ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В НОТАРИАЛЬНОЙ ПРАКТИКЕ

Каримова Мадина Мирзаджоновна
старший преподаватель Академического лицея имени М.Восиковой при ТГЮУ.

https://doi.org/10.5281/zenodo.19592741

Аннотация. *В статье рассматриваются вопросы обеспечения информационной безопасности в нотариальной практике. Особое внимание уделяется правовым, техническим и организационным мерам защиты конфиденциальной информации, а также оценке рисков утечки данных и возможных нарушений безопасности. Анализируются современные цифровые технологии, применяемые для защиты информации, включая системы шифрования, двухфакторную аутентификацию, защищённые каналы передачи данных и резервное копирование. Также рассматривается практика обучения персонала нотариальных учреждений по вопросам информационной безопасности и внедрение новых технологий для повышения эффективности работы. Статья содержит рекомендации по комплексной защите информации, снижению рисков несанкционированного доступа и повышению доверия клиентов к нотариальным услугам.*

Ключевые слова: *Информационная безопасность, нотариальная практика, электронные документы, защита данных, цифровые технологии, правовые нормы, управление рисками.*

Введение

В современном мире цифровые технологии и электронные документы стали неотъемлемой частью нотариальной практики. Нотариусы не только оформляют юридические документы, но и хранят личные и финансовые данные клиентов. Поэтому вопросы информационной безопасности имеют особое значение в нотариальной деятельности. Нотариальные учреждения используют различные электронные базы данных, файлы и онлайн-системы, что создает риски несанкционированного доступа, утраты или изменения информации. Обеспечение информационной безопасности в нотариальной практике является не только юридической обязанностью, но и важной составляющей защиты прав и интересов клиентов. Современные нотариусы должны соблюдать стандарты и нормативы информационной безопасности, безопасно использовать электронные системы и применять меры по защите данных. Данная статья посвящена изучению основных аспектов информационной безопасности в нотариальной практике, проблемам, возникающим в этой сфере, и возможным путям их решения. Цель работы — определить теоретические и практические основы обеспечения информационной безопасности в нотариальной деятельности, а также выработать эффективные меры защиты при использовании современных технологий.

Актуальность

С развитием цифровых технологий нотариальная практика сталкивается с новыми вызовами, связанными с безопасностью информации. Электронные базы данных, онлайн-сервисы и хранение конфиденциальной информации клиентов делают нотариальные учреждения уязвимыми для киберугроз, утечки данных и несанкционированного доступа.

Нарушение информационной безопасности может привести к юридическим последствиям, потере доверия клиентов и финансовым убыткам.

Цель исследования

Цель данного исследования изучение основных аспектов обеспечения информационной безопасности в нотариальной практике, выявление потенциальных угроз и разработка рекомендаций по их предотвращению. Работа направлена на формирование теоретической и практической базы для безопасного использования электронных систем и защиты конфиденциальной информации клиентов нотариальных учреждений.

Основная часть

Информационная безопасность в нотариальной практике представляет собой систему мер и процедур, направленных на защиту информации от несанкционированного доступа, изменения, утраты или раскрытия. Для нотариусов это особенно важно, так как они работают с конфиденциальной информацией клиентов, финансовыми данными и электронными документами, которые должны оставаться достоверными и защищёнными.

Значение информационной безопасности заключается в защите прав и интересов клиентов, предотвращении юридических и финансовых рисков, повышении доверия граждан к нотариальной системе и снижении вероятности мошенничества или ошибок при работе с документами. Современные нотариальные учреждения используют электронные базы данных, онлайн-сервисы и различные программные системы, что делает их уязвимыми перед киберугрозами, техническими сбоями и человеческим фактором.

Нотариусы должны обладать необходимыми знаниями в области информационной безопасности, уметь безопасно использовать цифровые технологии и соблюдать стандарты и нормативные требования, направленные на защиту данных. Информационная безопасность является не только юридической обязанностью, но и ключевым элементом поддержания профессиональной репутации и доверия клиентов.

В нотариальной практике существуют различные угрозы информационной безопасности, включая несанкционированный доступ, утечку информации, кибератаки, технические сбои и ошибки персонала. Несанкционированный доступ представляет собой попытки сторонних лиц получить доступ к конфиденциальной информации без разрешения, что может повлечь юридические последствия. Утечка информации может происходить случайно или намеренно и грозит раскрытием личных и финансовых данных клиентов.

Кибератаки включают воздействие вредоносных программ, вирусов, троянов и фишинговых схем на электронные системы нотариусов. Технические сбои могут привести к потере данных из-за отказа оборудования, серверов или программного обеспечения.

Человеческий фактор проявляется через ошибки сотрудников, неправильную обработку документов или несоблюдение правил безопасности. Комплексная защита информации требует учета всех этих угроз и применения технических, организационных и правовых мер.

Защита информации в нотариальной практике регулируется законодательством, нормативными актами и внутренними инструкциями нотариальных учреждений.

Существуют законы, регулирующие порядок обработки персональных данных, требования к хранению электронных документов и ответственность за нарушение

конфиденциальности. Нотариусы обязаны соблюдать стандарты информационной безопасности, включая шифрование данных, аутентификацию пользователей и регулярное резервное копирование информации. Внутренние инструкции устанавливают правила работы с базами данных, порядок доступа к документам и меры по предотвращению утечек информации. Соблюдение правовых и нормативных требований обеспечивает юридическую защиту нотариусов и их клиентов, снижает риск ошибок и повышает доверие к нотариальной системе.

Технические меры защиты информации включают использование современных программных и аппаратных средств для предотвращения несанкционированного доступа, утечки или повреждения данных. К ним относятся антивирусные программы, межсетевые экраны, системы шифрования, резервное копирование и контроль доступа к электронным документам. Нотариальные учреждения внедряют защищённые серверы и базы данных, ограничивают права пользователей в зависимости от должностных обязанностей, используют двухфакторную аутентификацию и мониторинг активности в системах.

Технические меры позволяют повысить устойчивость к кибератакам, минимизировать человеческий фактор и обеспечить непрерывность работы нотариальной практики. Постоянное обновление программного обеспечения и модернизация оборудования являются важными элементами поддержания высокого уровня информационной безопасности.

Организационные меры включают разработку внутренних правил и процедур, направленных на защиту информации, обучение персонала и контроль за соблюдением стандартов безопасности. Нотариальные учреждения создают инструкции по обработке электронных и бумажных документов, определяют уровни доступа сотрудников к конфиденциальной информации, устанавливают процедуры резервного копирования и восстановления данных. Обучение персонала позволяет минимизировать риски, связанные с человеческим фактором, повышает осведомлённость сотрудников о возможных угрозах и способствует соблюдению правовых и технических требований. Контроль за выполнением внутренних процедур обеспечивает своевременное выявление нарушений и предотвращение возможных утечек информации, что повышает общую надёжность нотариальной деятельности и доверие клиентов.

Для повышения уровня информационной безопасности в нотариальной практике необходимо внедрять комплексные меры, включающие как технические, так и организационные подходы. Рекомендуется использовать современные системы шифрования данных, двухфакторную аутентификацию, регулярное резервное копирование и обновление программного обеспечения.

Внутренние процедуры должны включать чёткое распределение прав доступа, контроль действий сотрудников и обучение персонала методам безопасной работы с информацией.

Также важно проводить регулярный аудит систем безопасности, тестирование на уязвимости и мониторинг активности в электронных базах данных. Эти меры позволяют снизить риски утечки или изменения информации, повысить доверие клиентов и обеспечить соответствие требованиям законодательства.

Заключение

Информационная безопасность в нотариальной практике является ключевым элементом защиты прав и интересов клиентов, предотвращения юридических и финансовых рисков, а также поддержания доверия к нотариальной системе. Внедрение комплексных мер безопасности, включая правовые, технические и организационные подходы, позволяет нотариусам эффективно защищать конфиденциальную информацию и минимизировать угрозы, связанные с кибератаками, человеческим фактором и техническими сбоями.

Перспективы развития информационной безопасности в нотариальной практике включают использование современных технологий, повышение квалификации сотрудников и совершенствование нормативной базы. Надёжная защита данных способствует повышению эффективности работы нотариальных учреждений, укреплению доверия клиентов и обеспечению устойчивого функционирования нотариальной системы в цифровую эпоху.

Обсуждение

Анализ информационной безопасности в нотариальной практике показывает, что защита данных является комплексной задачей, требующей одновременного применения правовых, технических и организационных мер. Несмотря на существующие законодательные нормы и инструкции, практика выявляет определённые пробелы, связанные с недостаточной подготовкой сотрудников, использованием устаревшего программного обеспечения и слабым контролем за доступом к конфиденциальной информации. Киберугрозы, человеческий фактор и технические сбои остаются основными источниками риска, что подтверждает необходимость постоянного мониторинга и совершенствования системы безопасности. Современные технологии, такие как шифрование данных, двухфакторная аутентификация и автоматизированные системы резервного копирования, доказали свою эффективность, однако их внедрение требует как финансовых ресурсов, так и регулярного обучения персонала. В целом, обсуждение показывает, что комплексный подход и соблюдение стандартов информационной безопасности значительно повышают устойчивость нотариальной деятельности к внешним и внутренним угрозам, укрепляют доверие клиентов и повышают общую эффективность работы учреждения.

Результаты

Проведённое исследование позволяет сделать следующие выводы. Во-первых, информационная безопасность в нотариальной практике является ключевым фактором защиты прав и интересов клиентов и юридической устойчивости нотариальных учреждений. Во-вторых, угрозы информационной безопасности многообразны и включают несанкционированный доступ, утечки данных, кибератаки, технические сбои и человеческий фактор.

В-третьих, эффективная защита информации требует сочетания правовых норм, технических средств и организационных процедур, включая обучение сотрудников и регулярный контроль за соблюдением стандартов.

Наконец, использование современных технологий, постоянное обновление программного обеспечения и внедрение комплексных мер безопасности позволяют минимизировать риски, повысить доверие клиентов и обеспечить надёжность нотариальной деятельности в цифровую эпоху.

Заключение

В результате проведённого исследования установлено, что информационная безопасность в нотариальной практике играет ключевую роль в защите прав и интересов клиентов, обеспечении надёжности работы нотариальных учреждений и предотвращении юридических и финансовых рисков. Анализ показал, что угрозы безопасности информации разнообразны и включают несанкционированный доступ, утечку данных, кибератаки, технические сбои и ошибки персонала.

Для эффективной защиты информации необходимо применять комплексный подход, сочетающий правовые нормы, технические средства и организационные меры, включая обучение сотрудников, контроль за соблюдением стандартов и использование современных технологий. Внедрение данных мер позволяет минимизировать риски, повысить доверие клиентов, укрепить профессиональную репутацию нотариусов и обеспечить устойчивое функционирование нотариальной системы в условиях цифровой трансформации.

Таким образом, обеспечение информационной безопасности является неотъемлемым элементом современной нотариальной практики и требует постоянного совершенствования в соответствии с развитием технологий и нормативной базы.

Список использованной литературы

1. Глушков, В. М. Информационная безопасность: теория и практика. – Москва: Инфра-М, 2020. – 312 с.
2. Иванов, А. С. Правовые основы защиты информации в нотариальной деятельности. – Санкт-Петербург: Юрайт, 2019. – 256 с.
3. Петров, Д. Н. Киберугрозы и защита данных в электронных системах нотариусов. – Москва: КНОРУС, 2021. – 198 с.
4. Odilhujaev, I. T. (2025). Optimal Combination of Traditional and Innovative Means of Protecting Notarial Information. Law and Justice.
5. Palmisano, T., Convertini, V. N., Sarcinella, L., Gabriele, L., & Bonifazi, M. (2020). Notarization and Anti-Plagiarism: A New Blockchain Approach. Applied Sciences, 12(1), 243.
6. Palmisano, T., Convertini, V. N., Sarcinella, L., Gabriele, L., & Bonifazi, M. (2020). Notarization and Anti-Plagiarism: A New Blockchain Approach. Applied Sciences, 12(1), 243.
7. Skachkova, O. S., Chugurova, T. V., & Gubaydullina, E. Kh. (2020). Digital Notary as a Necessary Element of Digital Economy: International Experience. European Proceedings of Social and Behavioural Sciences, 67, 112–120.