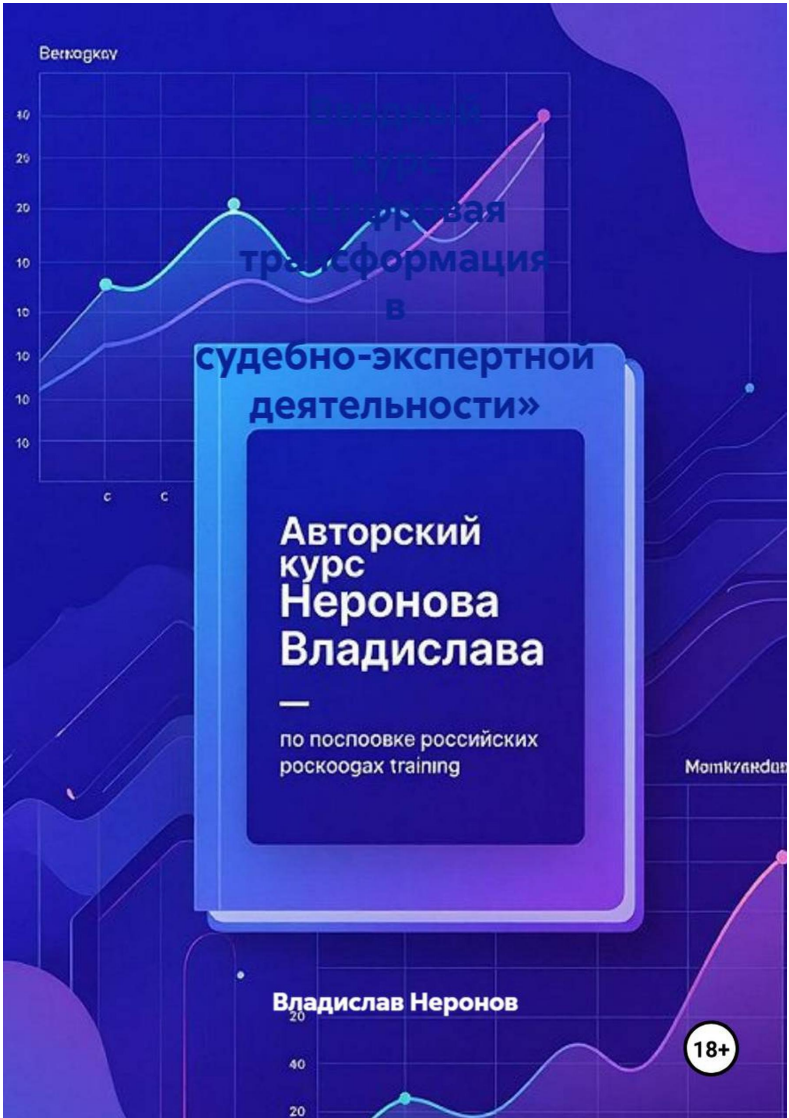

Авторский курс «Цифровая трансформация в судебно-экспертной деятельности»
Авторский курс Неронова Владислава
по поспоовке российских роскоодах training
Владислав Неронов
18+

Владислав Неронов

Вводный курс «Цифровая трансформация в судебно-экспертной деятельности»

https://litres.ru/74838624
SelfPub; 2026

Аннотация

Авторский курс Неронова Владислава по подготовке судебных экспертов в эпоху цифровой трансформации.

Содержание

Курс «Цифровая трансформация судебно-экспертной деятельности» 10

Лекция 1. Судебная экспертиза в эпоху цифровой трансформации: современное состояние отрасли и вектор её развития 10

Введение: почему это касается каждого эксперта даже гуманитария 10

1. Три источника давления на экспертную отрасль 11

2. Что это значит для эксперта на практике 12

3. Ключевое разграничение: цифровизация процедуры и цифровизация объекта 13

4. Мини-кейс 14

5. Куда движется отрасль: пять векторов на ближайшее десятилетие 15

Тест по лекции 1 16

Домашнее задание к лекции 1 17

Итог лекции 18

Курс «Цифровая трансформация судебно-экспертной деятельности» 19

Лекция 2. Электронный объект исследования: понятие, свойства, допустимость 19

Введение: главный сдвиг в мышлении 19

1. Понятие и структура электронного объекта 20
2. Подлинность и целостность: разграничение понятий 21
3. Копии, оригиналы и «проекции»: иерархия состояний объекта 22
4. Процессуальная допустимость: что требует суд 24
5. Мини-кейс 25
6. Что унести с лекции: три правила эксперта 25
Тест по лекции 2 26
Домашнее задание к лекции 2 28
Итог лекции 28
Курс «Цифровая трансформация судебно-экспертной деятельности» 30
Лекция 3. Целостность и достоверность цифрового объекта: идентификация, копирование, хеширование 30
Введение: доказательство живёт до начала исследования 30
1. Идентификация объекта: присвоение имени, которое нельзя перепутать 31
2. Копирование: как не уничтожить доказательство благими намерениями 32
3. Хеширование: математическая печать 33

неизменности
4. Типовые ошибки и их процессуальные последствия 35
5. Мини-кейс 36
6. Что унести с лекции: три правила 37
Тест по лекции 3 38
Домашнее задание к лекции 3 39
Итог лекции 40
Курс «Цифровая трансформация судебно-экспертной деятельности» 42
Лекция 4. Цифровая цепочка владения доказательством: от изъятия до исследования 42
Введение: доказательство — это путь, а не предмет 42
1. Понятие цифровой цепочки владения 43
2. Карта пути цифрового объекта: пять этапов 44
3. Кто несёт ответственность на каждом этапе: распределение ролей 46
Конец ознакомительного фрагмента. 47

Владислав Неронов
Вводный курс «Цифровая трансформация в судебно-экспертной деятельности»

Вводный курс «Цифровая трансформация в судебно-экспертной деятельности»

Вводный курс «Цифровая трансформация в судебно-экспертной деятельности»

Оглавление

Лекция 1. Судебная экспертиза в эпоху цифровой трансформации

Лекция 2. Электронный объект исследования

Лекция 3. Целостность и достоверность цифрового объекта

Лекция 4. Цифровая цепочка владения доказательством

Лекция 5. Методы цифровой фальсификации

Лекция 6. Электронная подпись и электронный документооборот как объект экспертизы

Лекция 7. Автоматизация экспертного производства

Лекция 8. Искусственный интеллект в судебной экспертизе

Лекция 9. Цифровая гигиена эксперта

Лекция 10. Эксперт 2.0

Содержание

Лекция 1. Судебная экспертиза в эпоху цифровой трансформации

Обзор ключевых трендов: электронные доказательства, цифровизация судопроизводства, новые объекты экспертизы. Дискуссионный вопрос: эксперт как участник цифровой экосистемы правосудия.

Лекция 2. Электронный объект исследования: понятие, свойства, допустимость

Цифровые документы, переписка, записи, метаданные — как объекты экспертного познания. Формирование понятийного аппарата, отличие цифрового объекта от его бумажной проекции.

Лекция 3. Целостность и достоверность цифрового объекта: идентификация, копирование, хеширование

Методы фиксации неизменности объекта. Ошибки при изъятии и хранении цифровых носителей, их процессуальные последствия для вывода эксперта.

Лекция 4. Цифровая цепочка владения доказательством:

от изъятия до исследования

Прослеживаемость объекта исследования на всех этапах. Стандарты работы эксперта с оригиналом, образом носителя и рабочими копиями.

Лекция 5. Методы цифровой фальсификации: от ретуши до генеративного синтеза

Современные технологии подделки изображений, аудио, видео и документов. Возможности и границы их экспертного выявления; вероятностный характер выводов.

Лекция 6. Электронная подпись и электронный документооборот как объект экспертизы

Проверка подлинности ЭП, анализ потоков документов, роль операторов ЭДО. Типовые вопросы эксперту и типовые ошибки в их формулировании.

Лекция 7. Автоматизация экспертного производства: цифровые инструменты лаборатории

Программно-аппаратные комплексы, автоматизированные рабочие места эксперта, ведение дел в электронных системах. Границы автоматизации: что остаётся за профессиональным суждением.

Лекция 8. Искусственный интеллект в судебной экспертизе: помощник, а не замена

Применение ИИ в распознавании, сравнении, поиске закономерностей. Риск «чёрного ящика»: проблема объяснимости и воспроизводимости результатов. Пределы допустимости ИИ-инструментов в производственной практике.

Лекция 9. Цифровая гигиена эксперта: защита данных, конфиденциальность, электронная подпись эксперта

Информационная безопасность объектов исследования и материалов дела. Персональные данные в экспертизе. Оформление и подписание заключения в электронной форме.

Лекция 10. Эксперт 2.0: профессиональные компетенции цифрового специалиста

Итоговая интегрирующая лекция. Модель компетенций эксперта цифровой эпохи: междисциплинарность, непрерывное обучение, коммуникация с судом и сторонами в цифровой среде. Перспективы развития отрасли на горизонте десяти лет.

Лекция 11. Нормативная база цифровой трансформации и технологии информационного моделирования: новый объект экспертизы

Курс «Цифровая трансформация судебно-экспертной деятельности»

Лекция 1. Судебная экспертиза в эпоху цифровой трансформации: современное состояние отрасли и вектор её развития

Введение: почему это касается каждого эксперта даже гуманитария

Уважаемые коллеги. Первый курс нашего цикла вводный и облегченный, и он адресован судебному эксперту любой специальности: почерковеду, строителю, автотехнику, бухгалтеру. Цифровая трансформация отрасли затронет всех, потому что меняется не методика меняются объекты исследований и форма работы.

Суд ещё десять лет назад изучал бумагу, показания и вещественные доказательства. Сегодня в делах всё больше

объектов, которые не существуют физически: переписка в мессенджерах, электронные договоры с квалифицированной подписью, записи с камер, метаданные файлов, данные бухгалтерских систем. Эксперт, который умеет работать только с «традиционными» объектами, рискует оказаться в положении мастера, ремонтирующего карбюратор, на СТО, где все машины — электрические.

Задача лекции 1 дать общую картину: где отрасль сейчас, что меняется и почему этот курс стоит пройти целиком.

1. Три источника давления на экспертную отрасль

Источник первый, доказательственная база стала цифровой.

Суд всё чаще назначает экспертизу электронных документов, записей и данных. Это означает: объект, который вы исследуете, существует в виде файла, копия которого технически идентична оригиналу, а «подлинность» — понятие из категории целостности данных, а не материального предмета.

Источник второй, судопроизводство оцифровывается.

Электронный документооборот в судах, подача заключе-

ния в электронной форме, видеоконференцсвязь при допросе эксперта. Форма представления заключения и подписания — уже не вопрос удобства, а вопрос процессуальной допустимости.

Источник третий, фальсификация стала доступной.

Инструменты, которые раньше требовали профессиональной студии (монтаж аудио и видео, ретушь изображений, подделка документов), сегодня есть в любом смартфоне и бесплатном редакторе. Генеративные модели умеют создавать реалистичный контент «из ничего». Объём потенциально недостоверных цифровых объектов в обороте растёт лавинообразно — и спрос на экспертов, умеющих это выявлять, растёт вместе с ним.

2. Что это значит для эксперта на практике

Следствия, которые уже сейчас видны в повседневной практике:

Расширение предметной области. В современном почерковедении и технико-криминалистической экспертизе документов появляются вопросы об электронной подписи, о происхождении файла-скана, о монтаже. Эксперт по «традиционным» объектам всё чаще встречает цифровые.

Смена формы работы. Приёмка материалов, переписка с судом, подписание и отправка заключения — в электронном виде. Умение работать с ЭП и защищёнными каналами становится базовой профессиональной гигиеной.

Рост ответственности. Цифровой объект легко копируется и, следовательно, легко подменяется. Ошибка в фиксации целостности (не вычислен хеш, не сохранены метаданные) может обесценить всё исследование — и она будет обнаружена на допросе.

Новые конкуренты и новые ожидания. Суды и стороны всё чаще ожидают от эксперта понимания цифровых объектов хотя бы на уровне корректной постановки задач и честного обозначения пределов компетенции.

3. Ключевое разграничение: цифровизация процедуры и цифровизация объекта

Важно с самого курса не путать два разных процесса.

Цифровизация процедуры — это когда по форме остаётся прежняя экспертиза (например, почерковедение), но подана она электронно, подписана ЭП, материалы переданы через защищённый канал. Здесь цифровизация — про форму.

Цифровизация объекта — это когда сам объект исследования является цифровым: файл записи, образ носителя,

база данных. Здесь цифровизация — про суть исследования, новые методики и новые риски.

Практический смысл разграничения: к первой ситуации эксперт может адаптироваться административно (обучиться ЭП и электронному документообороту). Ко второй — только методически: нужны новые знания, аппаратура и подходы. Большинство ошибок в отрасли возникает там, где эксперт смешивает эти уровни — например, исследует «скриншот» как документ, не понимая, что объектом должен быть исходный файл.

4. Мини-кейс

В районном суде по гражданскому спору о займе назначена почерковедческая экспертиза расписки. Вместе с распиской истец представил «подтверждающее» фото: смартфон на столе, на экране переписка в мессенджере с признанием долга. Вопросы в определении сформулированы так: «выполнен ли текст на фотографии действиями ответчика; соответствует ли изображение действительности?»

Вопрос для обсуждения: почему суд совершил типовую ошибку в постановке вопросов, и какие два разных исследования фактически «спрятаны» в этой формулировке? Ответ развёрнуто в домашнем задании ниже.

5. Куда движется отрасль: пять векторов на ближайшее десятилетие

Электронное производство как норма. Заключение, подписанное ЭП и поданное в электронном виде, станет стандартом, а не исключением.

Стандартизация цифровых объектов. Развитие единых требований к изъятию, фиксации и представлению цифровых доказательств — включая прослеживаемость целостности на всех этапах.

Автоматизация рутины. Типовые операции (предварительная обработка, ведение производства, формирование отчётов) — под программные комплексы. Профессиональное суждение остаётся за экспертом.

ИИ-инструменты с объяснимостью. Вспомогательные алгоритмы войдут в практику, но судебная экспертиза консервативна по своей сути: вывод эксперта должен быть объясним, воспроизводим и проверяем. «Чёрный ящик» не станет основанием категоричного вывода.

Междисциплинарность эксперта. Востребованным станет специалист «на стыке»: юрист с цифровыми компетенциями, инженер, понимающий процессуальные требования, и т. д.

Тест по лекции 1

1. Цифровизация судебной экспертизы затрагивает:

а) только компьютерно- техническую экспертизу;

б) всех экспертов независимо от специальности;

в) только экспертов, работающих с аудио и видео.

2. Исследуемый цифровой объект отличается от вещественного тем, что:

а) не может быть подделан;

б) его копия технически идентична оригиналу, а подлинность определяется через целостность данных;

в) не требует фиксации при приёмке.

3. «Цифровизация объекта» означает, что:

а) заключение подаётся в электронном виде;

б) экспертиза подписывается электронной подписью;

в) сам объект исследования является цифровым и требует новых методик.

4. Типовая ошибка при постановке вопросов эксперту по цифровым объектам:

а) слишком короткие вопросы;

б) смешение разных исследований в одном вопросе и вопросы правового характера;

в) избыточная детализация фактических обстоятельств.

5. Наиболее уязвимое звено при работе с цифровым объектом:

а) вычисление хеш-суммы;

б) фиксация целостности и прослеживаемости объекта до начала исследования;

в) оформление фототаблицы.

Ключ: 1 — б; 2 — б; 3 — в; 4 — б; 5 — б.

Домашнее задание к лекции 1

Кейс из раздела 4. В свободной форме (до одной страницы) объясните: какие два разных исследования «спрята-

ны» в формулировке вопросов суда; почему ни один почерковед не должен отвечать на второй из них; как следовало бы переформулировать вопросы (дайте свою формулировку).

Аудит собственной практики. Составьте таблицу из двух колонок: «Какие объекты из моей практики за последние 12 месяцев имели цифровую природу или цифровое сопровождение» и «Что мне не хватало для корректной работы с ними». Если таких объектов не было — укажите, почему (субъективная оценка): не встречались либо я их не замечал.

Один абзац на вырост. Ответьте письменно: какой из пяти векторов развития отрасли (раздел 5) отразится на вашей специальности раньше всего и почему.

Домашнее задание проверке не подлежит — оно для вас. Но мои коллеги на следующих лекциях будут возвращаться к его результатам.

Итог лекции

Судебная экспертиза меняется не потому, что кто-то «продвигает цифру», а потому, что изменились доказательства. Объекты стали цифровыми, форма — электронной, фальсификация — массовой. Эксперту, который хочет остаться в профессии востребованным, нужны три вещи: понимание природы цифровых объектов, цифровая гигиена (фиксация, целостность, ЭП) и честное обозначение пределов компетенции. Этому и посвящён курс.

Курс «Цифровая трансформация судебно-экспертной деятельности»

Лекция 2. Электронный объект исследования: понятие, свойства, допустимость

Введение: главный сдвиг в мышлении

В лекции 1 мы установили: доказательства стали цифровыми. Сегодня разберём фундаментальное понятие **электронный объект исследования**. И сразу главный сдвиг, который предстоит сделать мышлению каждого эксперта.

Вещественное доказательство существует в единственном экземпляре: это конкретная бумага, конкретный предмет. Его подлинность это «тот самый» предмет, изъятый в конкретном месте. Цифровой объект устроен иначе: он существует как **запись данных**, и его копия технически неотличима от оригинала. Понятие «тот самый» заменяется понятием **«неизменный с момента фиксации»** и вот здесь начинаются и возможности, и ловушки цифрового мира.

Задача лекции 2 освоить понятийный аппарат: что такое электронный объект, из чего он состоит, чем «подлинность» отличается от «целостности» и почему скриншот — это не документ, а лишь его бледная тень.

1. Понятие и структура электронного объекта

Электронный объект исследования — это совокупность записанных в цифровом виде данных, представленных для экспертного исследования, вместе с их служебной информацией.

Структурно любой цифровой объект состоит из двух слоёв:

Слой содержания — то, что «видит» пользователь: текст переписки, изображение, звук, запись. Это то, что суд и стороны «видят» и обсуждают.

Слой служебных данных (метаданные) — сведения о самом объекте: время и обстоятельства создания, программа-создатель, устройство, версия формата, история редактирования, геометки фотографий. Метаданные не видны в обычном просмотре, но именно они часто дают ответ на вопрос «когда и как создан объект».

Ключевая мысль: экспертиза цифрового объекта в общем случае — это исследование двух слоёв одновременно. Сторона, которая «потеряла» метаданные (пересохрани-

ла фото из мессенджера, переписала файл), фактически уничтожила половину доказательства — часто самую ценную половину.

К слоям добавляется третий элемент — **контекст представления**: формат файла, способ отображения, версия программы. Один и тот же документ Word на разных версиях может отображаться с переносами; одно и то же аудио — иметь разный слышимый результат после кодирования. Эксперт обязан понимать, что он исследует: исходный объект или его «проекцию» в конкретной среде.

2. Подлинность и целостность: разграничение понятий

Это центральное разграничение всей лекции — и постоянный источник путаницы в вопросах судов.

Подлинность (аутентичность) — ответ на вопрос: действительно ли объект происходит от заявленного источника (автора, устройства, момента)? Это утверждение о происхождении.

Целостность — ответ на вопрос: не изменён ли объект с момента определённой фиксации? Это утверждение о неизменности.

Вещественному миру это различие почти незнакомо: подлинная расписка и есть «не изменённая с момента создания». В цифровом мире это разные вещи: файл может быть

целостным (не изменялся с изъятия, подтверждено хеш-суммой), но **неподлинным** (создан злоумышленником за день до «фиксации»).

Практический вывод для эксперта: корректное экспертное заключение отвечает либо на вопрос о целостности («объект не изменялся с момента выгрузки, что подтверждается...»), либо на вопрос о происхождении/подлинности («объект создан программой X на устройстве Y в период Z»). Смешение этих утверждений в одной формулировке — методическая ошибка, которую легко вскрыть на допросе.

Инструмент фиксации целостности — хеш-сумма (криптографический «отпечаток» файла, обычно SHA-256). Два одинаковых файла дают одинаковую хеш-сумму; изменение даже одного байта меняет её полностью. Хеш-сумма — это то, что в цифровом мире заменяет печать и подпись на конверте. Мы подробно разберём её в лекции 3.

3. Копии, оригиналы и «проекции»: иерархия состояний объекта

Поскольку копия цифрового объекта технически идентична оригиналу, юристы и суды часто неправильно переносят на цифру понятие «копия» из вещественного мира. Эксперту важно держать в голове иерархию:

Исходный объект — данные в среде их естественного существования: переписка на сервере мессенджера, файл в

исходном хранилище. Наиболее доказательно ценен, но часто недоступен.

Образ (полная копия) носителя — посекторная копия устройства (жёсткого диска, телефона), вместе со всей служебной и удалённой информацией. Стандарт объекта для компьютерно-технических экспертиз.

Выгрузка/экспорт — полная выгрузка переписки или данных средствами самой системы (например, архив чата с метаданными). Сохраняет значительную часть служебной информации.

Файловая копия — сам файл, скопированный без изменений. Целостность сохранена, но «история происхождения» зависит от способа получения.

Скриншот, распечатка, пересохранённый файл — проекция объекта. Демонстрирует содержание, но по определению утратила метаданные исходника. Доказательная ценность — минимальная и требует отдельного обоснования.

Типовая ошибка, которую вы уже встретите в судах: сторона представит распечатку скриншотов как «подлинник переписки». Задача эксперта — корректно обозначить, что исследуется проекция, и честно указать, какие выводы на её основе возможны (обычно — вероятные или невозможные).

4. Процессуальная допустимость: что требует суд

Электронный объект, чтобы стать доказательством, должен пройти процессуальные фильтры. Для эксперта важно знать четыре критерия, по которым суды чаще всего «заворачивают» цифровые материалы:

Способ получения. Объект получен в ходе процессуального действия (осмотр, выемка, нотариальный протокол) либо истребован. «Прислал клиент по WhatsApp» — не способ получения.

Фиксация источника. Установлено, откуда объект: какое устройство, какой аккаунт, какой носитель. Без источника — объект «висит в воздухе».

Неизменность. Подтверждена целостность с момента фиксации (протокол, хеш, показания).

Возможность проверки. Другая сторона и суд имеют возможность убедиться в объекте; эксперт получает его в состоянии, пригодном для независимой проверки.

Обратите внимание: в четырёх критериях нет слова «качество». Суд может принять объект посредственного качества — если соблюдены критерии получения и фиксации. И наоборот: идеально «чистый» по качеству скриншот не спасёт отсутствием источника.

5. Мини-кейс

Арбитражный спор о поставке. Ответчик ссылается на переписку с истцом, где тот «признал» некомплект. В дело представлены: (а) распечатка скриншотов переписки в мессенджере, заверенная ответчиком; (б) файл «чат.pdf», полученный от ответчика по электронной почте; (в) от ответчика отказались предоставить телефон, с которого велась переписка.

Сторона истца просит признать переписку недопустимым доказательством. Суд назначает экспертизу представленных материалов.

Вопросы для размышления (развёрнуто — в домашнем задании):

Что реально исследует эксперт в объектах (а) и (б) — цифровые объекты или их проекции?

Какие из четырёх критериев допустимости не соблюдены и кем?

Может ли эксперт дать категоричный вывод о подлинности переписки по объектам (а) и (б)? Почему?

6. Что унести с лекции: три правила эксперта

Исследуй оба слоя. Содержание без метаданных полу-

доказательство. Метаданные без понимания содержания — пустой формализм.

Называй вещи по именам. В заключении не «документ», а «файловая копия документа формата PDF, хеш-сумма...»; не «переписка», а «распечатка скриншотов переписки, являющаяся проекцией...». Точность наименований — ваша защита на допросе.

Разграничивай утверждения. Целостность — про неизменность с фиксации. Подлинность — про происхождение. Не позволяйте суду и сторонам смешивать их в вопросах.

Тест по лекции 2

1. Электронный объект исследования включает:

а) только видимое пользователю содержание;

б) содержание, метаданные и контекст представления;

в) только файл в формате, понятном суду.

2. Целостность объекта — это:

а) отсутствие монтажа в записи;

б) неизменность объекта с момента определённой фикса-

ции;

в) принадлежность объекта заявленному автору.

3. Скриншот переписки относится к:

а) образу носителя;

б) выгрузке с метаданными;

в) проекции объекта с минимальной доказательной ценностью.

4. Два одинаковых файла:

а) имеют одинаковые хеш-суммы, а изменение одного байта меняет хеш полностью;

б) имеют хеш-суммы, зависящие от даты копирования;

в) не имеют хеш-сумм, если не подписаны ЭП.

5. Суд принимает цифровой объект как доказательство прежде всего по:

а) качеству изображения;

б) соблюдению критериев получения, фиксации источника и неизменности;

в) количеству страниц распечатки.
Ключ: 1 — б; 2 — б; 3 — в; 4 — а; 5 — б.

Домашнее задание к лекции 2

Кейс из раздела 5. В свободной форме (до одной страницы) ответьте на три вопроса из кейса. Особо сформулируйте: какие вопросы вы, как эксперт, поставили бы суду в ходатайстве о предоставлении дополнительных материалов.

Ревизия формулировок. Вспомните (или смоделируйте) 3 формулировки вопросов из определений судов, которые вы встречали по «цифровым» объектам. Перепишите каждую по правилам лекции: раздельно про содержание, целостность и происхождение. Соотнесите с ошибкой из мини-кейса лекции 1.

Практика «проекций». Найдите у себя в прошедших делах (или в открытой практике) объект-проекцию, который суд принял как полноценное доказательство. Одним абзацем: какие риски для вывода создала эта проекция и как бы вы сейчас предложили её исследовать.

Итог лекции

Электронный объект это содержание плюс метаданные плюс контекст. Подлинность и целостность — разные утвер-

ждения, и эксперт обязан их разграничивать. Объекты образуют иерархию от исходника до проекции, и доказательная ценность определяется положением в этой иерархии. Суд принимает объект по критериям получения, источника, неизменности и проверяемости — а не по «красоте» распечатки.

Курс «Цифровая трансформация судебно-экспертной деятельности»

Лекция 3. Целостность и достоверность цифрового объекта: идентификация, копирование, хеширование

Введение: доказательство живёт до начала исследования

В лекции 2 мы разграничили целостность и подлинность. Сегодня — практический урок о том, как целостность обеспечивается технически. И начнём с неудобной истины: **большая часть потерь доказательственной ценности происходит до того, как объект попал к эксперту** — при изъятии, пересылке, копировании и хранении. Но именно эксперт оказывается последним, кто может заметить и зафиксировать эти потери. Суд ждёт от вас не только вывода, но и честной оценки того, в каком состоянии объект дошёл до исследования.

Задача лекции 3 — освоить три практических инструмента: идентификацию объекта, корректное копирование и хеширование.

1. Идентификация объекта: присвоение имени, которое нельзя перепутать

Первый акт работы с любым цифровым объектом — его однозначная идентификация. Практическое правило: у каждого объекта должно быть описание, по которому другой эксперт (или оппонент) сможет найти и распознать его без дополнительных пояснений.

Минимальный набор идентификационных сведений для файла:

Имя файла — как представлено в материалах (при обязательной оговорке: имя можно переименовать, поэтому оно не является доказательственным признаком, а лишь рабочим обозначением).

Размер в байтах — точный, а не «округлённый» килобайтами.

Хеш-сумма (об этом ниже) — главный идентификатор.

Формат/расширение — и проверка соответствия: расширение .jpg при внутреннем формате PNG — уже сигнал о вмешательстве.

Источник и способ получения — с какого носителя, чьего устройства, кем передан, когда.

Для носителя (телефон, флешка, диск) добавляются: производитель и модель устройства, серийные номера, объём, состояние файловой системы. Для образа носителя — дополнительно сведения о методе копирования (см. раздел 2).

Практический стандарт: идентификация оформляется в акте приёмки (протоколе) и затем дословно переносится в вводную часть заключения. Расхождение идентификации в акте и в заключении — формальный дефект, за который эксперт может быть допрошен.

2. Копирование: как не уничтожить доказательство благими намерениями

Копировать цифровой объект можно «правильно» и «неправильно». Разница — в полноте и невмешательстве.

Правило первое: оригинал не трогаем. Все исследования ведутся на рабочих копиях. Оригинальный носитель хранится в исходном состоянии, желательно с защитой от записи (в идеале — аппаратной, через блокировщика записи). Любое «просто открою файл посмотреть» — это уже вмешательство: открытие документа в редакторе меняет служебные данные (время последнего доступа, иногда метаданные).

Правило второе: для носителей — только посекторное копирование (образ). Обычное «скопировать файлы» на новый диск — это потеря: удалённых файлов, служебных структур, разметки, истории операций файловой системы.

Правильный подход — создание **посекторного образа** носителя средствами специализированного ПО с обязательной верификацией (сравнением хеш-сумм оригинала и образа). Образ создан корректно, если его хеш совпадает с хешем оригинала.

Правило третье: не конвертировать, не сжимать, не «чистить». Каждый пересохранённый, конвертированный или «сжатый для удобства» файл — это новый объект, а не копия исходного. Сторона, которая прислала «фотографии по почте» вместо оригинальных файлов с телефона, уничтожила метаданные и, возможно, часть признаков. Ваша задача — не ругать (не ваша компетенция), а точно зафиксировать утраты в заключении.

Правило четвёртое: фиксируй цепочку владения. Кто и когда передал объект, где он хранился, кто имел доступ, когда и кому передан дальше. Цепочка владения в цифровом мире заменяет понятие «непрерывного наблюдения» за вещественным доказательством.

3. Хеширование: математическая печать неизменности

Хеш-функция принимает на вход данные любого объёма и возвращает короткую строку фиксированной длины («отпечаток»). Ключевые свойства, делающие её инструментом эксперта:

Детерминированность: один и тот же вход всегда даёт один и тот же выход.

Чувствительность: изменение даже одного байта исходных данных полностью меняет отпечаток (эффект «лавины»).

Практическая необратимость: по отпечатку нельзя восстановить данные; крайне маловероятно найти два разных файла с одинаковым отпечатком (при современном стандарте — **SHA-256**).

Что это даёт эксперту на практике:

Приёмка объекта. Хеш вычисляется сразу при получении файла/носителя. Значение вносится в акт приёмки. С этого момента любое последующее сравнение однозначно ответит: «тот же объект или другой».

Передача на исследование. Рабочая копия имеет тот же хеш — значит, исследование велось именно того объекта, который поступил.

Хранение и возврат. Перед возвратом носителя стороне хеш сверяется с актом приёмки. Расхождение — сигнал о вмешательстве в период хранения.

Ответ на допросе. «Как вы доказываете, что исследовали не изменённый объект?» — «Вычислением и сверкой хеш-сумм на этапах приёмки, копирования и возврата; значения приведены в заключении на странице N».

Что хеш НЕ даёт: он не подтверждает **подлинность** и **происхождение** объекта. Файл, созданный злоумышлен-

ником час назад, имеет абсолютно «законную» хеш-сумму. Хеш отвечает только на вопрос о неизменности **с момента первой фиксации**. Эксперт, который в заключении пишет «хеш-сумма подтверждает подлинность документа», совершает грубую методическую ошибку — и именно её мы будем ловить в кейсах курса.

Практика вычисления: стандартные утилиты командной строки (certutil в Windows, sha256sum в Linux/Mac), специализированные комплексы при работе с носителями. Важно: хеш вычисляется по оригинальному массиву данных файла, а не по его «отображению» — PDF-просмотрщик, печать, скриншот порождают иные данные с иными хешами.

4. Типовые ошибки и их процессуальные последствия

Сводка ошибок, которые вы будете находить в материалах (и которых должны избегать сами):

Хеш не вычислялся вовсе. Объект «плавает»: оппонент на допросе заявляет, что предоставленный ему файл отличается. Защиты нет.

Хеш вычислен от неверного объекта. От скриншота вместо файла, от копии вместо оригинала, от архива, внутри которого уже изменённые данные.

Копирование «поверх» оригинала. Носитель продолжал использоваться после изъятия — удалённые данные пе-

резаписаны, целостность утрачена невозвратно.

Работа без блокировки записи. Подключение носителя для «просмотра» изменило служебные данные — формально объект уже не идентичен изъятому.

Цепочка владения не документирована. Объект двое суток «побывал» в кабинете без фиксации — оппонент получает основание оспорить весь путь доказательства.

Подмена понятий в заключении: «хеш подтверждает подлинность» (ошибка смешения целостности и подлинности — см. лекцию 2).

Каждая из этих ошибок на допросе превращается в вопрос оппонента: «Каким образом объект, оказавшийся у вас, является тем же объектом, что был изъят?» — и отсутствие ответа обесценивает заключение, каким бы качественным ни было само исследование.

5. Мини-кейс

По корпоративному спору изъята флешка с бухгалтерскими файлами. Спустя три недели материалы поступают к эксперту. В сопроводительном письме указано: «флешка передаётся в состоянии, изъятом при осмотре». Эксперт подключает носитель к рабочему компьютеру для «первичного просмотра», находит нужные файлы, копирует их на рабочий диск, вычисляет хеш-суммы уже скопированных файлов — и приступает к исследованию.

На допросе представитель ответчика заявляет: за три недели до передачи к носителю имел доступ системный администратор компании, а эксперт не может подтвердить, что исследует данные в том виде, в каком они были изъяты.

Вопросы для размышления (развёрнуто — в домашнем задании):

Какие действия эксперта уже на первом этапе лишили его возможности опровергнуть заявление оппонента?

Что следовало сделать при приёмке носителя и что — при работе с ним?

Может ли заключение в такой ситуации содержать утверждение о целостности данных? В какой форме допустим вывод?

6. Что унести с лекции: три правила

Хеш — в первый час работы с объектом. Не «когда дойдут руки», а при приёмке. Значение — в акт, из акта — в заключение.

Хеш отвечает за неизменность, а не за подлинность. Не позволяйте ни себе, ни суду смешивать эти утверждения.

Оригинал неприкосновенен. Исследование — только на верифицированных копиях; любое касание оригинала — задокументированное и осознанное решение.

Тест по лекции 3

1. Хеш-сумма объекта служит для:

а) подтверждения авторства файла;

б) подтверждения неизменности данных с момента вычисления;

в) ускорения копирования файлов.

2. Корректный способ работы с изъятым носителем:

а) исследование на оригинале с аккуратным обращением;

б) создание посекторного образа с верификацией и исследование на копии;

в) копирование нужных файлов на рабочий диск и исследование их.

3. Два файла имеют разные хеш-суммы SHA-256. Это означает:

а) файлы точно различаются хотя бы одним байтом;

б) файлы созданы разными программами;

в) один из файлов подделан.

4. Наиболее грубая методическая ошибка в заключении:

а) указание наименования утилиты вычисления хеша;

б) утверждение, что совпадение хеш-суммы подтверждает подлинность документа;

в) указание размера файла в байтах.

5. Открытие документа в редакторе «для просмотра» перед исследованием:

а) не влияет на объект;

б) может изменить служебные данные объекта и лишить эксперта доказательства неизменности;

в) допустимо при наличии свидетеля.

Ключ: 1 — б; 2 — б; 3 — а; 4 — б; 5 — б.

Домашнее задание к лекции 3

Кейс из раздела 5. Ответьте на три вопроса кейса (до

одной страницы). Отдельно сформулируйте, какой вывод о целостности допустим в данной ситуации и в какой форме (категоричный/вероятный/о невозможности установить).

Практическое упражнение. Возьмите любой файл на своём компьютере. Вычислите его хеш-сумму SHA-256 стандартной утилитой. Откройте файл, внесите и сохраните одно незаметное изменение (например, пробел в конце документа), вычислите хеш повторно. Сравните значения. Одним абзацем опишите наблюдение и объясните, почему это свойство — основа экспертизы целостности.

Ревизия практики. Вспомните 2–3 объекта из ваших последних дел (или смоделируйте). По каждому: вычислялась ли хеш-сумма при приёмке? документировалась ли цепочка владения? исследовался ли оригинал? Что из этого вы измените в своей практике уже с следующего дела?

Итог лекции

Целостность цифрового объекта — не декларация, а результат технической дисциплины: идентификация при приёмке, посекторное копирование с верификацией, хеширование на каждом этапе, документированная цепочка владения. Хеш-сумма — главный идентификатор объекта и инструмент доказательства неизменности, но она ничего не говорит о подлинности и происхождении. Эксперт, который освоил эту дисциплину, защищён на допросе; эксперт, который её

игнорирует, рискует потерять всё заключение из-за одного вопроса оппонента.

Курс «Цифровая трансформация судебно-экспертной деятельности»

Лекция 4. Цифровая цепочка владения доказательством: от изъятия до исследования

Введение: доказательство — это путь, а не предмет

В лекции 3 мы освоили технические инструменты фиксации целостности. Сегодня собираем их в целостную систему. Вещественному доказательству в классическом понимании не нужен «паспорт пути»: предмет изъяли, упаковали, исследовали — и физический носитель сам является гарантией того, что это «тот самый» предмет.

Цифровой объект такой гарантии не имеет: его нельзя «узнать на ощупь». Единственное, что связывает объект, лежащий у эксперта, с объектом, изъятым при осмотре, — это **непрерывная и документированная цепочка владения**. Разрыв цепочки — даже на день, даже «в кабинете у

руководителя» — это разрыв доказательственной связи, который оппонент использует всегда, когда ему это выгодно.

Задача лекции 4 выстроить полную модель пути цифрового объекта: этапы, участники, документы, типовые разрывы и способы их предотвращения.

1. Понятие цифровой цепочки владения

Цифровая цепочка владения — это последовательность зафиксированных переходов цифрового объекта между участниками процесса (и вне его) с подтверждением неизменности объекта на каждом переходе.

Формула проста: **каждый переход = документ + сверка целостности**.

Если объект переходит от изъявшего лица к эксперту — должен быть документ о передаче и (в идеале) сверка хеш-суммы или её защита иными средствами (упаковка с печатями, опечатанные носители). Если объект хранится — должен быть понятен режим хранения и круг допущенных лиц. Если объект возвращается — сверка на выходе.

Ключевая мысль: цепочка владения — это не формальность для протокола. Это единственное основание, по которому эксперт вправе в заключении утверждать: «исследованию подвергнут объект, поступивший в материалов дела как…». Всё, что предшествовало первой фиксации, эксперт не подтверждает — он лишь корректно указывает пределы

своих знаний.

2. Карта пути цифрового объекта: пять этапов

Этап 1. Возникновение и изъятие (или добровольное предоставление).

Объект появляется в процессе: выемка носителя, изъятие при осмотре, истребование, предоставление стороной. Что критично на этом этапе:

фиксация источника (устройство, аккаунт, носитель) — без этого объект «без родословной»;

фиксация состояния (включён/выключен носитель, подключён ли к сети, применены ли блокировщики записи);

первичная упаковка с исключением вмешательства (опечатанные носители, контрольные пломбы, для файлов — вычисление хеша прямо при изъятии, если это возможно).

Этап 2. Хранение до исследования.

Здесь чаще всего теряется доказательственная ценность. Требования:

круг допущенных лиц минимален и документирован;

носители хранятся в условиях, исключающих случайное подключение;

для файлов — хранение в неизменном виде с известным

хешем;

журнал доступа (кто, когда, зачем) — хотя бы минимальный.

Этап 3. Передача эксперту.

Документ передачи + сверка. Идеальная практика: эксперт при приёмке вычисляет хеш и сравнивает со значением в акте изъятия/передачи. На практике часто хеш при изъятии не вычислялся — тогда эксперт фиксирует хеш **на момент приёмки** и честно указывает в заключении: «сведение о неизменности объекта до момента поступления не подтверждается, что ограничивает выводы о происхождении объекта».

Этап 4. Исследование.

Работа только на верифицированных копиях (лекция 3). Рабочая копия — с тем же хешем, что и оригинал. Все манипуляции документируются: использованное ПО, версии, параметры. Это база для воспроизводимости исследования другим экспертом.

Этап 5. Возврат, хранение после исследования, приобщение.

Перед возвратом носителя — финальная сверка хеша. Копии, созданные в ходе исследования, учитываются: где хранятся, кто имеет доступ, когда уничтожаются (если уничто-

жаются — протоколом).

3. Кто несёт ответственность на каждом этапе: распределение ролей

Эксперт часто считает, что всё, что было «до приёмки», — не его проблема. Это заблуждение: допрос строится именно вокруг стыков.

Изъятие, фиксация источника — зона следователя, суда, нотариуса, стороны. Эксперт не отвечает за изъятие, но обязан **заметить и отразить дефекты** изъятия в заключении: носитель подключён к сети, упаковка нарушена, источник объекта не установлен.

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.