

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СЛЕДСТВИИ И КРИМИНАЛИСТИКЕ



ТОМ 2. ПРАКТИЧЕСКОЕ
РУКОВОДСТВО 2026-2027

NIKEY ROMAN

Nikey Roman

ИИ в Следствии 2027

«Автор»

2026

Roman N.

ИИ в Следствии 2027 / N. Roman — «Автор», 2026

Срок следствия — 2 месяца (ст. 162 УПК РФ), а в деле — дамп смартфона на 30 000 сообщений, детализация соединений на сто тысяч строк и выписки по десяткам транзитных счетов? Прочитать этот океан данных вручную физически невозможно. Но загрузить материалы дела в публичный облачный сервис — значит нарушить тайну следствия (ст. 161 УПК РФ), 152-ФЗ и поставить под удар всю доказательственную базу. Второй том практического руководства от Nikey Roman — это готовый рабочий инструмент для действующих следователей, дознавателей, криминалистов, прокуроров и адвокатов. Никакой сухой теории и фантазий о «роботах-следователях»: только строгий процессуальный порядок, работа в изолированном контуре и проверенные алгоритмы, которые экономят десятки часов на рутине.

© Roman N., 2026

© Автор, 2026

Nikey Roman

ИИ в Следствии 2027

ИИ в следствии и криминалистике | Том 2 (2026–2027) | Nikey Roman

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СЛЕДСТВИИ И КРИМИНАЛИСТИКЕ

Том 2. Практическое руководство по работе с цифровыми следами и процессуальными актами (2026–2027)

Настольная книга следователя, дознавателя, криминалиста, прокурора и адвоката

Формат «Два в одном»: Полное издание + Рабочая тетрадь внедрения

Автор: Nikey Roman

Год издания: 2026

ПАСПОРТ ИЗДАНИЯ ДЛЯ ВИТРИНЫ ЛИТРЕС

Варианты заголовка и подзаголовка



Основной заголовок:

Искусственный интеллект в следствии и криминалистике. Том 2



Продающий подзаголовок (вариант 1):

Практическое руководство следователя и дознавателя: цифровые следы, промпты и процессуальные акты по УПК РФ (2026–2027)



Продающий подзаголовок (вариант 2):

От терабайтных дампов и биллинга до обвинительного заключения: настольная книга следователя, криминалиста и прокурора



Продающий подзаголовок (вариант 3):

Как анализировать переписки, выписки и видео за минуты, не нарушив ст. 161 УПК РФ и 152-ФЗ

Витринная аннотация (ЛитРес)

Срок следствия — 2 месяца (ст. 162 УПК РФ), а в деле — дамп смартфона на 30 000 сообщений, детализация соединений на сто тысяч строк и выписки по десяткам транзитных счетов? Прочитать этот океан данных вручную физически невозможно. Но загрузить материалы дела в публичный облачный сервис — значит нарушить тайну следствия (ст. 161 УПК РФ), 152-ФЗ и поставить под удар всю доказательственную базу.

Второй том практического руководства от **Nikey Roman** — это готовый рабочий инструмент для действующих следователей, дознавателей, криминалистов, прокуроров и адвокатов. Никакой сухой теории и фантазий о «роботах-следователях»: только строгий процессуальный порядок, работа в изолированном контуре и проверенные алгоритмы, которые экономят десятки часов на рутине.

Что внутри книги:



Защищённый контур (air-gap):

как организовать локальное рабочее место без выхода в сеть в соответствии с требованиями УПК РФ, 152-ФЗ, ПП РФ № 1119 и приказами ФСТЭК России № 17 и № 21.



Анализ цифровых следов:

быстрый поиск завуалированной речи и эвфемизмов в дампах мессенджеров (ст. 164.1 УПК РФ), проверка алиби по биллингу (ст. 186.1 УПК РФ) и реконструкция цепочек обналичивания.



Компьютерное зрение и фоноскопия:

работа с архивами «Безопасного города», черновая расшифровка ПТП (ч. 7 ст. 186 УПК РФ) и выявление признаков дипфейков для назначения судебной экспертизы.



Автоматизация протоколов и ст. 220 УПК РФ:

перевод живой речи в протокол допроса от первого лица без потери смысла (ст. 190 УПК РФ), сборка обвинительного заключения и аудит дела методом «Красной команды» (взгляд глазами прокурора и адвоката защиты до направления дела в порядке ст. 221 УПК РФ).



Готовый инструментарий + Рабочая тетрадь:

15 правил цифровой чистоты,

Банк из 25 процессуальных промптов

по формуле РНФК, памятка по допросу специалиста в суде, а также готовые бланки регламента отдела и журнала учёта обращений к локальной модели.

Искусственный интеллект не подменяет следователя и не создаёт доказательств — он берёт на себя черновую механику, чтобы человек принял законное и взвешенное решение.

Ключевые теги для ЛитРес

уголовный процесс, УПК РФ, криминалистика, настольная книга следователя, предварительное расследование, цифровые доказательства, искусственный интеллект в праве, нейросети для юристов, осмотр мобильного телефона, тайна следствия, обвинительное заключение, судебная экспертиза, дознание, практическое пособие для следователей.

ОБНОВЛЁННОЕ СОДЕРЖАНИЕ



ПАСПОРТ ИЗДАНИЯ И АННОТАЦИЯ



КОМУ АДРЕСОВАНА КНИГА



КАК ЧИТАТЬ КНИГУ

(Маршруты 1, 2, 3)



БЫСТРЫЙ СТАРТ: 3 рабочих приёма, которые сэкономят вам 4 часа уже сегодня



УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ



ВВЕДЕНИЕ. Цифровой водораздел следствия: от бумажного протокола к когнитивному анализу



1. Вызов эпохи «терабайтных дел»



2. Режим следственной тайны и границы допустимого



3. Что искусственный интеллект делает и чего не делает



4. Как устроен второй том



ГЛАВА 1. Тайна следствия (ст. 161 УПК РФ) и защищённый контур обработки данных



1.1. Уголовно-правовые риски и правовой режим предварительного следствия



1.2. Процессуальный статус результатов применения ИИ (ст. 74, 88 УПК РФ)



1.3. Архитектура изолированного следственного терминала



1.4. Аттестованный контур: 152-ФЗ, 149-ФЗ, ПП РФ № 1119, приказы ФСТЭК России № 17 и № 21 (Кейс 1.1)



ГЛАВА 2. Анализ больших массивов цифровых следов: мессенджеры, биллинг и транзакции



2.1. Анализ дампов переписок: работа с завуалированной речью



2.2. Работа с детализациями соединений: биллинг, координаты, алиби



2.3. Реконструкция финансовых потоков в экономических и коррупционных делах



2.4. Процессуальное закрепление цифровых доказательств: ст. 164.1, 83, 84, 89 УПК РФ, хеширование и цепочка сохранности (Кейсы 2.1–2.3)



ГЛАВА 3. Компьютерное зрение и мультимодальный ИИ в криминалистике



3.1. Анализ видеопотоков городских систем наблюдения («Безопасный город»)



3.2. Фоноскопический экспресс-анализ оперативных аудиозаписей (ПТП)



3.3. Цифровые фальсификации и дипфейки: от признака к решению

○

3.4. От признака к экспертизе: процессуальная оценка синтетических доказательств (Кейс 3.1)

○

3.5. Правовая этика: чего в этой главе делать нельзя

●

ГЛАВА 4. «Второй мозг» следователя: локальная база знаний по многотомному делу

○

4.1. Концепция персональной базы знаний (РКМ) в уголовном процессе

○

4.2. Интерактивный граф связей: от карточек к структуре дела

○

4.3. Работа с противоречиями в показаниях (Кейс 4.1)

○

4.4. Гигиена базы знаний: режим доступа, журналирование, резервные копии, удаление данных

●

ГЛАВА 5. Автоматизация следственных протоколов и процессуальных актов

○

5.1. Протокол допроса: от живой речи к процессуальной точности (ст. 189, 190 УПК РФ)

○

5.2. Протокол осмотра места происшествия и предметов (ст. 177, 180 УПК РФ)

○

5.3. Постановление о привлечении в качестве обвиняемого (ст. 171, 175 УПК РФ)

○

5.4. Аудит протокола перед подписанием: чек-лист и типовые дефекты (Кейс 5.1)

●

ГЛАВА 6. Обвинительное заключение (ст. 220 УПК РФ): синтез, аудит и карта соответствия

○

6.1. Структура обвинительного заключения и место ИИ в его сборке

○

6.2. Возвращение дела прокурором и судом: как снизить риск (ст. 221, 237 УПК РФ)

○

6.3. Метод «Красной команды»: взгляд глазами адвоката защиты

○

6.4. Карта соответствия: эпизод — доказательство — норма (Кейс 6.1)

●

ГЛАВА 7. Горизонт 2027: Предиктивная криминалистика и этика следствия

○

7.1. Предиктивные следственные версии: как ИИ помогает в неочевидных делах

○

7.2. Нейросетевая 3D-реконструкция места происшествия (NeRF и Gaussian Splatting)

○

7.3. Этика, презумпция невиновности и следственная интуиция

○

7.4. Что делать в понедельник утром: тридцать дней внедрения (Кейс 7.1)

●

ЗАКЛЮЧЕНИЕ

●

ПРИЛОЖЕНИЕ 1. Чек-лист цифровой чистоты следователя при работе с ИИ (Правила 01–15)

●

ПРИЛОЖЕНИЕ 2. Банк процессуальных промптов следователя: 25 шаблонов

●

ПРИЛОЖЕНИЕ 3. Памятка по допросу специалиста в суде касательно ИИ-исследований

●

ПРИЛОЖЕНИЕ 4. Словарь сокращений и терминов

●

ПРИЛОЖЕНИЕ 5 (БОНУС). Рабочая тетрадь внедрения: готовые бланки для подразделения

ИИ в следствии и криминалистике | Том 2 (2026–2027) | Аннотация и маршруты чтения

АННОТАЦИЯ

Первый том серии был посвящён судебной стадии, где доказательства уже собраны и подлежат оценке. Второй том обращён к переднему краю уголовной юстиции — к предварительному расследованию, где доказательства только появляются и где цена процессуальной ошибки особенно высока.

Книга отвечает на три практических вопроса. **Правовой:** какие данные о расследовании нельзя выносить за пределы служебного контура, как соотносятся тайна предварительного расследования (статья 161 УПК РФ), законодательство о персональных данных и требования к защите информации, и кто отвечает за ошибку. **Методический:** как формулировать задания модели по формуле РНФК, чтобы получать пригодную для работы аналитику, а не связный правдоподобный текст. **Технологический:** как организовать изолированное рабочее место, локальный поиск по материалам дела (RAG) и журналирование обращений к ИИ.

Отдельно и последовательно разбирается процессуальная сторона: результат работы алгоритма — это ориентирующая информация, а не доказательство; доказательственное значение имеют только процессуально оформленные материалы; решение принимает человек — следователь, эксперт, суд.

КОМУ АДРЕСОВАНА КНИГА

Следователю и дознавателю.

Книга даёт способ разгрузить себя на рутинной обработке больших массивов данных: переписки, детализации соединений, банковские выписки, видеозаписи, аудиопротоколы ПТП. Начинайте с Главы 1 (тайна следствия и контур), затем Глава 2 (цифровые следы) и Глава 5 (протоколы).

Криминалисту и специалисту-эксперту. Здесь — границы применимости компьютерного зрения, распознавания речи и синтетических медиа, а также корректная формулировка вопросов эксперту и процессуальная оценка результатов. Начинайте с Главы 3, затем Глава 5 и Приложение 3 (памятка по допросу специалиста).

Прокурору. Полезны Глава 6 (обвинительное заключение и аудит доказательственной цепочки) и Приложение 3: типовые уязвимости ИИ-исследований, которые защита проверяет в первую очередь. Начинайте с Главы 6.

Адвокату. Книга описывает не только возможности, но и слабые места цифровых доказательств: вопросы о сертификации, хеш-суммах, воспроизводимости, компетенции специалиста. Начинайте с Главы 3 (раздел 3.4) и Приложения 3.

КАК ЧИТАТЬ КНИГУ

Маршрут 1. Быстрый: за 90 минут

Прочитайте аннотацию и «Кому адресована книга», Введение и Главу 1 полностью, затем Приложение 1 (чек-лист цифровой чистоты). Этого достаточно, чтобы понять правовые границы и не совершить наиболее опасных ошибок при работе с материалами уголовного дела.

Маршрут 2. Практический: по рабочей задаче

Ваша задача

Разделы книги

Понять, что можно и что нельзя выносить за пределы контура

Глава 1 (1.1–1.4), Приложение 1

Научиться ставить задачи модели

Введение, Глава 1 (1.2), Приложение 2

Разобрать дамп переписки, биллинг, банковские выписки

Глава 2 (2.1–2.3), Кейсы 2.1–2.3

Обезопасить работу с электронными носителями

Глава 2 (2.4), Кейс 2.1

Проверить видео- и аудиоматериалы, распознать фальсификацию

Глава 3 (3.1–3.4), Кейс 3.1

Собрать «второй мозг» по многотомному делу

Глава 4 (4.1–4.4), Кейс 4.1

Подготовить и вычитать протокол

Глава 5 (5.1–5.4), Кейс 5.1

Подготовить обвинительное заключение и провести аудит

Глава 6 (6.1–6.4), Кейс 6.1

Выстроить порядок работы подразделения и внедрить бланки

Глава 7 (7.4), Приложение 1, Приложение 5

Найти готовый шаблон запроса

Приложение 2 (шаблоны 1–25)

Подготовиться к допросу специалиста в суде

Приложение 3

Разобраться в термине или сокращении

Приложение 4

Маршрут 3. Полный: последовательно

Книга построена как курс: правовые рамки (Глава 1) → работа с цифровыми следами (Глава 2) → видео, аудио и синтетические доказательства (Глава 3) → аналитическая база по делу (Глава 4) → процессуальные документы (Глава 5) → обвинительное заключение и его аудит (Глава 6) → горизонт 2027 года и этика (Глава 7). Оптимальный порядок для подразделения — по одной главе в неделю с применением к текущему делу.

Важно! Ни одно положение книги не является официальной методикой ведомства или указанием, обязательным к исполнению. Порядок работы определяется Уголовно-процессуальным кодексом РФ, ведомственными нормативными актами, указаниями руководителя следственного органа и прокурорским надзором.

БЫСТРЫЙ СТАРТ: 3 рабочих приёма, которые сэкономят вам 4 часа уже сегодня

Не хотите ждать, пока дочитаете книгу до конца? Вот три правила и один универсальный шаблон, которые можно применить к текущему делу на локальной рабочей станции прямо сейчас.

Правило 1. Никаких фамилий и номеров дел. Перед подачей любого текста в локальную модель проведите автозамену: *Иванов И.И. → Участник А., ООО «Вектор» → Контрагент 1*. Это базовый стандарт протокола «Закрытый контекст».

Правило 2. Запретите модели додумывать. Всегда включайте в конец задания жёсткую фразу: *«Используй только предоставленный текст. Если сведений нет — пиши "нет данных". Каждое утверждение сопровождай точной цитатой и таймкодом/номером строки»*.

Правило 3. Экспресс-промпт для поиска противоречий в двух протоколах допроса:

РОЛЬ: Аналитический помощник следователя в изолированном контуре. **НОРМАТИВНЫЙ БАЗИС:** ст. 88, 189, 190 УПК РФ. Ты не оцениваешь достоверность показаний, а только сопоставляешь текст. **ФАКТУРА:** Обезличенные тексты двух допросов одного лица (Допрос 1 и Допрос 2). **КРИТЕРИИ ВЫВОДА:** Составь таблицу из 4 столбцов: «Обстоятельство (время, место, участники, суммы)» — «Цитата из Допроса 1» — «Цитата из Допроса 2» — «Характер расхождения (уточнил / изменил / умолчал)». Ничего не домысливай от себя.

Полный банк из 25 специализированных промптов для дампов переписок, биллинга, банковских выписок, видеозаписей и аудита обвинительного заключения представлен в Приложении 2, а готовые бланки журнала учёта и регламента отдела — в Приложении 5.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение в тексте

Что означает

Как использовать

КЕЙС N.M.

Учебный разбор ситуации

Показывает путь от ошибки к процессуально корректному порядку работы

Шаблон N

Готовый промпт

Шаблон запроса из Приложения 2, адаптируется под конкретное дело

Чек-лист / ☐

Список для самопроверки

Проверка перед следственным действием или подписанием документа

Таблица

Сопоставление вариантов

Сравнение подходов, норм, рисков и последствий

> Важно!

Врезка-предупреждение

Положение, которое нельзя пропустить

> Процессуальная ловушка:

Врезка о скрытом риске

Ситуация, где формально верное действие ведёт к процессуальному дефекту

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Книга носит практический рекомендательный характер и не является нормативным правовым актом, официальной методикой правоохранительного органа, ведомственным приказом или юридической консультацией по конкретному делу. Описанные практики — предложения автора, которые применяются только в пределах, установленных Уголовно-процессуальным кодексом РФ и ведомственными актами.

Все примеры, фамилии, наименования организаций, номера дел, адреса, телефонные номера, таймкоды и реквизиты документов условны и приведены исключительно в учебных целях; совпадения случайны. Реальных персональных данных в книге нет.

Результат работы любой автоматизированной системы — ориентирующая аналитика, а не доказательство. Доказательственное значение имеют только сведения, полученные и закреплённые в порядке, предусмотренном УПК РФ. Процессуальные решения принимает и подписывает человек — следователь, дознаватель, эксперт, прокурор, суд; искусственный интеллект не заменяет ни одного из них и не несёт ответственности.

Нормы права и разъяснения высших судов приведены по состоянию на 2026 год и подлежат проверке по актуальной редакции перед применением. Автор не несёт ответственности за решения, принятые читателем на основании материалов книги.

ИИ в следствии и криминалистике | Том 2 (2026–2027) | Введение

ВВЕДЕНИЕ. Цифровой водораздел следствия: от бумажного протокола к когнитивному анализу

«Следователь XXI века расследует не просто следы на снегу или гильзы на полу. Он расследует терабайты невидимого цифрового эфира. Тот, кто пытается просеять этот океан данных вручную, обречён на провал. Тот, кто вооружён автономным интеллектом — видит истину насквозь». — Nikey Roman

1. Вызов эпохи «терабайтных дел»

Первый том этой серии был посвящён судебной стадии, где доказательства уже собраны, закреплены в протоколах и подлежат беспристрастной судебной оценке. Второй том обращён к самому пеклу уголовной юстиции — к стадии предварительного расследования, где доказательства только появляются, а цена процессуальной ошибки определяется не репутацией, а судьбами людей.

Ещё двадцать лет назад типовое уголовное дело умещалось в один-два тома: протоколы допросов свидетелей, заключения традиционных криминалистических экспертиз, протокол осмотра места происшествия. Сегодня картина иная:



Дело о дистанционном мошенничестве сопровождается криминалистическим дампом телефона с десятками тысяч сообщений — сотнями и тысячами страниц распечатки;



Дело о преступлении в сфере закупок или экономической деятельности включает выгрузки банковских проводок по десяткам счетов и значительные объёмы изъятой электронной переписки — от десятков гигабайт, а в отдельных делах до терабайт;



Детализации соединений абонентов, получаемые по судебному решению, насчитывают десятки и сотни тысяч строк с идентификаторами базовых станций и их координатами;



Городские системы видеонаблюдения накапливают значительные объёмы видеоматериалов, сопоставимые с тысячами часов записи по отдельному эпизоду.

По данным МВД России за первое полугодие 2025 года, более трети зарегистрированных преступлений совершаются с использованием информационно-телекоммуникационных технологий, а по экономическим и должностным составам ключевые доказательства всё чаще существуют именно в цифровой форме: переписка, сведения о соединениях, банковские транзакции, видеозаписи.

Человеческий мозг следователя, работающего в условиях жёсткого процессуального цейтнота (срок предварительного следствия — не свыше двух месяцев, часть 1 статьи 162 УПК РФ), физически не способен вручную сопоставить такой массив. Возникает парадокс: информации стало больше, но глубина доказывания упирается в биологический предел человека.

Именно здесь появляется предмет этой книги. Речь идёт не о «роботе-следователе» и не о замене процессуальных решений алгоритмом, а о разделении труда: механическая обработка массивов данных — машине, оценка доказательств, квалификация и решение — человеку. Назначение уголовного судопроизводства (статья 6 УПК РФ) не меняется от того, каким инструментом пользовался следователь.

Практика показывает, где выигрыш от аналитических инструментов наиболее ощутим, а где он иллюзорен.

Категория дел

Что даёт аналитическая обработка

Где предел

Дистанционное мошенничество, хищения с использованием электронных средств платежа

Быстрая навигация по дампу переписки, выявление аномалий активности, сопоставление с выписками

Установление умысла и роли каждого участника — только через следственные действия

Экономические и коррупционные составы

Реконструкция движения средств, выявление транзитных звеньев, подготовка вопросов для экспертизы

Оценка доказательств и квалификация — за следователем и судом

Преступления против личности, имущественные

Хронометраж видеозаписей, работа с детализациями соединений, проверка версий

Идентификация лица, выводы о событиях — только экспертным путём

Многоэпизодные дела, дела в отношении группы лиц

Ведение хронологии, карт соответствия «эпизод — доказательство — норма», поиск противоречий

Процессуальное решение по каждому эпизоду принимает следователь

Обратная сторона скорости — автоматизационная эйфория: чем убедительнее выглядит результат, тем меньше его хочется проверять. Поэтому в каждой главе книги есть раздел о том, что именно обязан перепроверить человек.

2. Режим следственной тайны и границы допустимого

Если судебное разбирательство по общему правилу открыто, то досудебное производство защищено режимом следственной тайны.

Данные предварительного расследования не подлежат разглашению, за исключением случаев, прямо предусмотренных частями второй, четвёртой и шестой статьи 161 УПК РФ. Это не «абсолютный запрет»: закон допускает предание гласности с разрешения следователя или дознавателя, не относит к разглашению сведения, распространённые самим следователем (прокурором) публично, и сведения о нарушении закона должностными лицами. Но для работы с нейросетями важен сам принцип: по умолчанию материалы дела за пределы служебного контура не выходят.

Часть 3 статьи 161 УПК РФ обязывает следователя предупредить участников уголовного судопроизводства о недопустимости разглашения данных без соответствующего разрешения, о чём отбирается подписка. Именно для лиц, предупреждённых в установленном законом порядке, предусмотрена ответственность по статье 310 УК РФ — разглашение данных предварительного расследования. Санкция этой статьи включает штраф до 80 000 рублей, обязательные работы до 480 часов, исправительные работы до двух лет либо арест до трёх месяцев.

Это уточнение принципиально. Субъектом статьи 310 УК РФ является предупреждённое лицо, а не следователь. Для самого следователя или дознавателя последствия неверной работы с данными носят прежде всего дисциплинарный характер, а уголовная ответственность возможна лишь при наличии всех признаков конкретного состава — например, статьи 283 УК РФ (разглашение государственной тайны: до четырёх лет лишения свободы по части первой, а если деяние повлекло по неосторожности тяжкие последствия — от трёх до семи лет), статьи 285 УК РФ (злоупотребление полномочиями), статьи 286 УК РФ (превышение полномочий) или статьи 293 УК РФ (халатность).

Отдельная плоскость — персональные данные участников. Их обработка ведётся в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» с учётом изъятий, установленных уголовно-процессуальным законодательством, а общие требования к защите информации определяет Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Обработка таких данных в системах, не аттестованных в установленном порядке и не отнесённых к ведомственному контуру, не допускается. Нарушение требований к обработке персональных данных влечёт административную ответственность по статье 13.11 КоАП РФ.

Отсюда главный практический вывод: передача материалов уголовного дела или персональных данных в публичный облачный сервис нарушает часть 1 статьи 161 УПК РФ и требования 152-ФЗ. Автоматического образования состава преступления нет: ответственность наступает по конкретной норме и при наличии всех её признаков. Но риск — дисциплинарный, административный, уголовный и, что не менее важно, доказательственный: сведения, ставшие достоянием третьих лиц, теряют доверие и создают основания для защиты от недопустимости.

Именно поэтому работа с материалами дела ведётся исключительно в аттестованном контуре, требования к которому установлены постановлением Правительства РФ от 01.11.2012 № 1119 и приказами ФСТЭК России № 17 и № 21.

3. Что искусственный интеллект делает и чего не делает

Границы применимости важнее возможностей, потому что именно за их нарушением следуют процессуальные дефекты.

Что делает. Извлекает факты из больших массивов текста и таблиц; строит хронологии и таблицы сопоставления; ищет противоречия между документами; выделяет в переписке эвфемизмы и аномалии активности; сопоставляет координаты базовых станций; формирует черновики процессуальных документов по заданной структуре; проверяет проект документа на формальные дефекты.

Чего не делает. Не устанавливает истину и не оценивает доказательства — это компетенция следователя и суда (статьи 74, 88 УПК РФ). Не определяет подлинность видео- и аудиоматериалов — это предмет экспертизы. Не принимает решений о виновности, о квалификации, о мере пресечения. Не несёт ответственности. Не может обосновать обвинение вероятностной оценкой: презумпция невиновности (статья 14 УПК РФ) несовместима с логикой «модель посчитала, что вероятность 94 %».

Результат работы модели — ориентирующая аналитика. Она нужна, чтобы следователь быстрее понял материалы дела, точнее спланировал следственные действия и не пропустил противоречие. Доказательственное значение имеют только сведения, полученные и закреплённые в порядке, установленном УПК РФ.

Операция

Кому поручается

Чем подтверждается результат

Первичная обработка массива: разбивка, индексация, поиск по ключевым словам

Программному средству

Протокол следственного действия, в котором указано применённое техническое средство (часть 5 статьи 166 УПК РФ)

Извлечение фактов, построение хронологии, сопоставление позиций

Программному средству с последующей проверкой

Ссылка на конкретный том, лист дела, файл, запись

Формулирование выводов о событии, виновности, квалификации

Только человеку

Постановление, обвинительное заключение, приговор

Установление подлинности видео- и аудиоматериалов, идентификация лица

Только эксперту

Заключение эксперта (статья 80 УПК РФ)

Оценка допустимости доказательства

Следователю, прокурору, суду

Решение по правилам статей 75, 88, 235 УПК РФ

Процессуальное решение и подпись

Только человеку

Подписанный процессуальный документ

Нижние три строки этой таблицы не делегируются ни при каких обстоятельствах: именно они образуют ту часть следственной работы, где закон требует личного решения и личной ответственности.

Процессуальная ловушка: красиво оформленный вывод модели психологически воспринимается как установленный факт. Именно так в проект постановления попадают формулировки, не подтверждённые ни одним листом дела. Правило простое: каждый вывод модели должен вести к конкретному источнику — тому, листу дела, файлу, записи.

Отдельно следует сказать о главном правиле цифровой работы следователя: любое изменение исходного файла доказательства недопустимо. Поэтому первым действием всегда становится фиксация контрольной суммы (например, SHA-256) и обеспечение цепочки сохранности носителя и копий.

4. Как устроен второй том

Книга состоит из семи глав и пяти приложений (включая бонусную Рабочую тетрадь внедрения).



Глава 1

закладывает правовой фундамент: режим следственной тайны, градации юридической силы результатов применения ИИ, оценка допустимости доказательств и архитектура изолированного рабочего места.



Глава 2

посвящена работе с большими массивами цифровых следов: переписки, детализации соединений, банковские операции и процессуальное закрепление результатов.



Глава 3

разбирает компьютерное зрение и мультимодальный анализ: видеозаписи, фоноскопию, признаки синтетических медиа и границу между признаком и экспертизой.



Глава 4

описывает «второй мозг» следователя — локальную базу знаний по многотомному делу, граф связей и работу с противоречиями в показаниях.



Глава 5

показывает автоматизацию процессуальных документов: протокол допроса, протокол осмотра, постановление о привлечении в качестве обвиняемого и аудит протокола перед подписанием.



Глава 6

посвящена обвинительному заключению: сборке, аудиту доказательственной цепочки и «взгляду глазами защиты».



Глава 7

смотрит в горизонт 2027 года: предиктивные версии, трёхмерная визуализация, этика и презумпция невиновности.



Приложения 1–5

носят рабочий характер: Приложение 1 — чек-лист цифровой чистоты из пятнадцати правил, Приложение 2 — банк из двадцати пяти процессуальных промптов, Приложение 3 — памятка по допросу специалиста в суде, Приложение 4 — словарь сокращений и терминов, Приложение 5 — Рабочая тетрадь внедрения с готовыми бланками для печати.

Инструмент меняет скорость работы, но не её смысл. Смысл остаётся прежним: устанавливать обстоятельства, подлежащие доказыванию, не нарушив права человека и требования закона. Переверните страницу. Добро пожаловать в цифровую криминалистику высокой точности.

— Nikey Roman, 2026 год

ИИ в следствии и криминалистике | Том 2 (2026–2027) | Глава 1. Тайна следствия и защищённый контур

ГЛАВА 1. Тайна следствия (ст. 161 УПК РФ) и защищённый контур обработки данных

«Данные предварительного расследования не подлежат разглашению — за исключением случаев, прямо предусмотренных частями второй, четвёртой и шестой статьи 161 УПК РФ. Работа с ними вне аттестованного контура эту границу переступает».

Все примеры, фамилии, адреса, номера и реквизиты в главе условны (учебный пример). Описанные практики — рекомендации автора, а не официальная методика ведомства; они не заменяют УПК РФ.

1.1. Уголовно-правовые риски и правовой режим предварительного следствия

В уголовном деле разглашение данных предварительного расследования способно:

- привести к уничтожению или сокрытию следов преступления соучастниками;
- создать условия для давления на свидетелей и потерпевших;
- сорвать негласные оперативно-розыскные мероприятия (ОРМ) и обесценить результаты прослушивания телефонных переговоров (ПТП);
- лишить следователя возможности провести следственное действие внезапно.

Вред от разглашения неустраим: сведения уже не вернуть, поэтому цена ошибки цифровой безопасности здесь выше, чем в гражданском споре.

Правовой режим ст. 161 УПК РФ

Формулировка «абсолютный запрет» неточна и вредна: она порождает иллюзию, будто любое упоминание материалов дела вовне автоматически противоправно, и приучает не замечать реальные границы. Корректно так: данные предварительного расследования не подлежат разглашению, за исключением случаев, прямо предусмотренных частями второй, четвёртой и шестой статьи 161 УПК РФ.

часть вторая — данные могут быть преданы гласности с разрешения следователя или дознавателя и только в том объёме, который признан допустимым, если это не противоречит интересам расследования и не нарушает права участников;

часть четвёртая — запрет не распространяется на сведения о нарушении закона органами государственной власти и их должностными лицами, на сведения, распространённые самими уполномоченными участниками публично, а также на оглашённые в открытом судебном заседании;

часть шестая — определяет, какие сообщения данных разглашением не являются: 1) изложение сведений по делу в ходатайствах, заявлениях, жалобах и иных процессуальных документах по этому делу, а также в заявлениях в государственные и межгосударственные органы по защите прав человека; 2) предоставление сведений специалисту при даче им письменного обязательства о неразглашении.

Предупреждение и подписка

Часть третья статьи 161 УПК РФ: следователь или дознаватель предупреждает участников уголовного судопроизводства о недопустимости разглашения без соответствующего разрешения ставших им известными данных предварительного расследования, о чём у них берётся подписка с предупреждением об ответственности по ст. 310 УК РФ. Предупреждение адресовано участникам уголовного судопроизводства и отбирается, когда это необходимо, а не механически «у каждого участника каждого следственного действия». Подписка — юридический факт, от которого зависит применение ст. 310 УК РФ.

Ответственность: точные адресаты и точные санкции

Ст. 310 УК РФ предусматривает ответственность лица, предупреждённого в установленном законом порядке о недопустимости разглашения. Это участник судопроизводства — свидетель, потерпевший, понятой, переводчик, специалист, защитник, — а не следователь; сам следователь адресатом этой статьи не является. Санкция включает четыре варианта: штраф до 80 000 рублей, обязательные работы до 480 часов, исправительные работы до двух лет либо арест до трёх месяцев.

Ст. 283 УК РФ («Разглашение государственной тайны») устроена иначе, и её санкцию нельзя приводить одной цифрой. Часть первая — разглашение сведений, составляющих государственную тайну, лицом, имеющим к ним доступ, — наказывается арестом на срок от четырёх до шести месяцев либо лишением свободы до четырёх лет. Часть вторая — то же деяние, повлёкшее по неосторожности тяжкие последствия, — лишением свободы от трёх до семи лет. «До семи лет» — это не «при наличии гостайны», а только при доказанных тяжких последствиях.

Для следователя (дознателя) последствия нарушения режима тайны носят прежде всего дисциплинарный характер. Уголовная ответственность возможна лишь при наличии всех признаков конкретного состава — в частности, ст. 283, 285, 286 или 293 УК РФ. Автоматического образования состава нет: требуется установить событие, субъекта и вину, а для ряда составов — существенное нарушение прав и законных интересов, корыстную или иную личную заинтересованность либо наступление тяжких последствий.

Передача материалов в публичный облачный сервис

Размещение фрагмента протокола допроса, персональных данных свидетеля или файла с материалами дела в публичном облачном сервисе нарушает ч. 1 ст. 161 УПК РФ, а применительно к персональным данным — Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Такие действия влекут дисциплинарную ответственность и административную ответственность по ст. 13.11 КоАП РФ, а при наличии всех признаков конкретного состава — уголовную ответственность (в том числе по ст. 283, 285, 286, 293 УК РФ). Именно поэтому работа с материалами дела ведётся исключительно в аттестованном контуре.

Важно! Обработка персональных данных участников уголовного судопроизводства осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» с учётом изъятий, установленных уголовно-процессуальным законодательством. Обработка таких данных в информационных системах, не аттестованных в установленном порядке и не отнесённых к ведомственному контуру, не допускается.

Действие

Нарушаемая норма

Основные последствия

Передача материалов дела и персональных данных в публичный облачный сервис
ч. 1 ст. 161 УПК РФ; 152-ФЗ

дисциплинарная ответственность; ст. 13.11 КоАП РФ; уголовная — при наличии всех признаков конкретного состава

Разглашение данных участником, предупреждённым по ч. 3 ст. 161 УПК РФ
ст. 310 УК РФ

штраф до 80 000 рублей, обязательные работы до 480 часов, исправительные работы до двух лет либо арест до трёх месяцев

Разглашение государственной тайны

ст. 283 УК РФ

ч. 1 — лишение свободы до четырёх лет; ч. 2 (тяжкие последствия по неосторожности) — от трёх до семи лет

Использование служебных возможностей вопреки интересам службы

ст. 285, 286 УК РФ

уголовная ответственность при наличии всех признаков состава

Ненадлежащее исполнение обязанностей по защите данных

ст. 293 УК РФ

уголовная ответственность при наличии всех признаков состава

Режим тайны следствия не отменяет процессуальных гарантий, а предполагает их. Изъятие электронных носителей и копирование информации производятся с учётом ст. 164.1 УПК РФ; получение сведений, доступ к которым ограничен, — в судебном порядке (ст. 29, 165 УПК РФ); действия и решения следователя обжалуются в порядке ст. 125 УПК РФ.

1.2. Процессуальный статус результатов применения ИИ (ст. 74, 88 УПК РФ)

Часть 1 статьи 74 УПК РФ устанавливает: «Доказательствами по уголовному делу являются любые сведения, на основе которых суд, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела».

Ключевые слова — «в порядке, определенном настоящим Кодексом». Сведения приобретают статус доказательства не благодаря источнику или технологии, а благодаря процессуальной форме, в которой они получены и закреплены. Модель — не субъект доказывания и не источник доказательства; процессуальную форму сведениям придаёт следователь.

Формы закрепления, применимые к цифровым результатам: протоколы следственных действий и судебного заседания (ст. 83 УПК РФ), иные документы (ст. 84 УПК РФ), заключение и показания эксперта и специалиста (ст. 80 УПК РФ), а также использование в доказывании результатов ОРД (ст. 89 УПК РФ, Федеральный закон от 12.08.1995 № 144-ФЗ).

Три градации юридической силы результатов работы ИИ

Градация

Что это

Как закрепляется

Доказательственное значение

1. Ориентирующая аналитика

гипотезы, сводки, нарезки, выявление связей

процессуально не закрепляется; отражается в планах и рабочих справках

основание для планирования следственных действий; самостоятельного доказательственного значения не имеет

2. Результат применения технического средства

распознавание речи, разметка видеозаписи, расчёт контрольных сумм

протокол следственного действия (ст. 83, ч. 5 и ч. 8 ст. 166 УПК РФ)

проверяется и оценивается по ст. 88 УПК РФ в совокупности с другими доказательствами

3. Заключение и показания эксперта (специалиста)

исследование признаков монтажа, дипфейка, методик обработки

ст. 80, 195, 196, 201, 204 УПК РФ

самостоятельное доказательство; эксперт несёт ответственность по ст. 307 УК РФ

Ориентирующая информация. Модель обрабатывает условный массив переписки и выдаёт гипотезу: «оплата обсуждалась под кодовым словом „синие папки“». Это криминалистическая зацепка, на основе которой планируются обыск, выемка или допрос; каждый шаг оформляется самостоятельным протоколом.

Результат применения технического средства. Часть 6 ст. 164 УПК РФ допускает применение технических средств; часть 5 ст. 166 УПК РФ требует указать технические средства, условия и порядок их использования, объекты и результаты; часть 8 ст. 166 УПК РФ — приложить к протоколу носители информации. Для цифровых материалов это означает: наименование и версия программы, режим обработки, перечень входных и выходных файлов, хеш-суммы до и после обработки.

Заключение эксперта (специалиста). Полное название ст. 80 УПК РФ — «Заключение и показания эксперта и специалиста». Если требуется исследование признаков монтажа, синтеза изображения или голоса, к делу приобщается не «распечатка ответа нейросети», а заключение лица, обладающего специальными знаниями, с описанием применённой методики и с ответственностью по ст. 307 УК РФ.

Недопустимость доказательств: правило, а не автоматизм

Статья 75 УПК РФ определяет недопустимые доказательства. Часть вторая содержит перечень: показания подозреваемого (обвиняемого), данные в отсутствие защитника и не подтверждённые в суде (п. 1); показания потерпевшего и свидетеля, основанные на догадке, предположении, слухе (п. 2); случаи, предусмотренные пунктами 2.1–2.3; п. 3 — «иные доказательства, полученные с нарушением требований настоящего Кодекса».

Из этого перечня не следует, что любой дефект протокола автоматически влечёт недопустимость. Недопустимость — результат оценки доказательства по правилам ст. 75 и ст. 88 УПК РФ: каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в совокупности — достаточности. Вопрос об исключении доказательства разрешается, как правило, по ходатайству стороны в порядке ст. 235 УПК РФ.

Отсюда три вывода. Неполнота протокола устраняется дополнением и уточнением, а не «спасением» задним числом. Оценку даёт следователь, а не программа. Если доказательство вызывает сомнения, их следует зафиксировать и проверить, а не укреплять ссылками на алгоритм.

Терминология серии: формула РНФК и «Нормативный якорь»

В книге используется единая формула рабочего промпта — **РНФК**:



Роль

— какая профессиональная позиция задаётся модели (например, «аналитик материалов уголовного дела»);



Нормативный базис

— нормы и правила, в границах которых формулируется результат (УПК РФ, требования к защите информации);



Фактура

— конкретные обезличенные данные, которые передаются в обработку;



Критерии вывода

— требования к результату: что считается выводом, а что — гипотезой, требующей проверки.

«Нормативный базис» здесь не украшение. Он реализует защитный протокол «Нормативный якорь»: прежде чем формулировать задачу, исполнитель фиксирует норму, по которой будет оцениваться результат, и только затем описывает, что требуется. Если запрос нельзя обосновать нормой, значит, он сформулирован неверно.

Процессуальная ловушка: «модель написала, что доказательство недопустимо» — юридически ничтожная фраза. Вопрос о недопустимости решает уполномоченное лицо или суд, а не сервис.

1.3. Архитектура изолированного следственного терминала

Для работы с материалами уголовного дела применяется принцип «воздушного зазора» (air-gap) — физического отсутствия сетевого канала между рабочей станцией и внешними сетями.

[ВНЕШНИЙ МИР] —X— [ФИЗИЧЕСКИЙ РАЗРЫВ СЕТИ] —X— [РАБОЧАЯ СТАНЦИЯ СЛЕДОВАТЕЛЯ] | |— Локальная языковая модель |— Локальный движок распознавания речи |— Зашифрованный локальный том

Технические решения указаны как примеры: для служебного применения используются решения, включённые в реестр российского программного обеспечения (реестр Минцифры), с учётом требований импортозамещения.

Основные правила оборудования рабочего места

Физическое отключение беспроводных интерфейсов. Модули Wi-Fi и Bluetooth блокируются на уровне BIOS/UEFI и, дополнительно, организационно.

Шифрование накопителей. Тома дела и рабочие копии хранятся в зашифрованных контейнерах; ключи учитываются отдельно от носителя.

Хеширование входящих файлов. (Хеш-сумма — результат криптографического преобразования для проверки неизменности файла.) Любой цифровой объект — дампы мобильного устройства, видеозапись, выгрузка переписки — получает контрольную сумму (например, SHA-256), что позволяет доказать неизменность массива при анализе.

Журналирование. Фиксируется, кто, когда, с каким файлом и каким инструментом работал; журнал подтверждает порядок работы при проверке.

Разграничение доступа. К материалам допускаются только лица, которым это необходимо по должности; копирование за пределы контура запрещено.

Резервное копирование и уничтожение копий. Резервные копии хранятся в том же контуре; временные файлы по завершении работы уничтожаются в установленном порядке.

Отсутствие внешней телеметрии. Настройки инструментов исключают автоматическую отправку данных и отчётов об ошибках.

Защитный протокол «Закрытый контекст»

«Закрытый контекст» — правило, по которому в обработку передаётся только необходимый для конкретной задачи минимум данных, только внутри аттестованного контура и, если характер задачи не требует иного, в обезличенном виде. Из него вытекают три операции, выполняемые до формулирования любого запроса:

- удалить или заменить идентификаторы (фамилии, адреса, телефоны, номера дел, точные даты) на маски: «подозреваемый А.», «свидетель К.», «потерпевший П.»;

- оставить ровно тот фрагмент, который необходим: не том дела целиком, а относящийся к вопросу эпизод;

- проверить, нельзя ли восстановить личность по совокупности оставшихся признаков — редкая должность, единственный адрес, узнаваемое событие.

Обезличивание снижает риск, но не отменяет правовой режим. Если по обработанным сведениям можно установить обстоятельства расследования, они по-прежнему охраняются ч. 1 ст. 161 УПК РФ.

Отдельно решается вопрос о переносе результата. Если подготовленный документ должен быть включён в дело, он выносится из контура только в том виде, который предназначен для приобщения, с отметкой о том, где и кем он подготовлен. Черновые файлы, промежуточные выгрузки и рабочие заметки остаются в контуре и к делу не приобщаются.

Изолированный контур не создаёт «процессуального комфорта»: он не отменяет ни судебный порядок получения разрешений (ст. 29, 165 УПК РФ), ни правила изъятия электронных носителей и копирования информации (ст. 164.1 УПК РФ), ни требования к протоколу (ч. 5 и ч. 8 ст. 166 УПК РФ), ни право участников обжаловать действия следователя (ст. 125 УПК РФ).

Чек-лист 1. Оценка защищённости контура перед обработкой материалов дела

- ☐ Информационная система аттестована в установленном порядке и отнесена к ведомственному контуру — иначе обработка персональных данных участников не допускается.
- ☐ Определён уровень защищённости персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119, реализованы меры приказов ФСТЭК России № 17 и № 21 — это нормативное основание требования к контуру.
- ☐ Обработка ведётся на рабочей станции с физически отключёнными беспроводными интерфейсами — сетевой канал сводит изоляцию к нулю.
- ☐ Применяемая модель развёрнута локально и не обращается к внешним серверам — внешний вызов означает передачу данных третьему лицу.
- ☐ Разграничены права доступа, ведётся журнал операций — журнал позволяет установить источник утечки.
- ☐ Носители и рабочие копии хранятся в зашифрованном виде, ключи учитываются отдельно — изъятие носителя не должно означать раскрытие материалов.
- ☐ Рассчитаны хеш-суммы исходных и результирующих файлов, оформлена цепочка сохранности — без этого невозможно доказать неизменность объекта.
- ☐ Резервные копии находятся в том же контуре, доступ к ним ограничен — резервная копия в публичном сервисе обесценивает всю защиту.
- ☐ Утверждён порядок уничтожения временных файлов по завершении работы — остаточные копии — типичный источник утечки.
- ☐ Применяемое программное обеспечение входит в реестр российского программного обеспечения либо согласовано в установленном порядке — требование импортозамещения.
-

☐ Участники предупреждены о недопустимости разглашения с отображением подписки (ч. 3 ст. 161 УПК РФ) — без подписки механизм ст. 310 УК РФ не работает.

1.4. Аттестованный контур: 152-ФЗ, 149-ФЗ, ПП РФ № 1119, приказы ФСТЭК России № 17 и № 21

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» определяет основания и условия обработки персональных данных, требования к их защите и права субъекта. Правовым основанием обработки для целей уголовного судопроизводства служат ст. 6, 9, 10 (специальные категории персональных данных), 11 (биометрические персональные данные) и 18 (обязанности оператора при сборе персональных данных) 152-ФЗ, а требования, методы и порядок обезличивания установлены постановлением Правительства РФ от 01.08.2025 № 1154. Ст. 13.1 152-ФЗ (введена с 01.09.2025) регулирует особенности обработки персональных данных, полученных в результате обезличивания, при формировании составов данных уполномоченным органом.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» задаёт общие рамки: понятие информационной системы, обязанности обладателя информации и оператора по недопущению неправомерного доступа, уничтожения, модифицирования и копирования информации.

Постановление Правительства РФ от 01.11.2012 № 1119 устанавливает уровни защищённости персональных данных при их обработке в информационных системах и требования, соответствующие каждому уровню; уровень определяется категорией данных и числом субъектов.

Приказы ФСТЭК России № 17 и № 21 (ФСТЭК — Федеральная служба по техническому и экспортному контролю) образуют методическую основу мер: приказ № 17 устанавливает требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, а приказ № 21 определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных.

Аттестация — проверка и документальное подтверждение соответствия информационной системы установленным требованиям. Система, не прошедшая аттестацию и не отнесённая к ведомственному контуру, для обработки персональных данных участников и материалов дела не используется, независимо от удобства сервиса.

Что можно обрабатывать и где

Вид данных

Правовой режим

Где допустима обработка

Сведения, составляющие государственную тайну
режим государственной тайны; ст. 283 УК РФ

только в помещениях и системах, допущенных к работе со сведениями соответствующей степени секретности

Персональные данные участников

152-ФЗ (ст. 6, 9, 10, 11, 18); ПП РФ № 1119

в аттестованных информационных системах ведомственного контура

Данные предварительного расследования

ч. 1 ст. 161 УПК РФ

в изолированном контуре; передача вовне — только в случаях ч. 2, 4, 6 ст. 161 УПК РФ

Обезличенные фрагменты без идентификаторов

152-ФЗ (ст. 6, 9, 10, 11, 18); ПП РФ № 1154

в ведомственном контуре; вывод за его пределы не допускается

Общедоступная правовая информация

149-ФЗ

допустимо в любом контуре, в том числе публичном

Обезличивание снижает риск, но не выводит данные из-под охраны: «обезличенный фрагмент» и «общедоступная норма» — не одно и то же.

Субъект ответственности — конкретный человек

Ответственность персонифицирована: административная — по ст. 13.11 КоАП РФ за нарушение законодательства о персональных данных; дисциплинарная — по нормам трудового законодательства и ведомственных актов; уголовная — при наличии всех признаков конкретного состава УК РФ (раздел 1.1). Ссылка на «так настроен сервис» значения не имеет: решение об обработке принимает должностное лицо. Гарантеей служит не только внутренний контроль, но и судебный контроль — ст. 29, 125, 165 УПК РФ, — а также презумпция невиновности (ст. 14 УПК РФ).

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.