательство, но и внутренние нарушения, которые сопряжены с неправомерным использованием служебного доступа.

В отличие от многих иных государственных структур, судебная система предъявляет особые требования к прозрачности и одновременной конфиденциальности. Это противоречие порождает ряд дилемм. С одной стороны, требуется обеспечить открытый доступ к судебным актам как к публичной информации. С другой — ограничить распространение персональных данных участников процессов [1, 6].

Стандартные меры защиты — антивирусные пакеты, межсетевые экраны, резервное копирование — играют лишь вспомогательную роль. Критически значимо внедрение комплексного подхода, представленного постоянным аудитом, моделированием угроз. Очень важна выработка сценариев реагирования на инциденты.

В дополнение к отмеченному, судебные информационные системы отличаются высокой интеграцией с внешними ресурсами:

- банки данных МВД;
- база налоговой службы;
- регистры недвижимости [3, 4].

Такая взаимосвязанность повышает эффективность работы, но одновременно увеличивает зону потенциальных рисков (атака на один узел способна повлечь цепную реакцию в смежных системах).

Правовое обеспечение в сфере кибербезопасности развивается быстрее, чем это было ещё десять лет назад; между тем, всё же отстаёт от динамики технологических угроз. В частности, в законодательстве часто не учитывается специфика судебных процессов в цифровой среде:

- допустимость электронных доказательств;
- ответственность операторов систем за утечку данных;

Недостаточная конкретизация приводит к коллизиям. К примеру, в некоторых случаях суды сталкиваются с невозможностью признания подлинности цифрового документа без дополнительной технической экспертизы, что существенно затягивает рассмотрение. Отсутствие унифицированных требований к сертификации программного обеспечения также создаёт риск использования уязвимых решений.

В увязке с отмеченным выше целесообразно выделить несколько направлений, которые, по мнению автора, помогут повысить надежность судебных информационных систем (таблица 2):

Таблица 2 – Перспективы укрепления киберустойчивости
(составлено автором)

Контекст	Характеристика
Развитие системного мониторинга	Постоянный анализ активности пользователей и сетевых событий позволяет выявлять подозрительные операции на ранней стадии.
Задействование технологий искусственного интеллекта	Алгоритмы машинного обучения дают возможность автоматически классифицировать аномалии, прогнозировать возможные инциденты.
Совершенствование нормативной базы	Речь идёт о создании единых стандартов безопасности для судебной сферы, включая требования к шифрованию, верификации цифровых доказательств.
Кадровая подготовка	Обучение сотрудников судов как техническим навыкам, так и вопросам правового регулирования digital-процессов.
Межведомственное сотрудничество	Обмен информацией о киберинцидентах между судами, правоохранительными органами, специализированными центрами.

Представляется, что только совокупное развитие указанных выше направлений поможет создать устойчивый к внешним и внутренним вызовам цифровой контур правосудия.

Выводы. Кибербезопасность государственных информационных систем, особенно в судебной сфере, становится стратегическим вызовом для стран. Угроза не ограничивается техническими сбоями — она затрагивает доверие к власти, легитимность решений, защиту конституционных прав граждан. Анализ показал, что проблематика носит комплексный характер, поскольку технические риски переплетаются с организационными, правовыми недостатками.

В целях минимизации угроз требуется развивать интегрированный подход, где совмещаются технологические инновации, продуманное законодательное регулирование, повышение компетенций специалистов и т. п. Судебная система, как институт, отвечающий за справедливость, правопорядок, требует особой степени защиты, так как компрометация

её информационных ресурсов характеризуется долгосрочными последствиями для государства и общества в целом.

Список литературы:

1. Ан В.Р., Табакаева В.А., Селифанов В.В. Разработка методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам критической информационной инфраструктуры, функционирующих на базе центров обработки данных // Интерэкспо Гео-Сибирь. – 2020. – Т. 6. – № 1. – С. 22-30.
2. Еловская М.А. Кибербезопасность и защита данных: вызовы цифрового мира // Актуальные направления научных исследований XXI века: теория и практика. – 2025. – Т. 13. – № 1 (68). – С. 117-127.
3. Кононов Д.А. Основные направления внедрения предиктивного правосудия и вопросы информационной безопасности судебной системы // Образование и право. – 2024. – № 4. – С. 271-274.
4. Лебедев В.Н. К вопросу о месте кибербезопасности в государственной системе информационной безопасности // Искусственный интеллект и большие данные (Big Data) в судебной и правоохранительной системе: реалии и требование времени. Материалы конференции. – Астана: 2023. – С. 127-135.
5. Михайлова Л.С. О некоторых проблемах обеспечения информационной безопасности судебных органов Российской Федерации // Конституционализм и государствоведение. – 2023. – № 2 (30). – С. 18-24.
6. Пенерджи Р.В., Гавдан Г.П. Информационная безопасность государственных информационных систем // Безопасность информационных технологий. – 2020. – Т. 27. – № 3. – С. 26-42.

References:

1. An V.R., Tabakaeva V.A., Selifanov V.V. Development of a Methodology for Cybersecurity Audit of State Information Systems Related to Significant Critical Information Infrastructure Objects Operated on the Basis of Data Processing Centers // Interexpo Geo-Siberia. – 2020. – Vol. 6. – No. 1. – Pp. 22-30.
2. Elovskaya M.A. Cybersecurity and Data Protection: Challenges of the Digital World // Actual Directions of Scientific Research in the 21st Century: Theory and Practice. – 2025. – Vol. 13. – No. 1 (68). – Pp. 117-127.
3. Kononov D.A. The Main Directions of Predictive Justice Implementation and Information Security Issues of the Judicial System // Education and Law. – 2024. – No. 4. – Pp. 271-274.
4. Lebedev V.N. On the Place of Cybersecurity in the State Information Security System // Artificial Intelligence and Big Data (Big Data) in the Judicial and Law Enforcement System: Realities and Requirements of the Time. Conference Proceedings. – Astana: 2023. – Pp. 127-135.
5. Mikhailova L.S. On Some Problems of Ensuring Information Security of the Judicial Bodies of the Russian Federation // Constitutionalism and State Studies. – 2023. – No. 2 (30). – Pp. 18-24.

6. Penerji R.V., Gavdan G.P. Information Security of State Information Systems // Security of Information Technologies. – 2020. – Vol. 27. – No. 3. – Pp. 26-42.