УДК 343.985 : 343.575

СПЕЦИФИКА ТАКТИКИ ДОПРОСА ОБВИНЯЕМЫХ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Яковлев Даниил Сергеевич

Алтайский государственный университет, Барнаул
sega708-1980@mail.ru

THE SPECIFICS OF INTERROGATION TACTICS OF THE ACCUSED IN CASES ABOUT CRIMES IN THE FIELD OF COMPUTER INFORMATION

Yakovlev Daniil S.

Altai State University, Barnaul
sega708-1980@mail.ru

Аннотация. В статье рассматриваются особенности тактики допроса обвиняемых по делам о компьютерных преступлениях. Автор анализирует специфику киберпреступлений, влияющую на криминалистические и психологические аспекты допроса, включая особенности поведения обвиняемых, использование цифровых доказательств и противодействие с их стороны. В статье детально структурированы основные стадии допроса: подготовительная (включая анализ материалов дела, изучение личности, техническую оснащенность и планирование), стадия непосредственного проведения (с акцентом на виды вопросов и психологические аспекты) и завершающая (оценка результатов и рефлексия следователя). Особое внимание уделяется необходимости привлечения IT-экспертов и работе с цифровыми следами. Делается вывод, что успешность допроса при расследовании киберпреступлений напрямую зависит от комплексной подготовки, гибкой тактики, учитывающей личность допрашиваемого, и грамотного использования технических средств. Предлагаются практические рекомендации по эффективному проведению допроса с учетом технической сложности и преступлений в сфере информационных технологий. Исследование может быть

Abstract. The article discusses the specifics of the tactics of interrogation of defendants in cases of computer crimes. The author analyzes the specifics of cybercrimes affecting the forensic and psychological aspects of interrogation, including the behavior of the accused, the use of digital evidence and their opposition. The main stages of the interrogation are structured in detail in the article: preparatory (including analysis of case materials, personality study, technical equipment and planning), the stage of direct conduct (with an emphasis on the types of questions and psychological aspects) and the final (evaluation of the results and reflection of the investigator). Special attention is paid to the need to involve IT experts and work with digital footprints. It is concluded that the success of interrogation in the investigation of cybercrimes directly depends on comprehensive training, flexible tactics that take into account the personality of the interrogated, and the competent use of technical means. Practical recommendations for effective interrogation are offered, taking into account the technical complexity and crimes in the field of information technology. The research may be useful to investigators, interrogators, field officers and other specialists involved in the investigation of cybercrimes.

полезно следователям, дознавателям, оперативным работникам .

Ключевые слова: тактика допроса, компьютерные преступления, киберпреступность, расследование, цифровые доказательства, противодействие следствию

Keywords: interrogation tactics, computer crimes, cybercrime, investigation, digital evidence, counteraction to the investigation

Для цитирования: *Яковлев Д.С.* Специфика тактики допроса обвиняемых по делам о преступлениях в сфере компьютерной информации // Проблемы правовой и технической защиты информации. 2025. № 13. С. 101–108.

For citation: *Yakovlev D.S.* Specifics of tactics of interrogation of accused persons in cases of crimes in the field of computer information. *Problems of Legal and technical protection of information*. 2025. No. 13. P. 101–108.

Как известно, допрос участников уголовного процесса (потерпевших, свидетелей, обвиняемых) по делам о преступлениях в сфере компьютерной информации требует учета специфики данного вида преступной деятельности. Криминалистическая тактика определяет эти приемы как систему научно обоснованных методов, обеспечивающих оптимальное получение и фиксацию доказательственной информации.

Технологичность и транснациональный характер киберпреступлений, активно исследуемые в криминалистике в последние годы, диктуют необходимость новых тактических решений, включая работу с цифровыми следами и преодоление противодействия расследованию [10–15].

При анализе преступлений в сфере компьютерной информации важно учитывать статистику: в 87% случаев подозреваемыми и обвиняемыми оказываются новички, или так называемые скрипт-кидди (молодые хакеры с ограниченными навыками) [7, с. 69]. Значительно реже правоохранительные органы сталкиваются с опытными хакерами, организаторами киберпреступных группировок или разработчиками вредоносного программного обеспечения (далее по тексту — ПО).

Эти особенности напрямую влияют на тактику допроса. Поскольку такие лица, как правило, не имеют устойчивой противоправной установки и глубоких познаний в юриспруденции, в ходе допроса эффективно применяется тактика, направленная на *формирование у обвиняемого личной заинтересованности в сотрудничестве со следствием*. Это позволяет разрешить конфликтную ситуацию в пользу следствия без применения сложных психологических методик.

Наглядной иллюстрацией данного подхода является уголовное дело № 1-954/2019, рассмотренное Заводским районным судом г. Кемерова по ч. 2 ст. 273 Уголовного кодекса Российской Федерации (далее — УК РФ). Подсудимый К., имевший лишь 8 классов образования, не работавший и обладавший низким уровнем IT-навыков, использовал для совершения преступления готовое вредоносное ПО, приобретенное у неустановленных лиц[1].

Тактика его допроса была выстроена следующим образом:

1. *Акцент на очевидность и неопровержимость доказательств.* Материалы дела свидетельствуют, что следствие рас-

[1] Приговор Заводского районного суда г. Кемерово (Кемеровская область) от 12.12.2019 года по делу № 1-954/2019 // Актофакт : [сайт]. URL: https://actofact.ru/case-42RS0005-1-954-2019-2019-12-03-2-0/?ysclid=mhet66zgal658903082 (дата обращения: 31.10.2025).

полагало неоспоримыми цифровыми уликами: данными о арендованных серверах, аккаунтах, через которые распространялось вредоносное ПО, а также о более чем 42 тысячах архивов с похищенной информацией. Ознакомление обвиняемого с объемом собранных доказательств создало почву для осознания бессмысленности отрицания своей вины.

2. *Разъяснение преимуществ особого порядка и досудебного соглашения*. Ключевым тактическим приемом стало разъяснение подсудимому положений гл. 40.1 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ). Ему была детально объяснена процедура и *последствия заключения досудебного соглашения о сотрудничестве*: существенное смягчение наказания (применение ч. 2 ст. 62 УК РФ, что ограничивает срок лишения свободы половиной от максимального) и возможность избежать реального лишения свободы.

3. *Создание условий для активного способствования раскрытию преступления*. Следствие не ограничилось пассивным признанием вины. От подсудимого было получено активное содействие: он неоднократно давал показания, изобличающие его самого, а также оказывал помощь в проведении оперативно-розыскных мероприятий, направленных на изобличение других лиц, занимающихся аналогичной деятельностью. Это стало исполнением его части обязательств по соглашению и было оценено судом как важное смягчающее наказание обстоятельство.

В результате грамотно выбранной тактики, основанной на работе с личностью обвиняемого и его заинтересованностью в смягчении участи, был достигнут комплексный положительный результат: подсудимый полностью признал вину, способствовал раскрытию преступления, а суд, учитывая его активную помощь, назначил наказание в виде 2 лет лишения свободы условно. Данный пример демонстрирует, что в отношении «скрипт-кидди» эффективной является тактика, сочетающая демонстрацию силы доказательств с предложением четкого и выгодного для обвиняемого процессуального алгоритма действий.

Теперь рассмотрим основные стадии допроса обвиняемых по делам о компьютерных преступлениях.

1. Подготовка к допросу по делам о киберпреступлениях

1.1. *Анализ материалов дела*

На этом этапе следователь должен:

– изучить временные рамки преступления, IP-адреса и другие технические данные, позволяющие восстановить хронологию событий и установить причастность подозреваемого;

– проверить достоверность источников информации на предмет возможных искажений, ошибок или умышленной дезинформации;

– выявить логические связи между эпизодами и обстоятельствами, указывающими на вину или невиновность подозреваемого.

На основе анализа формулируются четкие, логичные вопросы, исключающие двусмысленность или «ловушки». Также определяется тактика допроса, методы контроля над процессом и необходимость временных ограничений.

Техническая подготовка включает сбор и проверку цифровых доказательств (файлы, записи), а также обеспечение работоспособности оборудования для их воспроизведения. В сложных случаях целесообразно привлекать IT-специалистов для консультаций, поскольку следователь может не обладать достаточными техническими знаниями для глубокого понимания показаний.

1.2. *Постановка целей допроса*

На данном этапе применяются классические следственные методики, направлен-

ные на диагностику психологического состояния допрашиваемого и выбор оптимальной тактики для преодоления возможного противодействия.

1.3. ***Изучение личности подозреваемого***

Следователь собирает данные о социальном статусе, образовании, профессиональных навыках в сфере IT, техническом оснащении (используемые устройства, ПО), способе совершения преступления (одиночный или групповой характер, связь с хакерскими сообществами).

Эта информация помогает прогнозировать поведение подозреваемого на допросе.

1.4. ***Выбор и подготовка места допроса***

К помещению предъявляются следующие требования:

– конфиденциальность и безопасность (исключение внешнего наблюдения);

– техническая оснащенность (исправные аудио- и видеозаписывающие устройства);

– отсутствие отвлекающих факторов, способных повлиять на концентрацию допрашиваемого;

– оптимальный вариант — специализированный кабинет следователя, оборудованный для таких процедур.

1.5. ***Определение участников допроса***

Учитывая техническую сложность киберпреступлений, к допросу может привлекаться IT-эксперт. Его роль заключается в консультировании следователя по специализированным вопросам и помощи в преодолении интеллектуального противодействия со стороны технически подкованного подозреваемого.

1.6. ***Тактика поведения следователя***

Ключевые принципы:

– строгое соблюдение процессуальных норм (право на адвоката, предупреждение об ответственности за ложные показания);

– нейтральный, профессиональный тон — без давления, чтобы не спровоцировать негативную реакцию;

– гибкий подход к технически грамотным подозреваемым: уточняющие вопросы («правильно ли я понял, что эта программа позволяет...?»), акцент на сотрудничество.

При этом важно отметить, что конфронтация обычно неэффективна, поскольку IT-специалисты плохо реагируют на жесткое давление.

Особые случаи — это противодействие со стороны опытных хакеров, когда некоторые преступники, уверенные в своем техническом превосходстве, умышленно дают неполные или ложные показания и используют специфическую терминологию, чтобы запутать следователя.

Так, по делу о взломе и модификации данных (ст. 272, 273 УК РФ) подозреваемые П.1 и П.2, опытные программисты, саботировали следствие. Их вину удалось доказать только после анализа логов интернет-провайдера, сопоставления противоречий в их показаниях и привлечения свидетелей [6, с. 67]. Психологический аспект здесь заключается в «развиртуализации» преступления.

Также важно отметить, что киберпреступники часто не осознают реальный вред своих действий. Уместный в данной ситуации тактический прием — это демонстрация следующих последствий: какой ущерб понесли конкретные потерпевшие и какие реальные санкции грозят самому подозреваемому. Это помогает сломать восприятие преступления как «виртуального» и склонить к сотрудничеству.

1.7. ***Техническая подготовка к допросу***

При расследовании киберпреступлений техническая оснащенность играет ключевую роль. Для эффективного проведения допроса необходимы:

1) аудиофиксация. Использование цифровых диктофонов позволяет документально зафиксировать ход допроса. Важно соблюдать законность получения доказательств (ст. 164 УПК РФ), исключая нарушения прав подозреваемого;

2) видеозапись. Видеокамеры помогают зафиксировать невербальные реакции (мимику, жесты), что может быть полезно при анализе достоверности показаний. Запись должна вестись открыто, с предупреждением участников о ее проведении;

3) полиграф. Применяется только с согласия допрашиваемого (ст. 164 УПК РФ). Результаты носят справочный характер и не являются доказательством в суде, но могут помочь в выработке тактики допроса;

4) компьютерные технологии. Демонстрация цифровых доказательств (например, ноутбука с вредоносным ПО) может спровоцировать подозреваемого на откровенные показания. Для работы с техническими артефактами рекомендуется привлекать IT-экспертов, особенно при анализе сложных данных (логов, кода программ). При этом важно, чтобы все технические средства должны использоваться в рамках закона, без нарушения процессуальных норм.

1.8. ***Планирование допроса***

Ключевые этапы:

– оценка сложности преступления;

– совместно со специалистом определяется уровень технической составляющей деяния;

– формулируются точные вопросы, исключающие двусмысленность;

– подготовка материалов;

– закладки в деле для быстрого доступа к ключевым документам;

систематизация доказательств (скриншоты, логи, экспертные заключения);

– моделирование ситуаций.

Как отмечает А.Е. Викторова, следователь должен продумать возможные сценарии допроса, включая варианты поведения подозреваемого (от сотрудничества до противодействия), тактические приемы для каждого случая и использование графических и компьютерных моделей [3, с. 96]. При противоречиях в показаниях помогает визуализация событий (например, схема кибератаки).

2. Тактика проведения допроса подозреваемого

Вначале следователь должен тщательно организовать процесс допроса подозреваемого. В первую очередь, при приветствии и знакомстве с допрашиваемым важно проявлять внимательное и уважительное отношение. Это особенно касается свидетелей, чьи показания могут оказаться критически важными для раскрытия дела.

На стадии свободного изложения следователь должен предоставить возможность допрашиваемому высказать свои мысли о совершенном преступлении в произвольной форме. Однако необходимо помнить, что этот этап требует от следователя активного слушания, что подразумевает полное внимание и вовлеченность в рассказ допрашиваемого. В таких случаях может быть полезно использование аудио- или видеозаписи для более точной фиксации информации.

На этапе постановки вопросов следователь задает ряд вопросов, которые включают в себя разнообразные типы. К ним относятся открытые вопросы, такие как: «Не могли бы вы рассказать, как на вашем компьютере оказалось вредоносное программное обеспечение?»; дополняющие вопросы, например: «На каком сайте вы узнали о возможностях данной программы?» или «Какой никнейм имел человек, у которого вы приобрели вредоносную программу? Были ли вам известны неблагоприятные последствия для пользователей?»; уточняющие вопросы, такие как: «Поясните, пожалуйста, что означает [жаргонное слово]?»; и детализирующие вопросы, например: «Опишите, каким образом вредоносное ПО проникает на компьютер жертвы и какие функции оно выполняет?» Имеются и другие подобные виды вопросов.

Если допрос начинает сталкиваться с затруднениями, А.Е. Викторова предлагает следующее решение: «Следователь должен дать понять подозреваемому, что его

отказ давать показания не повлияет на дальнейший ход расследования. Более того, следователь может акцентировать внимание на положительных качествах и характеристиках допрашиваемого». Это может заставить подозреваемого раскрыть важные обстоятельства дела. Однако следует помнить о том, что допрос не должен содержать подсказок или попыток навязать мнение следователя, логических уловок и двусмысленных формулировок.

3. Завершающая стадия допроса: алгоритм действий следователя

Завершающая стадия допроса следователя включает несколько ключевых этапов. Прежде всего, это завершение беседы, которое подводит итог общению. Затем идет оценка результатов следственного действия, основанная на том, насколько полностью были достигнуты цели, установленные на этапе планирования. Не менее важным компонентом этой стадии является рефлексия — последний этап допроса, связанный с самокритическим анализом действий и решений, принятых следователем в процессе допроса. Данный этап позволяет оценить, насколько оперативно и эффективно проводился допрос, а также выявить изменения, которые необходимо внести в подход следователя для его более успешного проведения в будущем.

Как подчеркивают специалисты, рефлексия выступает важным инструментом для повышения эффективности работы специалистов, что в свою очередь способствует изучению опыта, снижению рисков в области информационной безопасности и улучшению качества расследования компьютерных преступлений [5, с. 42]. Если же допрос оказался неэффективным, результаты расследования могут оказаться неудовлетворительными.

Таким образом, можно заключить, что при реализации тактики допроса обвиняемых в ходе расследования преступлений в области компьютерной информации главными целями являются выяснение деталей произошедшего, определение наличия возможных свидетелей и выявление подозреваемых. При допросе подозреваемого необходимо установить, каким образом он получил доступ к компьютерной системе, какие действия он предпринимал, а также выяснить, действовал ли он самостоятельно или в составе группы.

На этапе подготовки к допросу основные задачи включают в себя анализ материалов дела, определение целей допроса с использованием классических следственных приемов, изучение личности подозреваемого или обвиняемого, выбор и подготовку места проведения допроса, а также определение участников и техническую подготовку, включая применение современных информационных технологий. Эта техническая подготовка является ключевым элементом тактики проведения допроса в расследовании преступлений в области компьютерной информации, поскольку в некоторых ситуациях именно она делает возможным проведение следственных действий.

Планирование допроса также важно: совместно с экспертом в соответствующей области определяется уровень технической сложности совершенного преступления. На этом этапе формулируются вопросы и устанавливается их последовательность, а также определяется порядок демонстрации материалов, имеющихся у следствия. Специалист предоставляет следователю необходимую терминологию, которая может пригодиться в процессе допроса. В рамках ситуационного подхода на этапе непосредственного допроса следователь использует показания потерпевшего и свидетелей для уточнения и возможного дополнения своей собственной модели произошедшего преступления [13].

На этапе проведения допроса его порядок должен быть выстроен следующим

образом: вначале, во время знакомства и приветствия, следует проявлять внимательность и уважение к лицу, проходящему допрос. На стадии свободного рассказа следователь предоставляет возможность допрашиваемому изложить информацию о криминальном деянии в неформальной обстановке. На этапе постановки вопросов следователь задает ряд различных вопросов, включая открытые, уточняющие и детализирующие.

Завершение допроса включает в себя несколько важных шагов: окончание беседы, оценка результатов следственного действия, которая основывается на степени достижения поставленных в ходе планирования целей, а также рефлексию — финальный этап, связанный с самокритическим анализом действий и решений, принятых следователем в процессе допроса.

Библиографический список

1. Акопян Р.М. Проблемы тактики допроса подозреваемого (обвиняемого) // Восточно-Европейский научный журнал. 2022. № 7–1 (83). С. 54–56.

2. Бойко Ю.Л. Проблемные вопросы тактики допроса подозреваемых, обвиняемых по преступлениям против личности // Сборник материалов криминалистических чтений. 2020. № 17. С. 10–11.

3. Викторова А.Е. Ситуационное моделирование в тактике допроса потерпевшего, свидетеля, подозреваемого и обвиняемого // Символ науки: международный научный журнал. 2021. № 1. С. 96–98.

4. Головин М.В. Тактические приемы допроса подозреваемого // Эпомен. 2020. № 44. С. 85–91.

5. Горбунова К.А., Киселев А.С. Тактика производства следственных действий при расследовании преступлений в сфере компьютерной информации : монография. М. : Проспект, 2023. 88 с.

6. Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М. : Проспект, 2023. 136 с.

7. Киселев А.С. Особенности тактики допроса обвиняемых при расследовании преступлений в сфере компьютерной информации // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 67–74.

8. Кузьмина Л.О., Сапсай М.В., Золотарева А.Р. Особенности тактики производства вербальных следственных действий при расследовании киберпреступлений // Наука и бизнес: пути развития. 2019. № 10 (100). С. 144–146.

9. Морозова Т.В., Жуковский С.Ф., Зуева В.В. Психологические и речекоммуникативные тактики ведения допроса в ходе предварительного следствия // Гуманитарная парадигма. 2020. № 4 (15). С. 131–138.

10. Поляков В.В. Криминалистическая классификация способов противодействия расследованию высокотехнологичных преступлений // Юридическая наука и правоохранительная практика. 2023. № 1 (63). С. 69–79.

11. Поляков В.В. Структура и содержание криминалистической характеристики высокотехнологичных преступлений // Актуальные проблемы российского права. 2024. № 7 (19). С. 147–159.

12. Поляков В.В. Транснациональные организованные группы с сетевой структурой и экосистемы транснациональных преступных групп // Проблемы правовой и технической защиты информации. 2024. № 12. С. 58–61.

13. Поляков В.В., Ширяев А.В. Проблемы тактики допроса по делам о компьютерных преступлениях // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: материалы XIII Международной научно-практической конференции: в 3 ч. Барнаул: Барнаульский юридический институт МВД России, 2015. Ч. 1. С. 123–126.

14. Рачева Н.В., Поскочинова К.А. Проблемные аспекты допроса подозреваемых при расследовании киберпреступлений // Технологии XXI века в юриспруденции: материалы II Международной научно-практической конференции (Екатеринбург, 22.05.2020) / под ред. Д.В. Бахтеева. Екатеринбург : Уральский государственный юридический университет, 2020. С. 520–529.

15. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская, А.И. Семикаленова, И.А. Рядовский, Т.А. Сааков. М. : Проспект, 2023. 256 с.