

Краснодарский университет МВД России

**ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ  
ДЕЛОПРОИЗВОДСТВА И РЕЖИМА**

Материалы  
Всероссийской научно-практической конференции  
(22 октября 2025 г.)

Краснодар  
2026

УДК 316.485.6+004.7  
ББК 66.4(0)+304.1  
О-641

Одобрено  
редакционно-издательским советом  
Краснодарского университета  
МВД России

Редакционная коллегия:

*А. В. Власенко*, кандидат технических наук, доцент (председатель);

*В. И. Еремченко*, кандидат юридических наук, доцент  
(заместитель председателя);

*А. К. Назаров*, кандидат физико-математических наук  
(ответственный секретарь);

*С. В. Концов*, кандидат социологических наук;

*А. М. Погребная*

**О-641**      **Организация деятельности подразделений** делопроизводства и режима [Электронный ресурс] : материалы Всерос. науч.-практ. конф., 22 окт. 2025 г. / редкол.: А. В. Власенко, В. И. Еремченко, А. К. Назаров и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2026. – 1 электрон. опт. диск.

ISBN 978-5-9266-2251-2

Содержатся материалы Всероссийской научно-практической конференции «Организация деятельности подразделений делопроизводства и режима», состоявшейся в Краснодарском университете МВД России 22 октября 2025 г.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 316.485.6+004.7  
ББК 66.4(0)+304.1

ISBN 978-5-9266-2251-2

© Краснодарский университет  
МВД России, 2026

## Содержание

|                                                                                                                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>Власенко А.В.</b> Внедрение технологий искусственного интеллекта в деятельность подразделений делопроизводства органов внутренних дел: комплексный анализ эффективности и угроз информационной безопасности..... | 4  |
| <b>Иванов С.И.</b> О некоторых аспектах соблюдения режима секретности при обеспечении конспирации оперативно-розыскной деятельности.....                                                                            | 9  |
| <b>Копцов С.В.</b> Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.....                                                                                           | 13 |
| <b>Куминов М.В.</b> Электронный документооборот под угрозой: как интегрировать принципы информационной безопасности в процессы делопроизводства.....                                                                | 17 |
| <b>Ларина А.Ю.</b> Реализация проблемно-поискового метода обучения в командной работе при проведении учебных занятий по учебной дисциплине «Делопроизводство и режим секретности в органах внутренних дел».....     | 23 |
| <b>Назаров А.К.</b> Эволюция современной киберкриминальной парадигмы: от шифровальщиков к Ransomware 2.0.....                                                                                                       | 28 |
| <b>Новикова А.А.</b> Применение OSINT-инструментов Maltego и Shodan в оперативно-розыскной деятельности органов внутренних дел: технологические и правовые аспекты.....                                             | 32 |
| <b>Победа А.С.</b> К вопросу о предварительном учете документов...                                                                                                                                                  | 39 |
| <b>Синицкий С.Д., Кущев А.В.</b> Об учете трудозатрат подразделений делопроизводства и режима.....                                                                                                                  | 41 |

**Власенко Александра Владимировна,**  
врио заведующего кафедрой информационной безопасности  
Краснодарского университета МВД России  
кандидат технических наук, доцент

## **ВНЕДРЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ПОДРАЗДЕЛЕНИЙ ДЕЛОПРОИЗВОДСТВА ОРГАНОВ ВНУТРЕННИХ ДЕЛ: КОМПЛЕКСНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **Аннотация**

Статья посвящена комплексному исследованию процессов внедрения технологий искусственного интеллекта (ИИ) в деятельность подразделений делопроизводства и документационного обеспечения управления (ДООУ) органов внутренних дел (ОВД) Российской Федерации. Проведен детальный анализ потенциальных направлений применения ИИ, включая интеллектуальную регистрацию, классификацию, контроль исполнения и семантический анализ документов. Систематизированы ключевые угрозы информационной безопасности, возникающие на различных этапах жизненного цикла AI-систем: от сбора данных до эксплуатации модели. Особое внимание уделено рискам, специфичным для правоохранительной деятельности, таким как целенаправленные атаки на данные, нарушение конфиденциальности служебной информации и отсутствие прозрачности алгоритмов. На основе проведенного анализа разработана концептуальная модель поэтапного внедрения ИИ в документооборот ОВД, предусматривающая создание защищенной отечественной программно-аппаратной платформы, формирование нормативно-правового поля и подготовку специализированных кадров. Сделан вывод о том, что преодоление выявленных системных противоречий между эффективностью и безопасностью требует разработки ведомственной стратегии, основанной на принципах безопасного и ответственного ИИ.

**Ключевые слова:** искусственный интеллект, делопроизводство, документооборот, органы внутренних дел, информационная безопасность, машинное обучение, обработка естественного языка, киберриски, нормативное регулирование.

### **Введение**

Цифровая трансформация государственного управления является одним из стратегических приоритетов Российской Федерации. Органы внутренних дел, как ключевой элемент правоохранительной системы, испытывают острую необходимость в повышении эффективности управления за счет внедрения передовых технологий. Подразделения делопроиз-

водства и документационного обеспечения управления (ДОУ), обрабатывающие огромные массивы служебной документации, остаются критически важным звеном, от которого зависит оперативность принятия решений и качество исполнения управленческих функций.

Традиционные методы организации делопроизводства, основанные на значительной доли ручного труда, уже не справляются с возрастающими объемами информации и требованиями к скорости ее обработки. В этом контексте технологии искусственного интеллекта (ИИ) представляют собой не просто инструмент оптимизации, а фактор кардинального изменения парадигмы документооборота. Однако интеграция ИИ в защищенную информационную среду ОВД, обрабатывающую сведения ограниченного распространения и иную конфиденциальную информацию, порождает комплекс уникальных вызовов, главным из которых является обеспечение информационной безопасности.

Целью данного исследования является проведение комплексного анализа потенциальных направлений, выгод, рисков и условий безопасного внедрения технологий искусственного интеллекта в деятельность подразделений делопроизводства ОВД.

Внедрение ИИ позволяет перейти от простой автоматизации рутинных операций к интеллектуализации всего документооборота. Можно выделить несколько уровней воздействия:

#### 1. Интеллектуальная автоматизация рутинных операций.

Системы на основе компьютерного зрения и обработки естественного языка (NLP) способны не только распознавать реквизиты входящих документов (исх. №, дата, корреспондент), но и верифицировать их подлинность, сверяя с электронной подписью или эталонными образцами бланков.

Алгоритмы машинного обучения, анализируя семантику документа, могут автоматически присваивать ему индекс по номенклатуре дел, определять степень срочности и секретности, а также направлять его конкретному исполнителю, учитывая его текущую загруженность, компетенцию и зону ответственности. Например, рапорт о правонарушении может быть автоматически направлен в соответствующее оперативное подразделение и зарегистрирован в КУСП.

#### 2. Аналитика и поддержка принятия решений.

Интеллектуальный контроль исполнительской дисциплины. Вместо простого отслеживания сроков, ИИ-системы могут прогнозировать риски срыва исполнения поручений на основе анализа сложности задачи, исторической загруженности исполнителя и внешних факторов. Система может активно предлагать руководителю скорректировать сроки или перераспределить нагрузку.

Семантический поиск и извлечение сущностей. Это одно из наиболее перспективных направлений для ОВД. Технологии NLP позволяют автоматически выявлять в текстах документов и протоколов ключевые сущно-

сти: ФИО фигурантов, свидетелей, госномера автомобилей, серии и номера паспортов, адреса, статьи УК РФ и УПК РФ.

Это позволяет автоматически формировать и связывать дела, карты и базы данных, выявлять скрытые связи между лицами, событиями и документами, облегчать работу следователей и оперативных работников, предоставляя им структурированную информацию из массива документов.

Генеративные AI-модели могут использоваться для составления проектов типовых документов (запросы, уведомления, ответы гражданам) и даже в написании более сложных документов, таких как обзоры или аналитические справки, на основе предоставленных данных и шаблонов.

Агрегируя и анализируя метаданные всего документооборота, ИИ может выявлять системные узкие места, оптимизировать бизнес-процессы и предоставлять руководству аналитику в режиме, близком к реальному времени, о нагрузке на подразделения, наиболее частых темах обращений и динамике исполнения поручений.

Внедрение ИИ создает новые векторы атак и уязвимости, которые требуют особого подхода к защите.

«Отравление данных». Злоумышленник может преднамеренно внести искажения в обучающую выборку. Например, добавив в набор данных для обучения классификатора документы, помеченные неверными индексами. Это приведет к систематическим ошибкам алгоритма при эксплуатации: срочный оперативный документ может быть классифицирован как второстепенный и утрачен.

Нарушение конфиденциальности обучающих данных. Сами данные, на которых обучается модель, являются критически важным активом. Их утечка равносильна утечке всей служебной информации, содержащейся в историческом массиве документов ОВД. Использование публичных или коммерческих облачных сервисов для обучения моделей абсолютно недопустимо.

Враждебные атаки. Злоумышленник может создать такой входной документ (например, внося незаметные для человека изменения в пиксели скана или в текст), который будет целенаправленно вводить модель ИИ в заблуждение, приводя к некорректной классификации или маршрутизации.

Проблема «объяснимости». Нейросетевые модели часто являются «черными ящиками»: невозможно понять логику, по которой было принято то или иное решение. В правоохранительной деятельности, где каждое действие должно быть обосновано и потенциально оспоримо в суде, это создает фундаментальную проблему. Почему документ был направлен именно в это подразделение? Почему он был помечен как несущественный?

Несанкционированный доступ к AI-сервису. Взлом API или интерфейса AI-системы может позволить злоумышленнику не только похищать обрабатываемые документы, но и манипулировать самой моделью.

Ориентация на зарубежные платформы и frameworks для разработки AI-решений создает риски санкционных ограничений и наличия в них заранее внедренных уязвимостей (закладок).

«Слепое доверие» алгоритму. Сотрудники могут начать безоговорочно доверять решениям ИИ, отключая критическое мышление, что приведет к пропуску ошибок, допущенных алгоритмом.

Для минимизации рисков и максимизации эффекта внедрение ИИ должно быть системным и регламентированным. Предлагается следующая многоуровневая модель:

**1. Нормативно-правовой уровень.**

Разработка и принятие Ведомственной концепции использования ИИ в МВД России. Этот документ должен определить стратегию, принципы, границы применения и зоны ответственности. Внесение изменений в Инструкцию по делопроизводству в ОВД. Необходимо закрепить правовой статус действий, совершенных с помощью ИИ, порядок их аудита и исправления, а также требования к протоколированию этих действий. Создание методических рекомендаций по проверке, сертификации и аудиту безопасности AI-систем.

**2. Технологический уровень.**

Создание защищенной отечественной программно-аппаратной платформы («AI-платформа МВД»). Платформа должна быть развернута в изолированной инфраструктуре, использовать импортонезависимое программное обеспечение и аппаратные ускорители. Реализация принципа «закрытого контура» данных. Все процессы – сбор данных, обучение моделей, эксплуатация – должны происходить внутри защищенного периметра МВД без доступа в публичные сети. Внедрение механизмов «объяснимого ИИ». Обязательное требование ко всем внедряемым системам – возможность формирования отчета о том, на основании каких данных и по каким признакам было принято решение. Регулярный пентестинг и аудит безопасности AI-систем на предмет уязвимостей и устойчивости к враждебным атакам.

**3. Организационно-кадровый уровень.**

Формирование профильных рабочих групп из числа сотрудников делопроизводства, IT-специалистов и представителей службы безопасности для управления проектами внедрения. Разработка и реализация программ повышения квалификации для сотрудников делопроизводства, направленных на формирование «цифровых компетенций» и критического восприятия решений ИИ. Подготовка специалистов в области AI-безопасности в ведомственных вузах.

**Заключение**

Технологии искусственного интеллекта обладают колоссальным потенциалом для трансформации делопроизводства ОВД, переводя его из затратной рутинной функции в стратегический актив, повышающий эф-

эффективность управления в целом. Реализация этого потенциала сопряжена с высокими рисками в области информационной безопасности, которые носят системный и многоуровневый характер.

Преодоление противоречия между эффективностью и безопасностью требует не точечных мер, а реализации комплексной ведомственной стратегии. Ключевыми элементами такой стратегии должны стать: создание независимой AI-платформы, формирование адекватной нормативной базы и масштабная подготовка кадров. Только при условии приоритета безопасности, основанного на принципах «безопасного» и «объяснимого» ИИ, можно обеспечить не только операциональную эффективность, но и надежную защиту служебной информации, что является императивом для любой правоохранительной системы.

### **Литература**

1. Стратегия развития искусственного интеллекта в Российской Федерации на период до 2030 года (утв. Указом Президента РФ от 10 октября 2019 г. № 490).
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/).
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](https://www.consultant.ru/document/cons_doc_LAW_61798/).
4. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2024. – 336 с.
5. Шаблинский И.Г. Правовое регулирование информационных отношений в сфере обработки персональных данных: учебное пособие для вузов / И. Г. Шаблинский ; под редакцией М. А. Федотова. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 52 с. Тарасов У.Л. Анализ угроз безопасности информации. – Новосибирск: НГУ, 2023. – 270 с.

**Иванов Святослав Игоревич,**  
начальник кафедры оперативно-розыскной деятельности в ОВД  
Краснодарского университета МВД России  
кандидат юридических наук, доцент

## **О НЕКОТОРЫХ АСПЕКТАХ СОБЛЮДЕНИЯ РЕЖИМА СЕКРЕТНОСТИ ПРИ ОБЕСПЕЧЕНИИ КОНСПИРАЦИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Современная практика осуществления оперативно-розыскной деятельности (далее – ОРД) оперативными подразделениями органов внутренних дел (далее – ОВД) свидетельствует о том, что сталкиваясь с необходимостью выявления латентных преступлений, пресечения и раскрытия тяжких и особо тяжких преступлений, совершенных организованными группами и преступными сообществами, с необходимостью преодоления противодействия со стороны проверяемых и разрабатываемых лиц. Для решения таких задач обязательным является соблюдение принципа конспирации, который выражается в сохранении в тайне сведений, относящихся к государственной и служебной тайне, а также информации, распространение которой может послужить причиной ее расшифровки от лиц, способных использовать данную информацию против интересов правоохранительных органов.<sup>1</sup> Из названного определения вытекает, что сущность конспирации заключается в сохранении в тайне от противоборствующей стороны, таких сведений, оглашение или утечка которых причинит вред субъекту конспирации.

Разбираясь с решением вопроса о сохранении сведений (информации) в тайне, прежде всего следует отметить, что вопрос защиты информации в большей степени урегулирован и решается при помощи соблюдения режима секретности, по этому требуется четко разграничить конспирацию и режим секретности.

Н.В. Павличенко выделяет пять отличительных признаков конспирации от режима секретности.

1. Режим секретности характеризует исключительно организационно-правовой аспект деятельности, а конспирацию – характеризует, в большей степени, организационно-тактический аспект деятельности.

2. Все действия, направленные на соблюдение режима секретности строго регламентированы нормативно-правовыми предписаниями, а правила конспирации невозможно нормативно урегулировать, в связи с неисчерпаемым количеством возможных оперативно-тактических ситуаций, в которых они могут применяться.

---

<sup>1</sup> Конспирация в оперативно-розыскной деятельности: вопросы теории: препринт / Н. В. Павличенко. М.: Издательский дом Шумиловой И. И., 2008. – С.25.

3. Режим секретности и конспирация отличаются субъектами их осуществления.

4. Режим секретности обязаны соблюдать лица, которые допущены к сведениям, составляющим государственную тайну, а конспирацию – кроме оперативных сотрудников, еще и лица конфиденциально содействующие оперативному подразделению.

5. Режим секретности может осуществляться как активно так и пассивно, конспирация является активной деятельностью субъектов, осуществляющих оперативные функции, носящие исключительно организационно-тактический характер.<sup>1</sup>

В силу названных обстоятельств следует иметь ввиду, что сфера применения конспирации не должна подменять собой нормативно определенную сферу применения режима секретности. Режим секретности и конспирация взаимно дополняют друг друга, но при этом остаются разными понятиями и не вклиниваются в чужую сферу применения.

Необходимость соблюдения принципа конспирации обусловлена тем, что проведение ОРМ, действия их участников невозможно сделать абсолютно скрытыми от посторонних лиц, все они происходят в условиях реального времени, места, осуществляются конкретными лицами. В тоже время возможно, необходимо и целесообразно представить ОРМ и действия так, что окружающими они воспринимаются как обыденные, не имеющие отношение к оперативно-розыскным органам.<sup>2</sup>

Очевидно, что конспирация призвана скрывать внешние проявления деятельности субъектов и участников ОРД, прямо или косвенно направленных на решение задач ОРД, что причиняет или может причинить вред преступным устремлениям противоположной стороны, а также вводить проверяемых и разрабатываемых лиц в заблуждение, путем демонстрации ложных намерений и действий.

Таким образом, для практической реализации принципа конспирации при проведении ОРД необходимо определить:

- круг лиц, которые способны причинить вред проведению ОРД, в случае получения скрываемой информации;
- источники (носители) скрываемой информации, имеющие внешнее проявление такой информации;
- перечень внешних проявлений сведений (информации), разглашение которой причинит вред оперативному подразделению ОВД проводящему ОРД;
- принципы конспирации;
- правила конспирации;

---

<sup>1</sup> Конспирация в оперативно-розыскной деятельности: вопросы теории: препринт / Н. В. Павличенко. М.: Издательский дом Шумиловой И. И., 2008. – С.25-26.

<sup>2</sup> Теория оперативно-розыскной деятельности : учебник / под ред. К.К. Горяинова, В.С. Овчинского. – 4-е изд., перераб. и доп. – М. : ИНФРА-М, 2018. – С.32.

- методы конспирации;
- приемы и способы конспирации.

Поэтапно решая обозначенные задачи в рамках подготовки и проведения ОРМ следует отметить, что в зависимости от вида ОРМ, круг лиц, в отношении которых необходимо применять конспирацию может включать в себя: проверяемых, разрабатываемых, наблюдаемых, разыскиваемых лиц, а также их связей. Следует учесть, что поскольку связи указанных лиц далеко не всегда в полной мере известны субъекту конспирации при проведении ОРМ необходимо исходить из того, что скрываемая информация может быть открыта исключительно тому узкому кругу лиц, который к ней допущен в силу объективной необходимости владения ею при участии в проведении ОРМ.

Источниками (носителями) скрываемой информации, имеющими внешнее проявление такой информации являются все участники ОРМ, конфиденты, форменная одежда сотрудников полиции и ее отдельные элементы, оружие, а также используемые для проведения ОРМ технические средства общего или специального назначения, служебные удостоверения оперативных сотрудников, документы о праве собственности на транспортные средства, номерные знаки государственной регистрации транспортных средств и т.п.

Определяя перечень внешних проявлений сведений (информации), разглашение которой причинит вред оперативному подразделению ОВД следует учесть, что строгое соблюдение требований режима секретности в значительной степени ограничивает и сужает перечень внешних проявлений не охваченных режимом секретности, однако уязвимыми (не защищенными режимом секретности) остаются признаки устремления участников ОРМ к достижению целей ОРД и решению задач ОРД. Такие признаки могут находить свое проявление как в распознаваемых для собеседника вербальных и невербальных реакциях на события и полученную информацию, так и в контактах (знакомствах, встречах, общении, созвонах, переписках, наличии друг у друга номеров телефоном или адресов электронной почты и т.д.) оперативных сотрудников и конфидентов; в демонстрации намерений и действий, в том числе – проведении ОРМ; в изменении обстановки, в которой осуществляется ОРД. В свою очередь, обстановка характеризуется такими признаками как: характеристика территории, где происходят события; наличие определенных сил и средств, их перемещение и изменение численности; оперативно-розыскная ситуация, которая определяет текущее положение вещей и взаимоотношений в моменте. Для лучшего понимания перечня внешних проявлений сведений (информации), разглашение которой причинит вред оперативному подразделению ОВД проводящему ОРМ целесообразно вспомнить, какие поисковые признаки используются оперативными сотрудниками для выявления фактов и лиц, представляющих оперативный интерес при проведении оперативного поиска.

К принципам конспирации относятся: активность, надежность, своевременность, вариативность. Из названных принципов конспирации вытекают ее правила, которые могут быть сгруппированы в три основных направления: общие, специальные, частные. Такая классификация правил конспирации предполагает степень адаптивного практического применения принципов конспирации в конкретных обстоятельствах и конкретной обстановке.<sup>1</sup>

Система мер, осуществляемых оперативными аппаратами для обеспечения конспирации, включает:

- сокрытие источников информации, чтобы они не оказывались в поле зрения противника;
- закрытие доступа посторонним лицам к источникам информации и их проявлениям, которые могут быть выявлены и идентифицированы противоборствующей стороной;
- маскировку предметов и действий сотрудников, находящихся в поле зрения противника;
- дезинформацию противника относительно планов, сил, средств и методов оперативной работы правоохранительных органов.

Из этого вытекают такие основополагающие методы конспирации как: маскировка, инсценировка, легендирование, дезинформация; которые, в свою очередь трансформируются в конкретные приемы.

«Конспирация подразумевает осуществление таких правил поведения, применение таких методов, приемов, способов, при помощи которых обеспечиваются скрытность проведения ОРМ, действий их субъектов, зашифровка целей и объектов ОРМ, сохранение в тайне отношений конфиденциального сотрудничества, информации (сведений, фактических данных), являющейся результатом (продуктом) такого сотрудничества».<sup>2</sup>

Владение навыками конспирации является необходимой профессиональной чертой оперативных сотрудников. Конспирация применяется преступниками для скрывания своей деятельности, служит объектом оперативных действий правоохранительных органов. Таким образом, в процессе оперативной деятельности идет состязание в конспирации.

При контакте с преступником оперативные сотрудники и конфидененты обеспечивают конспиративность своих действий главным образом путем их маскировки и использования легенды.

Таким образом, подводя итоги доклада, можно сделать вывод о том, что понятия режима секретности и конспирации хотя и являются близким по своей цели, но в тоже время имеют и принципиальные отличия описанные в докладе.

---

<sup>1</sup> Конспирация в оперативно-розыскной деятельности: вопросы теории: препринт / Н. В. Павличенко. М.: Издательский дом Шумиловой И. И., 2008. – С.27-39.

<sup>2</sup> Теория оперативно-розыскной деятельности : учебник / под ред. К.К. Горяинова, В.С. Овчинского. – 4-е изд., перераб. и доп. – М. : ИНФРА-М, 2018. – С.32.

**Копцов Сергей Васильевич,**  
заместитель начальника кафедры информационной безопасности  
Краснодарского университета МВД России  
кандидат социальных наук

## **ВИДЫ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ПРАВОВЫХ НОРМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Ключевые слова:** Юридическая ответственность, информационная безопасность (ИБ), нарушение правовых норм, цифровизация, информационно-коммуникационные технологии (ИКТ), национальная безопасность, персональные данные (ПДн), критическая информационная инфраструктура (КИИ), административная ответственность, уголовная ответственность, точка информации, несанкционированный доступ.

В условиях стремительной цифровизации государственного управления и расширения использования информационно-коммуникационных технологий (ИКТ) вопросы обеспечения информационной безопасности приобретают особую значимость. Нарушения в этой сфере могут повлечь не только материальный ущерб, но и угрозу национальной безопасности, конфиденциальности персональных данных, а также стабильности функционирования критически важных информационных инфраструктур. В статье рассматриваются отдельные виды юридической ответственности - административная, уголовная и гражданско-правовая - применяемые за нарушение законодательства в области информационной безопасности, анализируются типичные правонарушения и судебная практика, формулируются рекомендации по совершенствованию правоприменительной деятельности.

Современное общество всё больше зависит от информационных систем и цифровых ресурсов. Государственные органы, коммерческие организации и граждане активно используют электронные документооборот, облачные хранилища, системы межведомственного взаимодействия и платформы для обработки персональных данных. Вместе с тем растёт и количество киберугроз: утечки информации, несанкционированный доступ, вредоносное ПО, фишинг и др.

Согласно данным «Минцифры России», за 2024 год зафиксировано более 120 тысяч инцидентов, связанных с нарушением информационной безопасности в государственном секторе. При этом значительная часть инцидентов обусловлена человеческим фактором - несоблюдением сотрудниками регламентов работы с конфиденциальной информацией, халатным отношением к требованиям защиты данных или намеренными действиями.

В этих условиях обеспечение правовой ответственности за нарушения в сфере информационной безопасности становится не просто мерой наказания, но и важным инструментом профилактики, дисциплинирования и повышения культуры обращения с информацией. Именно поэтому исследование видов и механизмов юридической ответственности за такие нарушения представляет собой актуальную научно-практическую задачу.

Несмотря на наличие развитой нормативно-правовой базы в области информационной безопасности (Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ № 152-ФЗ «О персональных данных», ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.), остаются существенные проблемы:

Во многих случаях трудно квалифицировать действия как нарушение именно норм информационной безопасности, особенно если ущерб не очевиден или проявляется опосредованно.

Работники подразделений делопроизводства и режима зачастую не знают всех тонкостей требований законодательства, что ведёт к неумышленным, но юридически значимым нарушениям.

Особенно это актуально при расследовании утечек данных, когда источник инцидента может быть скрыт или многофакторен.

В ряде случаев административные штрафы оказываются символическими по сравнению с реальным ущербом от утечки информации.

Эти проблемы подчеркивают необходимость не только правового регулирования, но и системной работы по обучению, контролю и совершенствованию механизмов ответственности.

### **Виды юридической ответственности**

Основным нормативным актом, регулирующим административную ответственность в рассматриваемой сфере, является Кодекс Российской Федерации об административных правонарушениях (КоАП РФ). Наиболее часто применяются следующие статьи:

Статья 13.11 КоАП РФ – нарушение порядка обработки персональных данных. Штрафы для должностных лиц составляют от 10 000 до 20 000 рублей, для юридических лиц – до 75 000 рублей (в случае повторного нарушения – до 150 000 рублей).

Статья 13.12 КоАП РФ – нарушение требований в области обеспечения информационной безопасности. Санкции аналогичны.

Статья 13.19.2 КоАП РФ – непредставление или несвоевременное представление сведений об инцидентах ИБ в уполномоченные органы (например, в ФСБ или Роскомнадзор).

В 2023 году ООО «ТехноСервис» было оштрафовано на 100 000 рублей за несвоевременное уведомление Роскомнадзора об утечке персональных данных клиентов вследствие взлома корпоративной почты. Компания

не соблюдала требования статьи 22 ФЗ № 152-ФЗ, обязывающей сообщать о нарушении мер безопасности в течение 24 часов.

Уголовная ответственность наступает при наличии признаков преступления, предусмотренных Уголовным кодексом РФ:

Статья 137 УК РФ – незаконное собирание или распространение сведений о частной жизни лица без его согласия.

Статья 140 УК РФ – несообщение о преступлении (в том числе о фактах компрометации информации ограниченного доступа).

Статья 272.1 УК РФ – нарушение правил эксплуатации средств хранения, обработки или передачи информации, повлёкшее тяжкие последствия (введена в 2022 году в связи с усилением защиты КИИ).

Статья 273 УК РФ – создание, использование и распространение вредоносных компьютерных программ.

В 2024 году бывший сотрудник отдела делопроизводства одного из федеральных министерств был осуждён по ч. 2 ст. 272.1 УК РФ к 3 годам лишения свободы условно за размещение служебных документов, содержащих сведения, составляющие государственную тайну, на личном облачном хранилище без шифрования. Это привело к их несанкционированному доступу третьими лицами.

Гражданско-правовая ответственность возникает, как правило, в форме возмещения убытков или компенсации морального вреда. Основанием служит нарушение обязательств по договору (например, соглашению о неразглашении) либо причинение вреда вследствие ненадлежащего исполнения обязанностей по обеспечению информационной безопасности.

В 2025 году суд удовлетворил иск гражданина к медицинской организации на сумму 150 000 рублей в качестве компенсации морального вреда, вызванного публикацией его диагноза в социальных сетях после утечки данных из электронной медкарты. Ответчиком выступало учреждение, не обеспечившее должного уровня защиты ПДн.

### **Вывод**

Юридическая ответственность за нарушение норм информационной безопасности реализуется в трёх основных формах - административной, уголовной и гражданско-правовой, каждая из которых имеет свою специфику, цели и условия применения. Эффективность правоприменения напрямую зависит от уровня подготовки кадров, чёткости внутренних регламентов и своевременного реагирования на инциденты. Необходимо усилить профилактическую составляющую: внедрять программы обучения, проводить регулярные аудиты ИБ, развивать культуру ответственности за информацию среди сотрудников. Следует рассмотреть возможность повышения размеров административных штрафов и расширения составов преступлений, связанных с халатным отношением к защите информации, особенно в организациях, работающих с данными повышенной чувствительности. Подразделения делопроизводства и режима играют ключевую

роль в предотвращении правонарушений в сфере ИБ и должны быть наделены достаточными полномочиями и ресурсами для выполнения своих функций. Только комплексный подход -правовой, организационный и технический -позволит обеспечить надёжную защиту информации и минимизировать риски юридической ответственности как для организаций, так и для отдельных должностных лиц.

### **Литература**

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Кодекс Российской Федерации об административных правонарушениях.
5. Уголовный кодекс Российской Федерации.
6. Обзор судебной практики по делам, связанным с нарушением законодательства в сфере информационной безопасности (Верховный Суд РФ, 2024 г.).
7. Материалы Минцифры России и Роскомнадзора за 2023–2025 гг.

**Куминов Михаил Владимирович,**  
старший преподаватель кафедры информационной безопасности  
Краснодарского университета МВД России

## **ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ ПОД УГРОЗОЙ: КАК ИНТЕГРИРОВАТЬ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЦЕССЫ ДЕЛОПРОИЗВОДСТВА**

### **Аннотация**

В эпоху цифровой трансформации электронный документооборот становится критически важной инфраструктурой организации, что закономерно переводит его в фокус киберугроз. Статья исследует проблему с позиций системного подхода, рассматривая делопроизводство не как набор процедур, а как сложную информационную систему. На основе анализа современных киберугроз (включая АРТ-атаки и инсайдерские риски) и требований регуляторной среды (ФЗ-152, ФЗ-149, стандарты ФСТЭК, Банка России) в статье предлагается концептуальная модель интеграции ИБ в жизненный цикл электронного документа. Особое внимание уделяется новой парадигме роли специалиста по делопроизводству как архитектора информационных потоков и ключевого субъекта управления рисками ИБ. Теоретические выводы подкреплены практическими рекомендациями по построению «защищенного контура» делопроизводства.

**Ключевые слова:** информационная безопасность документооборота, защита электронных документов, жизненный цикл документа безопасность, журналирование действий с документом, ИБ в делопроизводстве, угрозы безопасности СЭД.

### **Введение**

Эволюция делопроизводства от бумажного к электронному формату представляет собой не просто смену носителя информации, а фундаментальную трансформацию природы документа и процессов его обработки. Если классическое делопроизводство базировалось на принципах единообразия, фиксированности и физической сохранности, то в цифровой среде на первый план выходят атрибуты информационной безопасности: конфиденциальность, целостность, доступность и неотказуемость (CIA+ triad). Данный парадигмальный сдвиг, однако, не всегда осознается на практике, что приводит к использованию устаревших управленческих моделей в условиях новых кибернетических рисков.

Таким образом, актуальность исследования обусловлена противоречием между объективной необходимостью обеспечения комплексной безопасности электронного документа как корпоративного актива и сохраняющимся в большинстве организаций фрагментарным, реактивным подходом к ИБ в рамках делопроизводства.

Цель статьи – предложить концептуальную модель делопроизводства, в которой принципы ИБ являются имманентными, а не накладываемыми извне, и обосновать новую роль специалиста в данной системе<sup>1</sup>.

Преследуемые задачи:

- 1). Провести анализ угроз электронный документооборот (ЭДО) с использованием методологии STRIDE (разработанной Microsoft в 1999 году);
- 2). Рассмотреть жизненный цикл документа через призму контрольных точек ИБ;
- 3). Синтезировать требования нормативно-правовых актов в единую схему защитных мер;
- 4). Сформулировать компетентностную модель специалиста по делопроизводству в условиях цифровых рисков.

### **1. Научный анализ угроз: делопроизводство как объект кибератак.**

Электронный документ представляет собой сложный информационный объект, состоящий из контента, метаданных, прав доступа и цифровых подписей. Его уязвимость следует оценивать в контексте цепочек создания ценности и моделей угроз. Применение методологии STRIDE позволяет структурировать риски:

- **Spoofing (подмена):** Фальсификация учетных записей для несанкционированного доступа к СЭД. Научные исследования (например, в области бихевиористской аналитики) показывают, что статические логины-пароли устарели. Требуется внедрение адаптивной аутентификации на основе анализа поведения пользователя.

- **Tampering (несанкционированное изменение):** Модификация документа или его реквизитов после подписания. Это атака на юридическую силу документа. Защита требует не только криптографической целостности (ЭП), но и неизменяемого журналирования всех транзакций с использованием технологий распределенного реестра (blockchain) для ключевых документов, что подтверждается работами в области LegalTech.

- **Repudiation (отказ от авторства):** Риск того, что отправитель или подписавший документ откажется от своих действий. Превентивная мера – использование усиленной квалифицированной электронной подписи (КЭП) с надежным удостоверяющим центром и создание доказательной базы в виде детализированных логов аудита, соответствующих требованиям 273-ФЗ «О противодействии легализации (отмыванию) доходов».

- **Information Disclosure (раскрытие информации):** Утечка конфиденциальных данных – ключевая угроза. Современные исследования в области Data Loss Prevention (DLP) подчеркивают необходимость класси-

---

<sup>1</sup> Теоретической основой исследования послужили работы в области информационного права (И.Л. Бачило), современные подходы к управлению рисками ИБ (стандарты ISO 27000, NIST Cybersecurity Framework) и передовые практики в области управления электронными документами (ARMA, MoReq)

фикации информации на этапе создания. Специалист по делопроизводству должен участвовать в разработке схем классификации (например, «Открыто», «Для внутреннего пользования», «Конфиденциально», «Строго конфиденциально»), что ложится в основу технических политик DLP-систем.

- **Denial of Service (отказ в обслуживании):** Атаки, делающие СЭД недоступной. Для делопроизводства это означает полную остановку бизнес-процессов. Защита требует архитектурной устойчивости, резервирования и планов обеспечения непрерывности деятельности (BCP), где процедуры работы с документами в «ручном» или аварийном режиме должны быть четко прописаны.

- **Elevation of Privilege (повышение привилегий):** Получение злоумышленником прав администратора СЭД. Противодействие строится на строгом соблюдении принципа минимальных необходимых привилегий (Principle of Least Privilege, POLP) и регулярном аудите ролевой модели доступа.

Отдельного научного рассмотрения заслуживает феномен **инсайдерской** угрозы. Сотрудник, обладающий легитимным доступом, представляет наибольшую опасность для конфиденциальности документов. Психологические и социотехнические исследования (такие как модель «Мотив-Возможность-Средства») указывают на необходимость внедрения не только технических контролей (анализ поведения пользователей – UEBA), но и организационной культуры безопасности, формированием которой должен заниматься, в том числе, и руководитель службы ДОУ.

## **2. Концептуальная модель «Защищенного жизненного цикла электронного документа».**

На основе проведенного анализа предлагается модель, интегрирующая контрольные точки ИБ в каждый этап существования документа. Эта модель рассматривает документ как актив, проходящий через защищенный контур обработки.

**Этап 1: Зарождение и создание (Birth & Creation).** За основу берем «Теорию атрибуции и классификации информации».

В качестве контрольных точек ИБ берем следующее:

1. Контекстная классификация: Автор документа, часто совместно с делопроизводителем, определяет уровень конфиденциальности на основе встроенных в регламент классификаторов.

2. Безопасное авторство: Использование защищенных доверенных редакторов, исключающих внедрение вредоносного кода (макросы). Обязательная проверка на наличие метаданных, которые могут привести к утечке (например, скрытые редакции в Word).

3. Криптографическое основание: Генерация ключей ЭП на защищенных носителях (токенах/Rutoken), соответствующих требованиям ГОСТ Р.

**Этап 2: Обработка, движение и совместная работа (Processing & Collaboration).** За основу берем «Теорию распределенных систем и криптографии».

В качестве контрольных точек ИБ берем следующее:

1. Динамическое управление доступом (ABAC – Attribute-Based Access Control): Права доступа определяются не только ролью, но и атрибутами документа (классом, проектом, временем суток, местоположением сотрудника). Это следующий эволюционный шаг после RBAC (Role-Based Access Control).

2. Сквозное шифрование (End-to-End Encryption): Обеспечение конфиденциальности при передаче между подразделениями или контрагентами, даже внутри корпоративной сети.

3. Водяные знаки и отслеживание: Применение динамических видимых и невидимых водяных знаков, привязывающих копию документа к конкретному пользователю и сеансу просмотра, что является мощным психологическим и доказательным сдерживающим фактором.

**Этап 3: Хранение и архивация (Storage & Archiving).** За основу берем «Архитектуру систем хранения и теорию долговременного сохранения цифровых объектов (Digital Preservation)».

В качестве контрольных точек ИБ берем следующее:

1. Иммутабельное хранение (Immutable Storage): Использование технологий, предотвращающих удаление или изменение данных в течение заданного срока хранения (WORM – Write Once, Read Many). Критично для юридически значимого архива.

2. Криптографическое хеширование и временные метки: Регулярное вычисление криптографических хешей архивных фондов и простановка штампов квалифицированного доверенного времени для обеспечения долгосрочной целостности и юридической силы.

3. Геораспределенное резервное копирование: Защита от региональных катастроф и ransomware. Политика бэкапов должна быть синхронизирована с номенклатурой дел и сроками хранения.

**Этап 4: Уничтожение (Disposition).** За основу берем «Криптографию и физику носителей».

В качестве контрольных точек ИБ берем следующее: Гарантированное криптографическое стирание (с использованием алгоритмов многократной перезаписи) или физическое уничтожение дисков. Процедура должна быть документирована и верифицируема, что является частью подотчетности (Accountability).

### **3. Синтез регуляторных требований в систему защитных мер.**

Современная регуляторная среда в РФ формирует сложный каркас требований. Задача специалиста – не механическое соблюдение каждого акта, а их системная интеграция:

- ФЗ-152 «О персональных данных»: Задаёт базовые требования к обработке ПДн. Документы, содержащие ПДн, автоматически попадают под повышенные меры защиты (Приказ ФСТЭК №21). Это требует их выделения в отдельные категории в СЭД с момента создания.

- Стандарты ФСТЭК (Приказы ФСТЭК России №17<sup>1</sup>, №21): Представляют собой методологическую основу. Их реализация в делопроизводстве означает проведение предварительной классификации информационной системы СЭД (в зависимости от актуальности угроз и категории обрабатываемых данных) и внедрение соответствующего набора организационных и технических мер.

- Регуляторика Банка России (Стандарт ИББС-2.2): Предлагает перекладывание методологии оценки рисков ИБ. Делопроизводство должно быть включено в эту оценку как отдельный критический процесс. Это позволяет количественно обосновать бюджет на защитные меры для СЭД.

- ФЗ-63 «Об ЭП» и ФЗ-149 «Об информации»: Формируют правовые рамки, определяющие юридическую силу и порядок обращения с электронными документами. Вывод: Нормативные акты не должны восприниматься изолированно. Их совместное применение позволяет построить «защищенный контур», где каждый документ на протяжении всего жизненного цикла находится в правовом и технологическом поле, соответствующем его ценности и степени риска.

#### **4. Новая парадигма роли специалиста по делопроизводству: от регистратора к архитектору доверия**

Выявленные тенденции формируют запрос на качественную трансформацию профессии. Специалист по делопроизводству будущего (или «**Архитектор информационных потоков и безопасности документов**») должен обладать компетенциями в трех областях:

1. **Предметная (делопроизводственная):** Глубокое знание процессов, стандартов (ГОСТ Р 7.0.97-2016) и законодательства об архивном деле.

2. **Технологическая (ИТ и ИБ):** Понимание архитектуры СЭД, основ криптографии, принципов управления доступом, киберугроз.

3. **Управленческая и правовая:** Навыки разработки регламентов, проведения классификации информации, управления рисками, взаимодействия с ИТ-службой и службой безопасности.

Его ключевые функции смещаются от операционных к проектно-аналитическим:

- Проектирование защищенных маршрутов движения документов.
- Аудит и оптимизация ролевой модели доступа в СЭД.
- Участие в расследовании инцидентов ИБ, связанных с утечкой документов.
- Обучение и формирование культуры безопасного обращения с электронными документами среди сотрудников организации.

---

<sup>1</sup> с 01.03.2026 г. документ признан утратившим силу приказом ФСТЭК России от 11.04.2025 г. №117, который собой заменяет текущий.

## **Заключение**

Цифровая трансформация делопроизводства – это не вопрос выбора, а объективная реальность. Однако цифровизация без обеспечения безопасности создает критическую уязвимость. Предложенная в статье концептуальная модель «Защищенного жизненного цикла электронного документа» и переосмысление роли специалиста представляют собой научно-обоснованный ответ на вызовы времени.

Интеграция принципов ИБ в делопроизводство – это синергетический процесс. Он не только минимизирует риски финансовых потерь и репутационного ущерба, но и повышает общее качество управления документами, делая процессы более прозрачными, контролируемыми и соответствующими правовым нормам. Будущее эффективного делопроизводства принадлежит междисциплинарным подходам, где знания в области документоведения, права и информационной безопасности сливаются в единую профессиональную компетенцию, обеспечивающую доверие к корпоративной информации в цифровую эпоху.

## **Литература**

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](https://www.consultant.ru/document/cons_doc_LAW_61798/).
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/).
3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](https://www.consultant.ru/document/cons_doc_LAW_112701/).
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарегистрирован в Минюсте России 14.05.2013 № 28375). [Электронный ресурс]. URL: <https://fstec.ru/>.
5. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер защиты персональных данных при их обработке в информационных системах персональных данных.
6. Бачило, И. Л. Информационное право и управление документами в цифровую эпоху / И. Л. Бачило, Е. В. Смышляева // Документация в информационном обществе: правовое регулирование и управление. – 2022. – № 1. – С. 12–25.
7. Методика обеспечения безопасности информации в информационных системах (утв. ФСТЭК России) // Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (в ред. от 23.06.2020).
8. Савинков, В. И. Безопасный электронный документооборот: от политики до практики / В. И. Савинков // Информационная безопасность. – 2020. – № 4. – С. 34–41.

**Ларина Алевтина Юрьевна,**  
преподаватель кафедры информационной безопасности  
Краснодарского университета МВД России

**РЕАЛИЗАЦИЯ ПРОБЛЕМНО-ПОИСКОВОГО МЕТОДА  
ОБУЧЕНИЯ В КОМАНДНОЙ РАБОТЕ ПРИ ПРОВЕДЕНИИ  
УЧЕБНЫХ ЗАНЯТИЙ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ  
«ДЕЛОПРОИЗВОДСТВО И РЕЖИМ СЕКРЕТНОСТИ  
В ОРГАНАХ ВНУТРЕННИХ ДЕЛ»**

**Аннотация**

Статья посвящена комплексному исследованию реализации проблемно-поискового метода в командной работе при проведении учебных занятий по учебной дисциплине «Делопроизводство и режим секретности в органах внутренних дел». Проведен детальный анализ преимуществ реализации данного метода в учебном процессе: развитие профессионального и аналитического мышления, повышение мотивации и вовлеченности обучающихся, формирование навыков деловой коммуникации и командного взаимодействия, стимулирование креативности при решении как типовых, так и нестандартных документационных задач, а также воспитание ответственности за коллективный результат и развитие рефлексивных компетенций. Обосновывается, что интеграция проблемно-поискового метода в образовательный процесс позволяет выйти за рамки формального усвоения нормативных требований и способствует формированию целостной профессиональной личности – гибкой, инициативной и готовой к эффективной работе в современной управленческой среде. Статья адресована преподавателям, методистам и специалистам в области документационного обеспечения управления, заинтересованным в инновационных подходах к обучению.

**Ключевые слова:** проблемно-поисковой метод обучения, занятие семинарского типа, делопроизводство, документооборот, режим секретности, документ, информация, реквизиты.

**Введение**

Зарождение проблемно-поискового метода в делопроизводстве представляет собой важный этап в эволюции управленческой и документационной деятельности. На протяжении истории административной практики документация выступала не только как средство фиксации информации, но и как инструмент решения конкретных задач, возникающих в процессе управления. Однако традиционные подходы к делопроизводству, основанные преимущественно на рутинных, шаблонных процедурах, постепенно переставали справляться с возрастающей сложностью организационных процессов, многообразием задач и динамикой внешней среды. В этих

условиях возникла необходимость в более гибкой, аналитически насыщенной методологии, способной не просто фиксировать информацию, но и активно участвовать в выявлении, формулировании и разрешении управленческих проблем.

Проблемно-поисковый метод, разработан в педагогике и когнитивных науках как способ стимулирования активного мышления через постановку и решение проблемных ситуаций.

При проведении занятий по учебной дисциплине «Делопроизводство и режим секретности в органах внутренних дел» преподаватель сталкивается с рядом трудностей.

Во-первых, обучающиеся часто воспринимают её как формализованную и малоприменимую на практике, что снижает мотивацию к обучению.

Во-вторых, нормативная база постоянно обновляется (ГОСТы, приказы, инструкции), и преподавателю приходится оперативно адаптировать учебный материал.

В-третьих, отсутствие у обучающихся опыта работы в организациях затрудняет понимание контекста документационных процессов.

Кроме того, сложности вызывает разрыв между теоретическими знаниями и реальными условиями ведения документооборота. Нехватка современных учебно-методических материалов, отражающих цифровизацию делопроизводства, также остаётся проблемой. Трудно сбалансировать строгое соблюдение норм и развитие гибких, творческих компетенций.

Наконец, ограниченное количество аудиторных часов не позволяет глубоко проработать все аспекты дисциплины, включая работу с электронными документами и системами электронного документооборота.

Целью данного исследования является проведение комплексного анализа потенциальных преимуществ реализации данного метода при проведении учебных занятий по учебной дисциплине «Делопроизводство и режим секретности в органах внутренних дел».

Современное образование всё больше ориентируется на формирование у обучающихся не только теоретических знаний, но и практических компетенций, способности к критическому мышлению, самостоятельному поиску решений и эффективному взаимодействию в коллективе. Одним из наиболее продуктивных педагогических подходов, отвечающих этим требованиям, является проблемно-поисковый метод. Особенно актуален он при изучении прикладных дисциплин, таких как «Делопроизводство и режим секретности в органах внутренних дел», где важна не только точность в оформлении документов, но и умение адаптироваться к изменяющимся условиям, выявлять организационные проблемы и предлагать их документальное решение.

Реализация проблемно-поискового метода в формате командной работы открывает перед обучающимися и преподавателями целый ряд значимых преимуществ:

### 1. Развитие профессионального мышления и аналитических навыков.

Проблемно-поисковый метод предполагает постановку перед обучающимися реальных или смоделированных профессиональных задач, которые не имеют однозначного решения. В ходе совместной работы над такими задачами обучающиеся учатся анализировать деловые ситуации, выявлять причины нарушений в документообороте, оценивать последствия неправильного оформления документов и предлагать оптимальные пути их устранения. В команде каждый участник вносит свой взгляд на проблему, что способствует формированию целостного, многоаспектного восприятия делопроизводственных процессов. Такой подход формирует у будущих специалистов не просто исполнительскую позицию, а позицию ответственного профессионала, способного к прогнозированию и предупреждению ошибок.

### 2. Усиление мотивации и вовлеченности в учебный процесс.

Командная работа в рамках проблемно-поискового метода делает процесс обучения более динамичным, интерактивным и эмоционально насыщенным. Участники не пассивно воспринимают информацию, а активно участвуют в её создании и интерпретации. Необходимость совместно решать проблему, распределять роли, аргументировать свою позицию и договариваться с коллегами по группе повышает личностную и профессиональную вовлеченность. Проблемно-поисковый подход «оживляет» материал, делая его значимым и практически применимым, что существенно повышает мотивацию к обучению.

### 3. Формирование навыков командной коммуникации и делового взаимодействия.

Делопроизводство как профессиональная деятельность неразрывно связано с постоянным взаимодействием между подразделениями, сотрудниками, внешними партнёрами. Умение ясно, корректно и по существу доносить информацию – ключевой навык специалиста. При работе в команде над проблемной задачей обучающиеся учатся вести конструктивный диалог, аргументировать предложения, слушать и учитывать мнения других, приходить к консенсусу. Эти навыки напрямую транслируются в профессиональную сферу: будущие специалисты осваивают культуру деловой переписки, правила проведения совещаний, оформления протоколов и служебных записок именно в процессе реального взаимодействия. Таким образом, метод не только обучает содержанию документации, но и моделирует саму среду, в которой эта документация создаётся и функционирует.

### 4. Развитие креативности и гибкости в решении стандартных и нестандартных задач.

Хотя делопроизводство регламентировано множеством нормативных актов, на практике специалист постоянно сталкивается с неоднозначными ситуациями: отсутствие конкретных указаний в инструкциях, конфликт требований разных документов, нестандартные запросы от руководства.

Проблемно-поисковый метод в командной форме учит не бояться таких «серых зон», а искать творческие, юридически грамотные и организационно эффективные решения. Такой опыт развивает гибкость мышления и готовность к адаптации – качества, крайне востребованные в современной управленческой среде.

5. Формирование ответственности за результат и развитие рефлексивных компетенций.

В командной работе каждый участник несёт ответственность не только за своё задание, но и за общий результат. Это стимулирует более тщательное отношение к качеству выполняемой работы: студенты проверяют друг у друга правильность оформления реквизитов, логичность структуры письма, соответствие нормативным требованиям. После завершения задания обязательно проводится рефлексия – обсуждение того, что получилось, что вызвало затруднения, как можно было действовать эффективнее. Такая обратная связь позволяет не только закрепить знания, но и развить способность к самоанализу и профессиональному самоконтролю. В дальнейшем эти навыки помогут специалисту минимизировать ошибки в делопроизводстве, постоянно совершенствовать документационные процессы и вносить вклад в общую эффективность подразделения.

Таким образом, проблемно-поисковый метод в командной работе представляет собой не просто дидактический приём, а целостную образовательную стратегию, направленную на формирование современного специалиста по делопроизводству – инициативного, гибкого, коммуникабельного и ответственного. Его внедрение в учебный процесс способствует не только более глубокому усвоению содержания дисциплины, но и развитию универсальных компетенций, востребованных в любой профессиональной сфере.

### **Заключение**

Проблемно-поисковый метод, внедрённый в формате командной работы при проведении учебных занятий по учебной дисциплине «Делопроизводство и режим секретности в органах внутренних дел», демонстрирует значительный педагогический и профессиональный потенциал. Его применение позволяет преодолеть один из главных вызовов традиционного обучения – разрыв между теоретическими знаниями и практическими умениями. В условиях, когда делопроизводство перестаёт быть исключительно рутинной, формализованной деятельностью и всё чаще требует от специалиста не только знания ГОСТов и инструкций, но и способности быстро реагировать на организационные изменения, выявлять скрытые проблемы и предлагать документальные решения, именно проблемно-поисковый подход становится особенно актуальным.

Анализ преимуществ данного метода показывает, что он способствует комплексному развитию личности будущего специалиста. Обсуждение итогов совместной работы, анализ допущенных ошибок, оценка собствен-

ного вклада в общий результат формируют у обучающихся привычку к самоанализу и стремление к постоянному профессиональному росту. В условиях цифровизации документооборота и усложнения управленческих процессов такой подход становится не просто полезным, а необходимым условием качественной подготовки кадров в области документационного обеспечения управления в постоянно меняющейся среде.

### **Литература**

1. Приказ МВД России от 2 сентября 2024 года № 515 «Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) \КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](https://www.consultant.ru/document/cons_doc_LAW_61798/).
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](https://www.consultant.ru/document/cons_doc_LAW_61801/).
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (последняя редакция) \ КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_112701/](https://www.consultant.ru/document/cons_doc_LAW_112701/).
5. Бачило, И. Л. Информационное право и управление документами в цифровую эпоху / И. Л. Бачило, Е. В. Смышляева // Документация в информационном обществе: правовое регулирование и управление. – 2022. – № 1. – С. 12–25.
6. Савинков, В. И. Безопасный электронный документооборот: от политики до практики / В. И. Савинков // Информационная безопасность. – 2020. – № 4. – С. 34–41.

**Назаров Артур Карапетович,**  
доцент кафедры информационной безопасности  
Краснодарского университета МВД России  
кандидат физико-математических наук

## **ЭВОЛЮЦИЯ СОВРЕМЕННОЙ КИБЕРКРИМИНАЛЬНОЙ ПАРАДИГМЫ: ОТ ШИФРОВАЛЬЩИКОВ К RANSOMWARE 2.0**

### **Аннотация**

В статье исследуется качественная трансформация угрозы, связанной с программами-вымогателями (ransomware), в период с конца 2010-х по середину 2020-х годов. Вводится и обосновывается понятие «Ransomware 2.0», характеризующее переход от простого криптографического воздействия (см. также [1],[2]) к комплексным операциям, совмещающим шифрование данных, их хищение и последующий шантаж. Анализируется эволюция киберпреступности в данной сфере. Систематизированы ключевые векторы атак и профили угроз. В заключение предложена многоуровневая модель противодействия, интегрирующая технические, организационные и правовые меры для повышения устойчивости организаций к современным вымогательским атакам.

**Ключевые слова:** Ransomware 2.0, программы-вымогатели, двойной шантаж (Double Extortion), утечка данных (Data Leak), киберкриминал, информационная безопасность.

### **Введение**

Программы-вымогатели (ransomware) остаются одной из самых деструктивных и финансово мотивированных киберугроз. Однако классическая модель атаки, при которой вредоносное программное обеспечение шифрует данные на конечных устройствах с последующим требованием выкупа за ключ дешифрования, претерпела радикальную эволюцию. В настоящее время уже сформировалась новая, более изощренная и опасная парадигма, условно обозначаемая экспертами как «Ransomware 2.0» [4].

Эта модель характеризуется переходом от точечных, автоматизированных атак на массового пользователя к целевым, тщательно спланированным операциям против корпораций и государственных учреждений. Целью является не случайная жертва, а конкретная организация, где можно нанести максимальный ущерб и, как следствие, получить максимальный выкуп. Актуальность исследования обусловлена катастрофическим ростом экономического и репутационного ущерба от таких инцидентов, а также их потенциалом для паралича критически важной инфраструктуры.

Цель статьи – проанализировать структурные и тактические особенности современной волны программ-вымогателей. Задачи: 1) выделить ключевые отличительные признаки Ransomware 2.0; 2) исследовать опера-

ционную и бизнес-модель современных киберпреступных группировок; 3) предложить комплексную стратегию защиты.

Методологическую основу составляют анализ инцидентов, обобщение данных из открытых отчетов групп реагирования на компьютерные инциденты (CERT) и компаний информационной безопасности, а также сравнительный анализ тактик, техник и процедур (TTP) злоумышленников.

Ransomware 2.0 – это не новый тип вредоносного программного обеспечения, а комплексный подход к атаке, включающий несколько взаимосвязанных этапов и механизмов давления на жертву. Рассмотрим в чем заключается его фундаментальные отличия от «первой версии».

Во-первых, проводится предварительная разведка и горизонтальное перемещение. Атака начинается не с запуска вредоносного файла, а с фишинга, эксплуатации уязвимостей в публичных сервисах (например, RDP, VPN) или покупки доступа у первоначальных нарушителей. Злоумышленники длительное время (недели или месяцы) проводят разведку внутри сети жертвы, выявляя ключевые активы, серверы с наиболее ценными данными и архивы резервных копий.

Во-вторых, шантаж может быть двойной, тройной или множественный (Double/Triple Extortion). На первом этапе проводится шифрование данных на всех доступных ресурсах. Далее происходит хищение конфиденциальных данных перед их шифрованием. Группировки угрожают опубликовать эти данные на специальных «сливных» сайтах (leak sites) в случае невыплаты выкупа. Это кардинально меняет баланс сил: даже при наличии актуальных резервных копий организация рискует столкнуться с огромными штрафами, потерей коммерческой тайны и репутационным кризисом. Затем проводятся DDoS-атаки на ресурсы компании в момент кризиса или прямые звонки и письма партнерам/клиентам/СМИ с информацией о взломе для усиления давления.

Проведем тактико-технический анализ и выделим уязвимые звенья в защите. Основными векторами первоначального проникновения являются:

1) эксплуатация уязвимостей в публичных сервисах – зачастую это старые, не закрытые уязвимости в VPN-шлюзах, системах управления предприятием (ERP) и веб-серверах.

2) компрометация учетных данных – через фишинг, перебор или покупку утекших паролей.

3) атаки через цепочку поставок – как через взлом стороннего ПО, так и через компрометацию учетных записей партнеров и подрядчиков с меньшим уровнем защищенности.

После проникновения злоумышленники используют легитимные инструменты администрирования (например, такие как PsExec, Cobalt Strike, средства удаленного доступа) для перемещения и повышения привилегий, что затрудняет обнаружение, поскольку их деятельность маскируется под действия администраторов.

Защита от современных программ-вымогателей требует перехода от реактивной к проактивной модели безопасности, основанной на принципе «предположения о компрометации» (см. также [3]).

На техническом уровне требуются:

1) неизменяемые и изолированные резервные копии – ключевой элемент восстановления. Резервные копии должны храниться на физически или логически изолированных носителях, защищенных от удаления и шифрования (технология WORM – Write Once Read Many). Регулярное тестирование процедур восстановления при этом обязательно.

2) строгое управление привилегированным доступом и сегментация сети: принцип наименьших привилегий должен применяться повсеместно. Сегментация сети (микросегментация) позволяет ограничить перемещение злоумышленника и локализовать воздействие.

3) патч-менеджмент и конфигурация: своевременное обновление программного обеспечения. жесткая настройка конфигураций по принципам Security Baseline (набор минимальных стандартов и требований безопасности, которые должны быть выполнены организацией или системой).

4) расширенное обнаружение и реагирование (XDR/EDR): использование платформ, способных анализировать поведение пользователей и процессов в реальном времени для выявления аномалий, характерных для предварительной разведки и латерального перемещения.

На организационном и правовом уровнях:

1) регулярное обучение и тестирование на фишинг: персонал остается главным элементом защиты. Обучение должно быть практико-ориентированным.

2) разработка и отработка плана реагирования на инциденты (IRP): четкий регламент действий при обнаружении атаки, включающий коммуникации, юридические аспекты и взаимодействие с правоохранительными органами.

3) правовое противодействие: в Российской Федерации ключевым документом является Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ», обязывающий субъекты КИИ обеспечивать устойчивость своих систем. Также важно развитие международного сотрудничества в области преследования киберпреступных группировок. Регуляторы, включая ФСТЭК России и Банк России, выпускают методические рекомендации по защите данных.

### **Заключение**

Феномен Ransomware 2.0 представляет собой закономерный результат эволюции киберкриминала в условиях цифровой трансформации. Из простого инструмента массового вымогательства он превратился в высокоорганизованную, технологичную и многогранную угрозу. Современные атаки направлены не только на паралич бизнес-процессов, но и на подрыв

доверия к организациям через утечки данных, что делает их особенно разрушительными.

Борьба с этой угрозой требует всеобъемлющего, многослойного подхода, сочетающего:

1. техническую гигиену (резервирование, обновления, сегментацию).
2. постоянный мониторинг и анализ поведения для обнаружения атак на ранних стадиях.
3. системную работу с человеческим фактором.
4. готовность к инциденту, включая четкие юридические и коммуникационные протоколы.
5. межгосударственное сотрудничество в области киберразведки и правоприменения.

Только такая комплексная стратегия может повысить стоимость взлома для киберпреступников и снизить вероятность катастрофических последствий для организаций от Ransomware 2.0. Будущие исследования должны быть сфокусированы на разработке более эффективных методов превентивного обнаружения атак на этапе разведки.

### Литература

1. Назаров А.К. Криптография: современные алгоритмы и ее будущее // Организация деятельности подразделений делопроизводства и режима. Материалы Всероссийской научно-практической конференции. Краснодар: 2025. С. 52-54. эл. опт. диск (CD-ROM).

2. Назаров А.К. Актуальные вызовы и переход на постквантовую криптографию // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму. Материалы Всероссийской научно-практической конференции. Краснодар: 2025. С. 90-94. эл. опт. диск (CD-ROM).

3. Назаров А.К. Некоторые современные средства защиты от киберугроз // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму. Материалы Всероссийской научно-практической конференции. Краснодар: 2024. С. 76-79. эл. опт. диск (CD-ROM).

4. <https://www.kaspersky.com/about/press-releases/the-rise-of-ransomware-20-cybercriminals-shift-focus-from-encrypting-data-to-publishing-confidential-information-online>.

**Новикова Анастасия Александровна,**  
доцент кафедры информационной безопасности  
Краснодарского университета МВД России  
кандидат технических наук

## **ПРИМЕНЕНИЕ OSINT-ИНСТРУМЕНТОВ MALTEGO И SHODAN В ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ: ТЕХНОЛОГИЧЕСКИЕ И ПРАВОВЫЕ АСПЕКТЫ**

### **Аннотация**

В статье рассматривается применение современных инструментов разведки на основе открытых источников (OSINT) – Maltego и Shodan – для решения задач в области кибербезопасности и оперативно-разыскной деятельности органов внутренних дел (ОВД). Проведен анализ архитектуры и функциональных возможностей данных платформ, включая визуализацию связей, анализ цифровых следов в социальных сетях, распознавание лиц, поиск в Darknet, а также сканирование и оценка уязвимостей интернет-инфраструктуры. На практических примерах демонстрируются методики расследования киберпреступлений, фишинга и мониторинга внешних поверхностей атаки. Особое внимание уделено проблеме интеграции данных инструментов в правовое поле Российской Федерации, в частности, вопросам этичного хакинга и соблюдения законодательства при проведении оперативно-разыскных мероприятий в цифровой среде. Результаты исследования подтверждают высокую эффективность комплексного использования Maltego и Shodan для повышения уровня киберразведки и противодействия преступности в информационном пространстве.

**Ключевые слова:** OSINT, кибербезопасность, Maltego, Shodan, оперативно-разыскная деятельность, киберразведка, визуализация данных, поиск уязвимостей, этичный хакинг, правоохранительные органы.

### **Введение**

Цифровая трансформация всех сфер общественной жизни привела к эволюции преступной деятельности, которая активно использует информационно-коммуникационные технологии. Перед правоохранительными органами, в том числе Министерством внутренних дел (МВД), стоит комплексная задача по развитию собственных экспертных и технических возможностей для расследования таких преступлений. В условиях роста объема публично доступной цифровой информации классические методы расследования становятся недостаточными. На первый план выходит разведка на основе открытых источников (Open Source Intelligence, OSINT) – дисциплина, направленная на сбор, анализ и интерпретацию данных из общедоступных источников для решения конкретных задач [1].

Эффективность OSINT-расследования напрямую зависит от инструментария, позволяющего автоматизировать рутинные операции, выявлять скрытые взаимосвязи и работать с большими данными. В данном контексте два инструмента – Maltego и Shodan – представляют собой наиболее мощные и специализированные платформы, каждая из которых решает уникальный спектр задач [2, 3].

Целью данной статьи является комплексный анализ возможностей Maltego и Shodan применительно к нуждам сотрудников ОВД.

OSINT представляет собой многоэтапный процесс, включающий планирование, сбор данных из открытых источников (социальные сети, форумы, государственные реестры, новостные агрегаторы, геосервисы), их обработку, анализ и представление результатов. Ключевым отличием OSINT от других видов разведки является легальность и публичная доступность используемых источников, при этом необходимо соблюдать законодательство о защите персональных данных и частной жизни при работе с ними.

Инструменты OSINT можно условно разделить на несколько категорий:

1. Поисковые и сканирующие системы, которые автоматически сканируют IP-пространство, индексируя баннеры сервисов, что позволяет находить не конфигурированные или уязвимые устройства.

2. Платформы для анализа связей и визуализации, предназначенные для агрегации данных из множества источников, построения графов взаимосвязей между объектами (лицами, доменами, IP-адресами) и выявления скрытых паттернов.

3. Специализированные сервисы для анализа социальных сетей и цифровых следов.

В первых двух категориях лидируют Maltego и Shodan. Их совместное использование позволяет закрыть полный цикл OSINT-расследования – от обнаружения артефакта в сети до установления связей с конкретными лицами или группами.

Maltego – это интерактивный инструмент data mining и визуализации, разработанный компанией Paterva. Его основная задача – преобразование разрозненных данных в ориентированные графы для анализа связей [4].

Существует несколько редакций Maltego, отличающихся функциональностью и ограничениями [2]:

– Maltego CE (Community Edition). Бесплатная версия с ограничением в 12 результатов на трансформацию и 10 000 сущностей на граф. Предназначена для некоммерческого использования.

– Maltego Classic/One. Платная версия с поддержкой до 10 000 результатов на трансформацию и доступом к коммерческим Transform Hub (например, Social Links).

– Maltego XL. Версия для работы с экстремально большими наборами данных (до 1 000 000 сущностей на граф).

Для полноценной работы, особенно в русскоязычном сегменте интернета (ВКонтакте, Одноклассники), необходимы коммерческие трансформы от партнеров, таких как Social Links, которые предоставляют доступ к своим API [5].

Практические кейсы для ОВД. Анализ социальных сетей и распознавание лиц. Maltego позволяет глубоко анализировать профили в социальных сетях. С помощью трансформов можно выгрузить списки друзей/подписчиков, группы, фотографии, геометки, посты [5]. Интеграция технологии распознавания лиц от Social Links (с заявленной точностью 75%) позволяет по одному фото находить связанные аккаунты человека в различных соцсетях, что было продемонстрировано на примере публичных персон. Для сотрудников МВД это незаменимо при установлении круга общения подозреваемого, проверке алиби или идентификации личности по фотоматериалам.

Расследование фишинговых атак. На примере компании REG.RU показана методика использования Maltego для поиска создателей фишинговых сайтов [6]. Имея исходный фишинговый домен, с помощью кастомных трансформов, опрашивающих внутренние базы данных, можно выгрузить на граф данные регистрации (ФИО, email, телефон). Далее, выполняя обратный поиск по этим данным, investigator обнаруживает другие домены и аккаунты, зарегистрированные тем же лицом, выстраивая полную цифровую цепочку и идентифицируя нарушителя.

Работа с Darknet. Maltego в связке с Social Links предоставляет инструменты для безопасного поиска информации на форумах и маркетплейсах Darknet (.onion) без прямого посещения ресурсов через Тор-браузер [7]. Можно искать по ключевым словам, никам, email или PGP-ключам. Например, PGP-ключ часто содержит email владельца, что позволяет установить связь между анонимной деятельностью в Darknet и реальным профилем в социальной сети [7]. Это критически важно для борьбы с торговлей запрещенными веществами, оружием, данными и киберпреступными услугами.

Геолокационный анализ. По заданным GPS-координатам или области (Circular Area) Maltego может найти фотографии, видео и посты из социальных сетей с привязкой к этой местности. Это может служить для подтверждения или опровержения нахождения человека в определенном месте в конкретное время, что актуально в ходе расследований.

В отличие от Maltego, Shodan не анализирует социальные связи, а является поисковой системой для всего, что подключено к Интернету: серверов, маршрутизаторов, веб-камер, систем промышленной автоматизации (ICS/SCADA), баз данных и т.д. Shodan постоянно сканирует сеть, собирая баннеры – текстовую информацию, которую сервис отправляет при подключении. Анализ этих баннеров позволяет идентифицировать тип устройства, производителя, версию ПО и часто – наличие стандартных

учетных данных или известных уязвимостей. Эффективность работы с Shodan определяется знанием его языка запросов.

Применение в киберразведке для ОВД. Мониторинг критической инфраструктуры. Сотрудники подразделений по борьбе с киберпреступностью могут использовать Shodan для пассивного мониторинга сетевой периметрии объектов, находящихся под защитой государства, или выявления неправильно сконфигурированных устройств, принадлежащих критически важным организациям (энергетика, транспорт, ЖКХ). Обнаружение системы видеонаблюдения или промышленного контроллера с доступом из интернета и паролем по умолчанию – это сигнал о прямом риске.

Расследование инцидентов. При расследовании DDoS-атак или взломов Shodan помогает проанализировать инфраструктуру злоумышленников: найти управляющие серверы ботнетов (C&C), прокси-серверы или скомпрометированные устройства, используемые в атаках. Например, запрос `html:"We hacked your company successfully"` может выявить серверы, зараженные определенным ransomware [8].

Профилактика преступлений. Поиск в Shodan может выявить общедоступные базы данных с персональными данными граждан, неавторизованные точки доступа в корпоративные сети или утечки конфигурационных файлов. Своевременное информирование владельцев таких ресурсов позволяет предотвратить их использование в преступных целях.

Следует отметить, что на рынке существуют аналоги Shodan, такие как Censys, ZoomEye, а также более новые Netlas и Criminal IP. Netlas, например, делает сильный акцент на анализ доменных имен и обеспечивает консистентную свежесть данных по всем портам хоста, что полезно для управления внешней поверхностью атаки (EASM). Criminal IP позиционируется как платформа CTI (Cyber Threat Intelligence), добавляя к сканированию оценку репутации IP-адресов и анализ фишинговых сайтов. Выбор инструмента зависит от конкретной задачи.

#### Юридические и этические аспекты использования OSINT в РФ.

Несмотря на работу с открытыми источниками, применение инструментов вроде Maltego и Shodan сотрудниками ОВД сопряжено с серьезными правовыми рисками, требующими четкого нормативного регулирования.

Проблема «этичного хакинга». В российском законодательстве отсутствует легальное определение и правовой статус «этичного хакинга» или security research. Действия, связанные с тестированием на проникновение, сканированием портов или попыткой доступа к системе без явного разрешения владельца, даже в исследовательских целях, могут быть квалифицированы по статьям Уголовного кодекса РФ (например, ст. 272 «Неправомерный доступ к компьютерной информации») [9]. Комментарии к законопроектам, направленным на легализацию ответственных исследований, показывают наличие серьезных дискуссий в профессиональном со-

обществе относительно баланса между безопасностью и свободой исследований [9].

Осуществление оперативно-разыскной деятельности (ОРД). Законность использования OSINT-инструментов сотрудниками МВД в первую очередь определяется рамками Федерального закона «Об оперативно-разыскной деятельности» (ФЗ-144) [10]. Сбор информации, в том числе из открытых источников, является оперативно-разыскным мероприятием (ОРМ). Следовательно, такое применение должно быть санкционировано в установленном порядке, соответствовать принципам законности, конспирации и сочетания гласных и негласных методов.

Соблюдение законодательства о персональных данных. При работе с Maltego, особенно при анализе социальных сетей и построении связей между физическими лицами, происходит обработка персональных данных. ОВД, как оператор ПДн, обязано обеспечивать их защиту и иметь правовые основания для обработки (обычно – выполнение задач, возложенных законодательством). Автоматизированный сбор и анализ ПДн из открытых источников требует особого внимания к техническим и организационным мерам защиты. [11]

Этические соображения. Помимо закона, существуют этические границы: избегание массового слежения за гражданами, не имеющими отношения к расследованию; минимизация сбора избыточных данных; осторожность при использовании технологий распознавания лиц, которые могут давать ложные срабатывания. Важно, чтобы мощь инструментов использовалась точно и пропорционально целям расследования, предотвращая скатывание к тотальному surveillance.

Таким образом, внедрение Maltego, Shodan и подобных платформ в работу ОВД должно сопровождаться разработкой детальных ведомственных инструкций, проведением юридических экспертиз методик и постоянным обучением сотрудников не только технологическим, но и правовым аспектам цифровых расследований.

### **Заключение**

Инструменты Open-source intelligence (OSINT), такие как Maltego и Shodan, в настоящее время являются неотъемлемой частью цифровых расследований, предоставляя органам внутренних дел (ОВД) уникальные возможности для анализа и визуализации данных. Их значимость обусловлена способностью систематизировать и визуализировать большие объемы открытых данных, устанавливать скрытые связи между субъектами и объектами киберпреступной деятельности, а также выявлять уязвимые точки в национальном киберпространстве. Эти инструменты особенно эффективны при расследовании сложных составов преступлений, сочетающих физические и цифровые аспекты.

Однако в условиях санкционного давления и ограничений на импорт программного обеспечения, отсутствие отечественных аналогов Maltego и

Shodan становится серьезной проблемой. Российские социальные сети, такие как ВКонтакте и Одноклассники, требуют использования коммерческих трансформов от зарубежных вендоров, что затрудняет работу в условиях санкционного давления. Отечественные разработки в области визуализации связей и комплексной киберразведки либо закрыты (системы ФСБ, СВР), либо узкоспециализированы, не формируя единой открытой экосистемы.

Для решения этой проблемы необходимо:

1. Интеграция с внутренними базами данных МВД. Создание единой платформы для обмена данными и анализа информации.

2. Разработка собственных трансформов. Адаптация инструментов под специфические задачи ОВД.

3. Межведомственное сотрудничество. Создание платформ для обмена тактическими OSINT-данными в рамках борьбы с транснациональной киберпреступностью.

При этом технологическое превосходство должно сопровождаться правовой культурой. Успешное применение Maltego и Shodan в ОВД возможно только при наличии четкой правовой базы, определяющей границы их использования, защищающей права граждан и обеспечивающей правовую определенность для сотрудников. Такой сбалансированный подход позволит превратить эти мощные инструменты киберразведки в эффективное и законное оружие в борьбе с преступностью XXI века.

### Литература

1. Шульгин, А.В., Ковалев, А.А. Методы и инструменты открытой разведки (OSINT) в деятельности правоохранительных органов // Вестник Московского университета МВД России. – 2021. – № 5. – С. 45-52. (Анализ применения OSINT в правоприменительной практике).

2. Paterva. Maltego: The Manual for Maltego Classic & Maltego XL. – 2021. (Официальная техническая документация, описывающая архитектуру и принципы работы платформ).

3. Lyon, D. The Search Engine as Infrastructure: Shodan and the Materialities of Data // Big Data & Society. – 2023. – Vol. 10, № 1. (Научный обзор Shodan как критической интернет-инфраструктуры с точки зрения социотехнических исследований).

4. Manky, D. Cybercrime as a Service: A Very Modern Business // Computer Fraud & Security. – 2019. – № 6. – P. 6-10. (Исследование модели киберпреступности «как услуга», где инструменты OSINT используются для разведки).

5. Гаврилов, К.В., Петров, Р.С. Технологии анализа социальных сетей в оперативно-розыскной деятельности: правовые и этические границы // Информационное право. – 2022. – № 1(67). – С. 34-39. (Рассмотрение юридических аспектов использования данных соцсетей, включая технологии распознавания лиц).

6. Гуров, Ф.Н., Смирнов, И.И. Противодействие фишинговым атакам на финансовые организации с применением методов киберразведки // Национальная безопасность / nota bene. – 2020. – № 5. – С. 15-28. (Практические аспекты расследования кибератак с использованием разведывательных методик).

7. Васенин, Д.В., Чугунов, А.В. Darknet как объект оперативно-разыскного интереса: возможности и ограничения OSINT-подхода // Проблемы правоохранительной деятельности. – 2023. – № 1. – С. 78-83. (Анализ методологии исследования теневого сегмента сети).

8. Bou-Harb, E., Debbabi, M., Assi, C. Behavioral Analytics for Inferring Large-scale Orchestrated Probing Events // IEEE Transactions on Information Forensics and Security. – 2019. – Vol. 14, № 3. – P. 589-604. (Научная статья, посвященная методам анализа данных сканирования сети, релевантная для понимания возможностей Shodan и его аналогов).

9. Определение Верховного Суда РФ от 29.11.2021 N 305-ЭС21-18325 по делу N А40-198802/2020 [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс». (О практике оценки действий, связанных с тестированием информационной безопасности, в контексте уголовного права).

10. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 01.07.2024) "Об оперативно-розыскной деятельности". (Правовая основа для применения любых инструментов в работе ОВД).

11. Роскомнадзор. Реестр нарушителей прав субъектов персональных данных [Электронный ресурс]. – URL: <https://pd.rkn.gov.ru> (Официальный источник, содержащий информацию о запрете деятельности ряда иностранных компаний на территории РФ).

**Победа Александр Сергеевич,**  
старший преподаватель кафедры информационной безопасности  
Краснодарского университета МВД России

## **К ВОПРОСУ О ПРЕДВАРИТЕЛЬНОМ УЧЕТЕ ДОКУМЕНТОВ**

В соответствии с требованиями нормативных правовых актов исполнители должны подготавливать отдельные виды документов на листах бумаги, предварительно учтенных в подразделениях делопроизводства и режима, или на листах из специальных блокнотов.

При небольшом объеме подготавливаемых документов данная норма не вызывает каких-либо сложностей, и многие подразделения идут по первому пути, т.е. подготавливают документы на предварительно учтенных отдельных листах.

Однако, при подготовке большого количества документов или документов, содержащих большое количество страниц, возникают значительные временные затраты на предварительный учет листов, которые включают в себя время на отбор необходимого количества листов, предоставление необходимых штампов и регистрационных номеров, а также подписей сотрудников режимно-секретных подразделений.

На данном фоне логичным представляется более широкое использование специальных блокнотов. Как правило, такие блокноты изготавливаются типографским способом (здесь и далее речь будет идти о специальных блокнотах, содержащих 100 листов). Но учитывая значительное сокращение финансирования на изготовление типографской продукции, а также всем известные сложности при реализации государственных контрактов, не всегда представляется возможным обеспечить всех должностных лиц необходимым количеством специальных блокнотов.

Ни один нормативный правовой акт не определяет порядок изготовления специальных блокнотов. Учитывая достаточно хорошую обеспеченность подразделений делопроизводства и режима средствами оргтехники, представляется вполне возможным оформлять такие блокноты в указанных подразделениях своими силами. Данная процедура включает в себя печать контрольного листа к каждому блокноту и маркировку самих листов блокнота. Что снова влечет за собой значительные трудозатраты на маркирование листов (простановка штампов, регистрационных номеров, подписей).

В ходе анализа структуры документооборота различных подразделений установлено, что на каждые 10000 подготовленных документов расходуется около 150 специальных блокнотов (далее – комплект специальных блокнотов) (конкретные объемы документооборота подразделений в данной статье не рассматриваются ввиду того, что они являются сведениями ограниченного распространения).

Экспериментальным способом установлено, что для создания каждого блокнота, соответствующего предъявляемым требованиям, сотрудник подразделения делопроизводства и режима тратит около 15 минут.

Таким образом на изготовление одного комплекта специальных блокнотов расходуется 37,5 часов рабочего времени, что практически соответствует одной рабочей неделе. При штатной численности подразделений 1-2 человека, а также в условиях нынешнего значительного некомплекта, такие трудозатраты являются существенными.

С целью обеспечения возможности снижения такой нагрузки предлагается разработать программный или программно-аппаратный комплекс (далее - Комплекс), который позволит создавать и наносить уникальную в рамках номера блокнота маркировку на листы бумаги, а также формировать контрольный лист к каждому блокноту.

Рассматриваемый Комплекс должен соответствовать следующим основным требованиям:

1. Обеспечивать функционирование на уже имеющихся средствах оргтехники, в операционных системах Windows и Linux.
2. Обеспечивать максимальный уровень автоматизации (пользователь должен только задавать необходимые регистрационные данные и загружать бумагу в принтер).
3. Обеспечивать уникальность маркировки в пределах 3-5 лет (рассчитывается исходя из реального объема документооборота подразделений, в которых планируется внедрение Комплекса).
4. Маркировка листов должна быть устойчивой к копированию и сканированию.
5. Формирование маркировки должно зависеть от учетных данных пользователя, под учетной записью которого осуществляется работа, даты и иных переменных параметров (с целью защиты от подделки).
6. Программная часть должна обеспечивать разграничение прав доступа для пользователей.

Указанные требования, а также пути их реализации будут более подробно рассмотрены в ходе дальнейшего исследования.

Разработка и внедрение такого Комплекса позволит высвободить существенный объем рабочего времени для решения других задач оперативно-служебной деятельности подразделений делопроизводства и режима, что особенно актуально в условиях значительного некомплекта сотрудников.

**Синицкий Сергей Демьянович,**  
кандидат технических наук, доцент  
старший научный сотрудник  
научно-исследовательского центра

Краснодарского высшего военного училища  
имени генерала армии С.М. Штеменко;

**Кущев Андрей Владимирович,**  
начальник научно-исследовательской лаборатории  
научно-исследовательского центра  
Краснодарского высшего военного училища  
имени генерала армии С.М. Штеменко

## **ОБ УЧЕТЕ ТРУДОЗАТРАТ ПОДРАЗДЕЛЕНИЙ ДЕЛОПРОИЗВОДСТВА И РЕЖИМА**

### **Аннотация**

В статье с позиций системного анализа рассматриваются вопросы учета труда по возможным направлениям деятельности подразделений делопроизводства и режима.

**Ключевые слова:** сложность, организация, взаимодействие.

### **Введение**

Вопросы учета трудозатрат в организациях различной ведомственной принадлежности напрямую взаимосвязаны с системой оплаты труда и имеют приоритетную направленность в организации работы организаций. Однако, механизм учета трудозатрат и приведения его к реальной заработной плате работников соответствующих подразделений, до сих пор четко не отработан.

ГОСТ Р 59733-2021[1] определяет, что: «Организация должна разработать процедуры систематического мониторинга и анализа результативности процесса оценки сложности на регулярной основе через запланированные промежутки времени», причем под сложностью понимается «состояние организации системы с множеством разнообразных и автономных, но взаимосвязанных и взаимозависимых компонентов или частей, взаимодействующих друг с другом и с внешними элементами конечным множеством нелинейных способов». Вышеуказанный ГОСТ предполагает оценивать сложность работы организаций на основе количества взаимодействий между компонентами организаций. В настоящей статье предлагается учитывать количество взаимодействий за определенный период времени и с учетом норм труда, определенных нормативными правовыми актами, определять наиболее трудозатратные направления деятельности подразделений делопроизводства и режима.

В этих целях предлагается:

1. Построить схему функционирования деятельности подразделений делопроизводства и режима, включив в нее: направления деятельности – N (например: секретное делопроизводство, режим секретности и т.д.), технологические процессы – P (например: мероприятия режима секретности, техническое обслуживание ПЭВМ и т.д.) и технические средства – S (например: средства вычислительной техники, персонал и т.д.) Пример схемы приведен на рисунке 1.

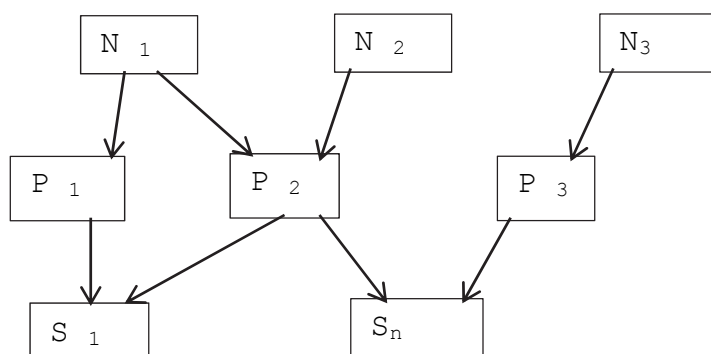


Рисунок 1. Схема функционирования деятельности организации

2. Построить матрицу взаимодействий, обозначив взаимодействие компонент условным знаком, например «+» как представлено в таблице 1.

Таблица 1

Матрица взаимодействий деятельности организации

|                  | N <sub>1</sub> | N <sub>2</sub> | N <sub>3</sub> | P <sub>1</sub> | P <sub>2</sub> | P <sub>3</sub> | S <sub>1</sub> | S <sub>n</sub> |
|------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| N <sub>1</sub>   |                |                |                | +              | +              |                | +              | +              |
| N <sub>2</sub>   |                |                |                |                | +              |                | +              | +              |
| N <sub>3</sub>   |                |                |                |                |                | +              |                | +              |
| P <sub>1</sub>   | +              |                |                |                |                |                |                |                |
| P <sub>2</sub>   | +              | +              |                |                |                |                |                |                |
| P <sub>3</sub>   |                |                | +              |                |                |                |                |                |
| S <sub>1</sub>   | +              | +              |                |                |                |                |                |                |
| S <sub>n</sub>   | +              | +              | +              |                |                |                |                |                |
| C <sub>1-n</sub> | 4              | 3              | 2              | 1              | 2              | 1              | 2              | 3              |

где сумма выполненных взаимодействий «+» по столбцам

$$C_{1-n} = \sum N_1^{S_n}.$$

Даже из подсчета взаимодействий схемы функционирования деятельности организации в статичном состоянии можно сделать вывод, что наиболее сложные: - направления деятельности –  $N_1$ ; технологические процессы –  $P_2$ ; технические средства –  $S_n$ .

3. Через определенные периоды времени необходимо подсчитать количество выполненных взаимодействий (например, обработка входящих документов, составление актов на уничтожение документации, техническое обслуживание ПЭВМ и т.д.) и проставить результаты вместо знаков «+» в таблице 1. Пример приведен в таблице 2.

Таблица 2

Матрица количества выполненных взаимодействий

|           | $N_1$ | $N_2$ | $N_3$ | $P_1$ | $P_2$ | $P_3$ | $S_1$ | $S_n$ |
|-----------|-------|-------|-------|-------|-------|-------|-------|-------|
| $N_1$     |       |       |       | 4     |       |       | 4     | 5     |
| $N_2$     |       |       |       |       | 1     |       | 3     | 2     |
| $N_3$     |       |       |       |       |       | 4     |       | 1     |
| $P_1$     | 4     |       |       |       |       |       |       |       |
| $P_2$     | 3     | 1     |       |       |       |       |       |       |
| $P_3$     |       |       | 4     |       |       |       |       |       |
| $S_1$     | 4     | 3     |       |       |       |       |       |       |
| $S_n$     | 5     | 2     | 1     | 2     |       |       |       |       |
| $C_{1-n}$ | 16    | 6     | 5     | 6     | 1     | 4     | 7     | 8     |

Сравнивая результаты сложения по столбцам таблиц 1 и 2, можно отметить, что изменились результаты оценки сложности деятельности организации, что объясняется тем, что в таблице 2 учтена динамика процесса деятельности организации.

4. Для получения трудозатрат подразделений делопроизводства и режима необходимо результаты суммирования по столбцам таблицы 2 умножить на нормы времени, определенные нормативными правовыми актами [2,3]. Пример норм времени приведен в таблицах 3 и 4.

Таблица 3

## Пример норм времени на обработку входящих документов

| Наименование работы           | Единица измерения объема работы | Норма времени, ч |
|-------------------------------|---------------------------------|------------------|
| Обработка входящих документов | 10 документов                   | 0,65             |

Исполнители – работники канцелярии, экспедиции.

Таблица 4

## Пример норм времени на учет документов

| Наименование документов                    | Единица измерения | Норма времени, ч | № нормы |
|--------------------------------------------|-------------------|------------------|---------|
| Приказ                                     | документ          | 0,07             | 1       |
| Решение, постановление                     | - " -             | 0,1              | 2       |
| Телеграмма                                 | телеграмма        | 0,05             | 3       |
| Сводка                                     | сводка            | 0,48             | 4       |
| Опись                                      | опись             | 0,12             | 5       |
| Письма - извещения                         | письмо            | 0,05             | 6       |
| Приказ (постановление), взятый на контроль | документ          | 0,08             | 7       |

Исполнитель – специалист I категории

Как видно даже из минимального количества представленных примеров норм времени, практически все действия работников подразделений делопроизводства и режима имеют установленные нормативными правовыми актами нормы времени.

Вывод: по результатам учета трудозатрат руководитель организации сможет аргументированно перераспределять ресурсы и фонд заработной платы подразделений делопроизводства и режима.

### Литература

1. ГОСТ Р 59733-2021 Надежность в технике. Руководство по разработке процесса оценки сложности систем организации.
2. Нормы времени на работы по документационному обеспечению управленческих структур федеральных органов исполнительной власти, утвержденные постановлением Министерства труда и социального развития Российской Федерации от 26 марта 2002 г. № 23.
3. Межотраслевые типовые нормы труда на работы по обеспечению защиты государственной тайны в шифровальных подразделениях, утвержденные постановлением Минтруда России от 6 мая 2014 г. № 6с.

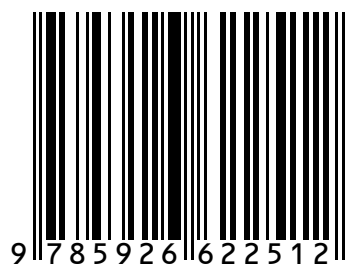
*Научное издание*

**ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ  
ДЕЛОПРОИЗВОДСТВА И РЕЖИМА**

Материалы  
Всероссийской научно-практической конференции  
(22 октября 2025 г.)

*В авторской редакции*  
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2251-2



Подписано в печать 02.02.2026.

Авт. л. 2,5. Заказ 419.

Краснодарский университет МВД России  
350005, г. Краснодар, ул. Ярославская, 128.