3 **Ольгейзер, И. А.** Безопасность роспуска составов на сортировочных горках. Граничные условия функционирования при эксплуатации горочных систем автоматизации / И. А. Ольгейзер // Проблемы безопасности на транспорте : материалы докладов IX Междунар. науч.-практ. конф. В 2 ч. Ч. 1 / под общ. ред. Ю. И. Кулаженко. – Гомель : БелГУТ, 2019. – С. 65–66.

4 Идентификация критических состояний технологических процессов на основе методов предиктивной аналитики / С. М. Ковалев [и др.] // Автоматика и телемеханика. – 2023. – № 4. – С. 115–130. – DOI: 10.31857/S0005231023040074.

5 Исследование параметров основного удельного сопротивления движению вагонов при скатывании с сортировочной горки / С. А. Бессоненко [и др.] // Известия Транссиба. – 2023. – № 1 (53). – С. 53–62.

6 Устройство счета и контроля расцепа вагонов / И. А. Ольгейзер [и др.] // Автоматика, связь, информатика. – 2024. – № 5. – С. 9–11. – DOI: 10.62994/AT.2024.5.5.001.

7 Инновационные алгоритмы машинного зрения для диагностики продольного профиля сортировочных путей / А. И. Долгий [и др.] // Автоматика, связь, информатика. – 2022. – № 8. – С. 7–9. – DOI: 10.34649/AT.2022.8.8.002.

8 Компьютерное зрение для контроля сортировочных процессов / А. Е. Хатламаджиян [и др.] // Автоматика, связь, информатика. – 2021. – № 3. – С. 8–11. – DOI: 10.34649/AT.2021.3.3.002.

9 **Хатламаджиян, А. Е.** Интегрированный пост автоматизированного приёма и диагностики подвижного состава на сортировочных станциях / А. Е. Хатламаджиян, А. И. Лебедев // Вагоны и вагонное хозяйство. – 2019. – № 2 (58). – С. 9–13.

УДК 378.00

ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ АДВОКАТСКОЙ ТАЙНЫ ПРИ ОКАЗАНИИ ЮРИДИЧЕСКОЙ ПОМОЩИ В ОБЛАСТИ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Е. С. ТИТОВ
Уральский государственный университет путей сообщения, г. Екатеринбург, Российская Федерация

Адвокатская тайна – один из ключевых элементов правосудия, гарантирующий клиентам конфиденциальность информации, сообщаемой адвокату в процессе оказания юридической помощи. Вопрос сохранения тайны приобретает особую важность, когда заказчиком юридических услуг выступает государство, однако это не является государственной тайной. В таких случаях адвокаты могут столкнуться с дополнительными техническими вызовами, связанными с информационной безопасностью сведений, которые передаются и обрабатываются в цифровом пространстве, учитывая, что системы и сети, а также автоматизированные системы управления, функционирующие в сфере транспорта, как правило, относят к критической информационной инфраструктуре. Современные технологии, особенно при взаимодействии с государственными структурами, создают определенные риски для сохранения конфиденциальности.

Целью работы является анализ технических проблем обеспечения адвокатской тайны в условиях оказания юридической помощи государству, а также рассмотрение возможных решений и мер по их минимизации.

Основные технические проблемы:

1 Риски утечки данных в процессе передачи информации. Адвокаты часто используют цифровые каналы связи (электронная почта, мессенджеры, облачные сервисы) для передачи конфиденциальной информации. Государственные органы могут требовать передачи информации через защищенные каналы, однако даже в таких случаях существует риск компрометации и утечки данных из-за следующих факторов:

– недостаточный уровень шифрования или применение устаревших, несертифицированных алгоритмов;

– неадекватное управление ключами шифрования, особенно когда государственные органы требуют доступ к ключам;

– уязвимости протоколов передачи данных (например, недостаточная защита при использовании VPN или TLS);

– участие в процессе множества заинтересованных сторон: следователи, прокуроры, адвокаты, их подзащитные (доверители), свидетели, дознаватели, судьи и другие участники процессов правосудия, имеющие процессуальные статус и права на доступ к той или иной информации.

2 *Необходимость соблюдения стандартов информационной безопасности.* Государственные структуры могут предъявлять особые требования к техническим стандартам, что может усложнить процесс взаимодействия с адвокатами. Среди распространённых проблем:

– несоответствие используемых адвокатами систем хранения и обработки данных государственным требованиям;

– неполная совместимость систем адвокатов с государственными системами передачи данных, что может потребовать использования промежуточных решений, повышающих риски утечек (лоскутная автоматизация);

– доступ государственных органов к инфраструктуре или системам, через которые проходит юридическая переписка (Privileged Access);

– дополнительные жёсткие требования регуляторов в связи с отнесением транспортной отрасли к критической информационной инфраструктуре.

3 *Технические возможности для отслеживания действий пользователей.* При оказании юридической помощи государству адвокаты могут сталкиваться с проблемами, связанными с тем, что государственные органы имеют доступ к различным средствам наблюдения и контроля, таким как системы мониторинга интернет-трафика и анализ активности пользователей на устройствах. Это создает риск несанкционированного доступа к информации, передаваемой адвокатом в процессе работы:

– мониторинг сетевых коммуникаций может раскрыть конфиденциальные детали переписки, что создаёт риски использования такой информации в качестве доказательств;

– использование корпоративных или государственных устройств адвокатами может позволить государству отслеживать действия пользователя, что нарушает принцип адвокатской тайны.

4 *Недостатки в управлении доступом.* Важно учитывать, что государственные структуры могут вводить свои собственные правила доступа к информации, что создает следующие риски:

– неконтролируемый доступ к юридической информации со стороны сотрудников государственных и контролирующих органов;

– возможность случайной или намеренной утечки данных, когда информация доступна большому количеству лиц, либо скомпрометирована в средствах массовой информации в результате целенаправленной атаки (APT).

5 Необходимость обеспечения достоверности, допустимости и относимости доказательств.

Возможные решения:

1 *Использование сильных методов шифрования и протоколов безопасности.* Для защиты адвокатской тайны при передаче информации государству необходимо применять современные алгоритмы шифрования, такие как AES-256, ГОСТ 34.12-2018 и более современные версии протоколов TLS. Также стоит обратить внимание на регулярное обновление сертификатов и применение двухфакторной аутентификации для всех участников процесса передачи данных.

2 *Соблюдение международных стандартов по защите информации.* Следование международным стандартам (например, ISO/IEC 27001) и внедрение передовых практик по защите информации позволит адвокатам и государственным структурам снизить риски утечки данных и обеспечить конфиденциальность юридической переписки.

3 *Использование защищённых каналов связи.* Важно предусмотреть использование специализированных платформ для безопасного обмена юридической информацией, которые обеспечивают как шифрование, так и контроль доступа к информации. Примером могут служить системы на базе технологии блокчейн, обеспечивающие неизменяемость и защиту данных.

4 *Ограничение доступа и аудит действий.* Адвокатам стоит внедрять практики ограничения доступа к конфиденциальной информации и проводить регулярный аудит всех операций с юридическими данными. Это включает:

– минимизацию числа лиц, имеющих доступ к конфиденциальной информации. Разграничение доступа на основе одной или нескольких моделей;

– логирование всех действий с юридическими данными для последующего анализа на предмет возможных нарушений;

– контроль превилигированного доступа, например, со стороны контролирующих органов. Privileged Access Management (PAM).

5 *Обучение и повышение осведомлённости.* Адвокатам, работающим с государственными структурами, необходимо постоянно повышать свою осведомлённость в области кибербезопасности и защиты данных. Государственные заказчики также должны обеспечивать обучение своих сотрудников и адвокатов правильным методам обращения с конфиденциальной информацией и практическими навыками в этой области.

6 Цифровые подписи, метаданные, методы стеганографии и «невидимая маркировака» могут обеспечить определение достоверности, истории происхождения документа или выявить канал утечки.

7 *Использование модели доступа* на основе ролей.

Заключение

Обеспечение адвокатской тайны в условиях работы с государственными органами требует тщательного подхода к техническим аспектам информационной безопасности. Современные технологии, используемые для передачи и обработки данных, должны быть надёжно защищены от несанкционированного доступа. Только так возможно сохранить доверие клиентов и гарантировать соблюдение правовых норм при оказании юридической помощи.

Важной задачей является постоянное улучшение систем защиты информации, а также повышение уровня осведомлённости всех участников процесса. Совокупность технических и организационных мер позволит минимизировать риски утечки адвокатской тайны и обеспечить надежную защиту конфиденциальной информации.

Список литературы

1 **Акинина, Н. Ю.** Проблемы соблюдения адвокатской тайны / Н. Ю. Акинина // Вестник Югорского государственного университета. – 2015. – Вып. 1 (36). – С. 95–98.

2 **Пилипенко, Ю. С.** Адвокатская тайна: теория и практика реализации : автореф. дис. … д-ра юрид. наук / Ю. С. Пилипенко. – М., 2009. – 56 с.

3 Научно-практический комментарий к Федеральному закону от 21 ноября 2011 г. № 324-ФЗ «О бесплатной юридической помощи в Российской Федерации» (постатейный) [Электронный ресурс] / М. Л. Баранов [и др.] ; под ред. Ю. А. Дмитриева. – М., 2012. – Режим доступа : http://www.consultant.ru. – Дата доступа : 09.09.2024.

УДК 625.161

СОВЕРШЕНСТВОВАНИЕ АЛГОРИТМА ФОРМИРОВАНИЯ ИЗВЕЩЕНИЯ О ПРИБЛИЖЕНИИ К ПЕРЕЕЗДУ

А. М. ТРУНАЕВ

Ростовский государственный университет путей сообщения, г. Ростов-на-Дону, Российская Федерация

Системы переездной железнодорожной сигнализации – это сложные автоматизированные системы с непрерывным рабочим процессом и последовательной структурой. По требованиям безопасности при неисправности системы разрешающее показание светофора должно перекрываться на запрещающее [1]. Пока не будет устранена неисправность, переездные устройства перекрывают движение через переезд, что является одной из причин простоя автотранспорта перед переездом. Поезд на участке приближения отсутствует, а автотранспортные средства простаивают перед закрытыми переездными устройствами. Другой более распространённой причиной является заблаговременное закрытие переездных устройств при приближении поезда к переезду, при уменьшенном скоростном режиме поезда по участку. Это следствие несовершенства систем формирования извещения.

Существующие системы оповещения о приближении поезда можно разделить на дискретные и координатные. Преимуществами дискретных систем оповещения являются простота и надежность. К недостаткам относятся:

– наличие кабелей для подключения устройств оповещения (в большинстве случаев);

– включение заградительных сигналов без учета скорости и ускорения (торможения) поезда. Это часто влечет за собой преждевременное закрытие железнодорожного пути и автомобильного переезда, что в свою очередь приводит к длительным остановкам движения автотранспорта на переездах. Это является источником неоправданного стресса водителей, который часто перерастает в