

ХАКЕР КАРДИНГ АНТИФРОД

Путь в кибербезопасность



ДАНИИЛ КУПРИЙ

Даниил Куприй

Хакер. Кардинг. Антифрод.

Путь в кибербезопасность

<https://litres.ru/74558599>

SelfPub; 2026

Аннотация

Хакер. Кардинг. Антифрод. Три слова, одна цепочка: кто-то ищет слабые места в системах, а кто-то закрывает их раньше, чем они станут проблемой. И в каждом звене нужен один и тот же склад ума: острый глаз, быстрая реакция и привычка думать на шаг вперёд.

Если вы внимательны к деталям, любите разбираться, как всё устроено, и не принимаете всё на веру, эта книга покажет, где такой склад ума оплачивается официально: антифрод, кибербезопасность, тестирование, баг-баунти, комплаенс. Что делают специалисты каждый день, чего ждут работодатели, как войти без диплома и куда расти.

Без воды и инструкций: профессии, цифры и понятный план действий.

Даниил Куприй
Хакер. Кардинг. Антифрод.
Путь в кибербезопасность

Глава 1. Что у вас уже есть

Людям с хакерским складом ума редко приходит в голову, что у них есть что-то ценное. Им кажется, что они просто любопытные, дотошные или упрямые. В школе их называли «слишком много спрашиваешь», в компании друзей — «вечно всё разбираешь». Они не считают это навыком, потому что для них это так же естественно, как дышать.

Но если присмотреться, за этим «характером» стоит набор вполне конкретных, измеримых качеств. Их можно назвать, проверить у себя, развить и показать работодателю. И, что важно, за них платят: банки, платёжные сервисы, маркетплейсы и IT-компании постоянно ищут людей, которые умеют замечать слабые места раньше других.

В этой главе мы разберём четыре качества, на которых держится работа в антифроде, кибербезопасности, тестировании и смежных профессиях. Для каждого качества мы посмотрим, как оно выглядит в жизни и в работе, как его можно тренировать легально и где подстерегает ловушка. В конце вы найдёте тест на самопроверку и упражнения на неделю.

Почему «смекалка» — это не одно качество

Обычно под смекалкой понимают что-то общее: «он со-

образительный». Для профессии такое описание бесполезно. Работодателю нужно знать, что именно вы умеете: замечать аномалии в таблице, находить неочевидный сценарий в приложении, принимать решение за секунды или понимать, как манипулируют людьми.

Это четыре разных способности. У большинства людей одна-две выражены сильно, остальные средне. И это нормально: в отрасли найдётся место для каждого сочетания, о чём мы поговорим ближе к концу главы.

Качество 1. Внимание к деталям

Что это такое

Внимание к деталям — это не педантичность и не умение долго читать. Это способность замечать то, что не вписывается в картину. Не просто видеть все элементы, а чувствовать, какой из них лишний, неожиданный или странный.

Человек с такой способностью замечает, что в письме от «банка» чуть иной тон, чем обычно. Что в таблице одно число выбивается из ряда. Что в интерфейсе кнопка стоит не на том месте, где её ждёшь. Часто он не может сразу объяснить, что именно не так, но ощущение «что-то здесь не то» появляется раньше, чем разумное объяснение.

Как это выглядит в работе

Антифрод-аналитик проверяет тысячи операций в день. Он не читает каждую внимательно, это невозможно. Вместо этого он держит в голове образ того, как выглядит нормальное поведение клиента, и мгновенно цепляется за отклонения: перевод в необычное время, сумма, чуть отличающаяся от привычных, цепочка получателей, зарегистрированных в один день.

Специалист по комплаенсу сравнивает операции клиента с его профилем. Тестировщик замечает, что после обновления у одной из страниц изменился отступ, а значит, что-то в вёрстке пошло не так. Аудитор читает договор и видит, что в приложении другая формулировка, чем в основном тексте. Везде работает один и тот же механизм: сравнить с нормой и заметить расхождение.

Как тренировать легально

- Игры на поиск различий и логические задачи с несоответствиями: они развивают именно сопоставление с нормой.
- Чтение открытых разборов инцидентов (постмортемов) компаний: попробуйте сначала найти в описании, где могла быть ошибка, а потом сверьтесь с авторами.
- Работа с таблицами: возьмите любой открытый набор данных, например государственную статистику, и найдите в нём выбросы и странности.
- Вычитка текстов: корректура развивает глаз на мелкие несоответствия лучше многих курсов.

Ловушка

У внимания к деталям есть обратная сторона: если не уметь расставлять приоритеты, человек начинает видеть проблему везде. В антифродде это называется ложными сра-

батываниями: заблокировать честного клиента так же дорого, как пропустить мошенника. Поэтому внимательность нужна в паре со здравым смыслом: замечать всё, но реагировать только на то, что действительно важно.

Качество 2. Техническая сообразительность

Что это такое

Это умение быстро разобраться, как устроено незнакомое приложение, сервис или система, и не бояться экспериментировать. Не обязательно уметь программировать. Важно другое: вы не боитесь незнакомого интерфейса, пробуете разные сценарии, читаете документацию и делаете выводы из поведения системы.

Такие люди обычно с детства разбирали технику, копались в настройках игр, пробовали «а что будет, если нажать вот это». Их любопытство работает как исследовательский метод: гипотеза, проверка, вывод.

Как это выглядит в работе

QA-инженер перед релизом задаёт приложению вопросы, о которых разработчики не подумали. Что будет, если отключить интернет посередине операции? Что случится, если отправить форму дважды подряд? Что произойдёт, если ввести число там, где ждут текст? Он ищет крайние случаи, где продукт ведёт себя непредсказуемо.

Специалист по тестированию на проникновение (пентестер) делает то же самое на другом уровне: по заказу компании и с её разрешения он проверяет, можно ли обойти защиту, и описывает, как это закрыть. Исследователь в программе баг-баунти изучает сервис и сообщает владельцу о найденной уязвимости. Принцип один: понимать, как система устроена, чтобы увидеть, где она может сломаться.

Главное правило: только с разрешения

Здесь проходит граница между профессией и проблемой. Тренироваться и искать уязвимости можно только в системах, которыми вы владеете, на специально созданных учебных площадках и в рамках официальных программ, где владелец прямо разрешил проверку. Проверка чужого сервиса без разрешения, даже из любопытства и даже без вреда, может быть нарушением закона. Профессионалы начинают карьеру именно с усвоения этого правила.

Как тренироваться легально

- Учебные платформы и соревнования формата CTF (Capture The Flag): на них специально созданы уязвимые системы для практики. Примеры: Hack The Box, TryHackMe, бесплатные лаборатории PortSwigger Web Security Academy. Актуальность и условия проверяйте на их сайтах.

- Домашняя лаборатория: виртуальные машины на собственном компьютере, где можно безопасно изучать, как устроены системы.
- Открытые материалы OWASP: описание типовых классов уязвимостей веб-приложений и способов защиты.
- Тестирование собственных проектов: сделайте простое приложение или сайт и попробуйте найти в нём слабые места.
- Бесплатные курсы по основам сетей, баз данных и информационной безопасности.

Ловушка

Самая распространённая ошибка новичков — ломать ради самого ломания. Профессионал думает иначе: он находит проблему, документирует её и помогает исправить. Отчёт, который нельзя воспроизвести и понять, не имеет ценности. Умение объяснить находку простыми словами важнее умения найти её.

Качество 3. Скорость реакции

Что это такое

Способность быстро принимать решение, когда ситуация меняется, и не терять при этом точности. Это не импульсивность, а скорее тренированная выдержка: вы видите новые данные, оцениваете их и действуете, пока время ещё работает на вас.

Как это выглядит в работе

В антифроде есть понятие окна реагирования: время между началом подозрительной операции и моментом, когда деньги уже не вернуть. Оно измеряется секундами и минутами. Если аналитик сомневается слишком долго, деньги уходят. Если действует слишком быстро и блокирует честного клиента, банк теряет доверие.

Аналитик SOC (центра мониторинга безопасности) видит поток событий, где большинство шум. Когда среди них появляется настоящая атака, у него минуты на то, чтобы отделить её от сбоя и запустить реагирование. Специалист поддержки платёжной системы в ходе разговора с клиентом должен быстро понять, ошибка это или признак компрометации

счёта.

Как тренироваться

- Разбор учебных кейсов на время: дайте себе пять минут на решение по условному инциденту, потом сравните с эталоном.
- Командные соревнования и киберучения, где нужно действовать быстро, в том числе формат Blue Team (защита).
- Любые дела, где нужно держать концентрацию под давлением: шахматы на время, настольные игры, симуляторы.
- Привычка проговаривать решение вслух: «вижу это, думаю то, делаю так». Она ускоряет мышление и помогает потом объяснять решения коллегам.

Ловушка

Скорость без точности превращается в хаос. В профессии ценится не тот, кто реагирует быстрее всех, а тот, кто быстро выбирает правильное действие и умеет сказать «я не уверен, нужна вторая пара глаз». Эта привычка отличает сильных специалистов от опасных.

Качество 4. Понимание чужих уловок

Что это такое

Способность видеть, как манипулируют вниманием, доверием и страхом людей, и предугадывать такие ходы. Человек с этим качеством замечает давление срочностью («решайте сейчас, иначе будет поздно»), ложное чувство безопасности («это просто формальность»), игру на авторитете («я из службы безопасности»).

Это не цинизм и не недоверие к людям. Это понимание того, как работают приёмы, которые встречаются в письмах, звонках и сообщениях. Такие приёмы называют социальной инженерией.

Как это выглядит в работе

Специалисты по социальной инженерии проводят для компаний проверки с разрешения: имитируют фишинговые письма, звонят сотрудникам от имени «техподдержки» и смотрят, кто попадётся. Цель не поймать людей, а выявить слабые места и научить сотрудников им противостоять. Антифрод-аналитики используют то же понимание: они знают, какими фразами и сценариями жертв подталкивают к пере-

воду денег, и строят правила, которые останавливают такие операции.

Как тренироваться

- Изучайте открытые разборы реальных случаев фишинга и мошенничества: банки и регуляторы регулярно публикуют их с описанием признаков.
- Проходите учебные тренинги по распознаванию фишинга: многие компании и платформы делают их бесплатными.
- Читайте книги по психологии влияния и поведенческой экономике, где описаны приёмы убеждения и когнитивные искажения.
- Практика на себе: когда вам приходит подозрительное сообщение, разберите его по признакам и объясните, на что оно давит.

Ловушка

Если долго смотреть на обман, легко начать видеть его везде. Профессионалы удерживают баланс: понимают приёмы, но сохраняют уважение к людям, которых защищают. Антифрод работает именно потому, что за каждой подозрительной операцией стоит человек, который мог просто растеряться.

Мини-кейс: два рабочих дня, одна цепочка

Посмотрим, как все четыре качества работают вместе. Антифрод-аналитик видит в ленте операцию: перевод на новый счёт, открытый неделю назад. Сумма небольшая, время подозрений не вызывает. Формально всё в норме. Но система отмечает деталь: владелец счёта за последние три года ни разу не переводил деньги новым получателям.

Аналитик открывает карточку получателя. Счёт создан неделю назад, за это время через него прошло двенадцать переводов от разных людей, и каждый уходил дальше на другой счёт по одному и тому же шаблону. Отдельно каждая операция выглядит безобидно. Вместе они образуют цепочку транзита, через которую проводят деньги от одного пострадавшего к итоговому получателю.

Что здесь сработало? Внимание к деталям заметило нетипичное поведение клиента. Техническая сообразительность помогла разобраться в карточке получателя и связать операции. Скорость реакции позволила остановить цепочку, пока деньги не ушли дальше. Понимание уловок подсказало, что такая схема строится так, чтобы каждый шаг выглядел обычным. Один человек, четыре качества, одна остановленная цепочка.

Пятое качество, о котором редко говорят: выдержка к рутине

К четырём качествам стоит добавить ещё одно, которое не звучит эффектно, но определяет, останется ли человек в профессии. Это готовность к рутине. Большинство рабочих дней в антифроде, QA или комплаенсе выглядят буднично: проверить десятки обычных случаев, чтобы найти один необычный. Разбирать однотипные алерты. Заполнять отчёты. Читать документацию.

Один удачный перевод или один найденный баг ничего не доказывают. Призвание проверяется повторяемостью: можете ли вы делать это систематически, день за днём, даже когда ничего интересного не происходит. Именно готовность к рутине ради редкого момента, когда всё сходится, отличает устойчивого специалиста от того, кто искал только острых ощущений.

Откуда берутся эти качества и почему они редко встречаются вместе

Никто не рождается с готовым навыком замечать подвох. Обычно он формируется раньше и по совсем другой причине. У кого-то это увлечение видеоиграми и понимание, как устроены их системы изнутри. У кого-то ранний опыт разборки техники. У кого-то склад характера, который не позволяет принимать что-либо на веру. Само качество нейтрально: активом оно становится в зависимости от того, куда его применили.

Большинство людей обладают одним-двумя из четырёх качеств, но редко всеми сразу. Поэтому в отрасли так много разных направлений: одни требуют больше внимания к деталям, другие больше технической смекалки. Человеку, у которого сильно выражено только одно качество, не нужно ставить на себе крест: найдётся место именно для этой сильной стороны.

Четыре профиля: какой из них ваш

- Детектив. Сильнее всего внимание к деталям и распознавание паттернов. Подходит для антифрода, комплаенса и AML.
- Исследователь. Сильнее всего техническая сообрази-

тельность и любопытство. Подходит для пентеста, баг-баунти, QA и безопасности приложений.

- Оператор. Сильнее всего скорость реакции и выдержка. Подходит для SOC, реагирования на инциденты и поддержки платёжных систем.

- Психолог. Сильнее всего понимание людей и чужой логики. Подходит для социальной инженерии, обучения сотрудников и расследований.

Профили не взаимоисключающие: у многих два основных. Но выбрать главный полезно, потому что он подскажет, с какой профессии начинать в главе 2.

Тест для самопроверки

Ответьте на вопросы честно, ориентируясь на то, как вы поступаете в реальности, а не на то, как хотели бы. Отмечайте «да», если это про вас верно чаще, чем нет.

Внимание к деталям

- Я замечаю опечатки, несостыковки и странности там, где другие их не видят.
- Мне быстро становится понятно, что в тексте, письме или таблице что-то не так, даже если я не сразу могу объяснить что.
- Я перепроверяю цифры и факты, прежде чем на них опереться.

Техническая сообразительность

- Я не боюсь незнакомых интерфейсов и пробую разные варианты, чтобы понять, как всё работает.
- Мне интересно, как устроены вещи изнутри, и я готов потратить на это время.
- Я читаю документацию или инструкции, когда не получается с первого раза.

Скорость реакции

- Я сохраняю ясную голову, когда ситуация быстро меняется.
- Мне легче принять решение сразу и скорректировать, чем долго обдумывать.
- Я умею признавать, что не уверен, и просить помощи.

Понимание чужих уловок

- Я замечаю, когда на меня давят срочностью или авторитетом.
- Я могу объяснить, почему человек поступил именно так, а не просто оценить его поступок.
- Мне интересно, как работают манипуляции и как от них защищаться.

Выдержка к рутине

- Я могу несколько часов подряд заниматься однотипной проверкой, если знаю, что где-то есть нестыковка.
- Я довожу начатое до конца, даже когда становится скучно.

Как читать результат

Посчитайте «да» в каждом блоке. Если в одном или двух блоках у вас три-два ответа «да», это ваши сильные стороны. Если «да» в основном по рутине и вниманию, смотрите на антифрод и комплаенс. Если по технике и любопытству, на пентест, QA и баг-баунти. Если по скорости и выдержке, на SOC и поддержку платёжных систем. Если по пониманию людей, на социальную инженерию и расследования. Если «да» мало везде, это не приговор: большинство навыков тренируются, и в конце главы есть упражнения.

Три мифа о хакерском мышлении

Миф 1. Нужно быть гением в программировании

Большинство начальных позиций в антифродде, комплаенсе и QA не требуют программирования. Нужны внимательность, логика и умение читать таблицы. Программирование помогает в пентесте и безопасности приложений, но и там его изучают по ходу карьеры.

Миф 2. Хакер это тот, кто взламывает без правил

В профессиональной среде всё устроено строго наоборот: легальный специалист работает по правилам, с разрешением владельца, по договору и с отчётом. Именно эти рамки и делают его работу профессией, а не проблемой.

Миф 3. Такие навыки либо есть, либо нет

Каждое из четырёх качеств можно развивать. Внимание

тренируется практикой сопоставления, техническая сообразительность опытом и курсами, скорость реакции разборами кейсов, понимание уловок изучением реальных примеров. Исходные данные важны, но регулярная практика в итоге решает больше.

Что сделать после этой главы

Прочитать главу недостаточно. Вот план на неделю, который займёт по полчаса в день.

- День 1. Пройти тест выше и определить свой главный профиль.
- День 2. Выбрать одно качество, которое хочется усилить, и найти для него одно упражнение из раздела «Как тренировать».
- День 3. Прочитать два открытых разбора инцидентов или случаев мошенничества и записать, на что обратили внимание вы, а на что авторы.
- День 4. Пройти бесплатный вводный урок на учебной платформе по безопасности или тестированию.
- День 5. Открыть два сайта с вакансиями и выписать требования для ролей, соответствующих вашему профилю.
- День 6. Написать короткий абзац о том, как вы однажды заметили то, чего не заметили другие. Это заготовка для резюме и собеседования.
- День 7. Подвести итог: что получилось, что было скучно, что захотелось продолжить.

Коротко о главном

- Хакерское мышление складывается из четырёх конкретных качеств: внимание к деталям, техническая сообразительность, скорость реакции, понимание чужих уловок.
- Пятое качество, которое решает, останетесь ли вы в профессии, это выдержка к рутине.
- Все эти качества можно тренировать легально: на учебных площадках, в соревнованиях и на собственных проектах.
- Граница между профессией и проблемой одна: разрешение владельца системы.
- Выберите свой главный профиль, он подскажет, с какой профессии начинать в следующей главе.

Глава 2. Где это оплачивается

В первой главе мы разобрали, из чего складывается хакерское мышление. Теперь главный вопрос: где его оплачивают? Ответ шире, чем кажется. Это не только «кибербезопасность» в привычном понимании, а целое семейство профессий, где люди ищут слабые места, замечают аномалии и останавливают мошенничество.

Банки, платёжные сервисы, маркетплейсы, телеком-компании, IT-разработчики, консалтинговые фирмы и государственные структуры постоянно ищут таких специалистов. Рынок в этой сфере растёт быстрее, чем успевают готовить кадры, поэтому компании нанимают и тех, кто пришёл из смежных областей и без профильного диплома.

В этой главе мы разберём шесть направлений подробно: чем занимаются, как выглядит рабочий день, какие требования предъявляют, как войти без опыта и куда расти. Затем поговорим о том, как выбрать своё направление, составить резюме, пройти собеседование и пережить испытательный срок.

Карта профессий

Начнём с общей картины. Ниже шесть направлений, где навыки из первой главы оплачиваются официально.

Профессия

Что делает

Какой навык особенно ценится

Антифрод-аналитик

Отслеживает подозрительные транзакции и паттерны мошеннических схем

Внимание к деталям, распознавание паттернов

Специалист по кибербезопасности

Ищет уязвимости в системах до того, как их найдёт злоумышленник

Техническая сообразительность, любопытство к обходам

QA-инженер

Находит ошибки и дыры в продукте до релиза

Скрупулёзность, умение ломать систему

Поддержка платёжных систем

Расследует спорные транзакции, блокировки, чарджибеки

Знание того, как движутся деньги в системе

Баг-баунти-хантер

Ищет и законно сдаёт уязвимости за вознаграждение

Техническая смекалка, упорство

Комплаенс/AML-специалист

Проверяет операции на признаки отмывания денег

Понимание схем, внимательность к деталям

Это не исчерпывающий список: рядом существуют безопасность приложений, расследование инцидентов, аналитика угроз, безопасность облачных сервисов и другие. Но эти шесть дают самые доступные точки входа и хорошо иллюстрируют, как один и тот же склад ума работает в разных ролях.

Что объединяет эти профессии

В каждом случае речь идёт об одном: видеть то, что другие пытаются скрыть или не замечают, понимать логику чужих действий, действовать быстро и точно. За это платят зарплату, дают трудовую книжку, социальные гарантии и карьерный рост. Работа идёт по правилам, в рамках закона и по договору, а результаты можно записать в резюме.

1. Антифрод-аналитик

Чем занимается

Задача антифрод-аналитика отличить одну подозрительную операцию от тысяч обычных, не заблокировав при этом честного клиента. В банках, маркетплейсах и платёжных системах такие специалисты работают в связке с автоматическими системами скоринга: алгоритм ловит типовые паттерны, а человек решает пограничные случаи, где цена ошибки высока в обе стороны.

Помимо разбора отдельных операций, аналитик занимается и более широкими задачами: ищет новые схемы, которые алгоритм ещё не знает, предлагает правила для их блокировки, анализирует причины ложных срабатываний и готовит отчёты для руководства.

Один день аналитика

Утро начинается с очереди алертов, которые система накопила за ночь. Большинство ложные: человек просто потратил больше обычного или зашёл в новый магазин. Но несколько алертов в день оказываются настоящими. Например, счёт открыт недавно, на него в течение часа поступа-

ют переводы от разных людей, а затем всё выводится одним платежом.

Аналитик не может просто заблокировать: нужно убедиться, что это действительно похоже на мошенничество, а не на честный перевод между друзьями. Ошибка в любую сторону стоит денег или доверия клиента. Во второй половине дня идёт разбор пограничных случаев, которые алгоритм не смог решить сам, и обновление правил на основе новых схем, замеченных за неделю.

Какие навыки ценятся

- Внимание к деталям и распознавание паттернов.
- Уверенная работа с таблицами; на следующем уровне базовый SQL.
- Умение коротко и ясно обосновать решение письменно.
- Устойчивость к монотонной работе и умение не терять концентрацию.

Как войти без опыта

Самый частый путь проходит через смежные позиции: поддержку клиентов банка, операционный отдел, обработку спорных операций. Через год-полтора человек уже знает типовые сценарии обмана и готов перейти в аналитику. Второй путь через специализированный курс по антифроду или ос-

новам аналитики и стажировку.

Куда расти

От младшего аналитика к старшему, затем к руководителю группы или отдела. Смежные направления: разработка антифрод-правил, построение моделей, продуктовый риск-менеджмент, расследования.

2. Кибербезопасность

Чем занимается

Это целая отрасль с несколькими направлениями. Три самых заметных:

- SOC-аналитик (центр мониторинга безопасности). Следит за потоком событий в сети компании, отличает атаки от сбоев и запускает реагирование.
- Пентестер. По заказу компании и с её разрешения проверяет системы, пытаясь найти слабые места до того, как их найдут злоумышленники. Результат работы — подробный отчёт с рекомендациями.
- Специалист по социальной инженерии. Проверяет, насколько сотрудники устойчивы к фишингу и манипуляциям, и обучает их распознавать угрозы.

Один день SOC-аналитика

Аналитик видит перед собой поток событий безопасности со всей сети компании. Несколько тысяч событий в час, и большинство из них шум. Но попытка войти в систему с необычного адреса в час ночи, с верным паролем с первой попытки, повод присмотреться. Он сопоставляет это с дру-

гими событиями: тот же аккаунт через пять минут пытается получить доступ к внутренней базе. Ни одно из событий само по себе ничего не доказывает, но вместе они складываются в картину, которую нужно остановить до того, как данные покинут компанию.

Какие навыки ценятся

- Основы сетей, операционных систем и работы с журналами событий.
- Любопытство и привычка проверять гипотезы.
- Умение составить понятный отчёт: что найдено, как воспроизвести, чем опасно, как исправить.
- Готовность к сменной работе в SOC и к постоянному обучению: технологии быстро меняются.

Как войти без опыта

Через базовые курсы по информационной безопасности (обычно от трёх до шести месяцев регулярных занятий), практику на учебных платформах и участие в соревнованиях CTF. Многие начинают с позиции младшего аналитика SOC или специалиста технической поддержки с последующим переходом.

Куда расти

К ведущему аналитику, руководителю SOC, специалисту по расследованию инцидентов, архитектору безопасности. Отдельная ветка: консалтинг и независимая практика.

3. QA-инженер (тестирование)

Чем занимается

QA-инженер проверяет продукт до того, как с ним столкнётся пользователь. Его задача — найти все способы, которыми приложение может сломаться, и сообщить об этом разработчикам. Это часто первая точка входа в технические профессии без необходимости программировать.

Один день QA-инженера

Релиз выходит завтра утром. Инженер получает сборку вечером и должен за несколько часов понять, что в ней могло сломаться. В задаче написано «проверить форму оплаты». На практике это означает: ввести отрицательную сумму, оставить поля пустыми, отправить форму дважды подряд, оборвать соединение на середине запроса и посмотреть, спишутся ли деньги.

Хороший тестировщик думает не «как это должно работать», а «как это может сломаться». Именно этот навык: держать в голове нестандартный сценарий, пока все вокруг проверяют стандартный, и есть качество из первой главы, превращённое в профессию.

Какие навыки ценятся

- Скрупулёзность и системное мышление.
- Умение чётко описать ошибку: шаги воспроизведения, ожидаемый и фактический результат.
- Основы тест-дизайна: как составлять проверки так, чтобы покрыть как можно больше сценариев.
- На следующем уровне: автоматизация тестирования и базовое программирование.

Как войти без опыта

Через курсы по ручному тестированию (обычно два-четыре месяца), практику на открытых проектах и демонстрационных сайтах и тестовые задания. Многие компании берут людей из совсем других профессий, если те показывают внимательность и логику.

Куда расти

В автоматизацию тестирования, в лидеры QA-команд, в тестирование безопасности и дальше в кибербезопасность. QA часто становится трамплином в другие направления.

4. Специалист поддержки платёжных систем

Чем занимается

Такие специалисты разбирают спорные списания, недошедшие платежи, блокировки карт и признаки компрометации счетов. Здесь важно понимать, как деньги движутся между банками, платёжными шлюзами и магазинами, и видеть нетипичные случаи.

Один день специалиста

Клиент пишет: деньги списались, а товар не пришёл. Специалист открывает цепочку платежа: банк клиента, платёжный шлюз, счёт магазина. В большинстве случаев это простая задержка у банка-получателя. Но иногда цепочка выглядит странно: деньги ушли не в магазин, а на счёт, который час назад ещё не существовал. Тогда специалист видит в этом не частность, а сигнал для антифрода, и передаёт случай дальше с подробным описанием.

Какие навыки ценятся

- Понимание, как устроены платёжные цепочки.
- Вежливая и ясная коммуникация с клиентами, в том числе в стрессовых ситуациях.
- Аккуратность в документировании обращений.
- Умение вовремя эскалировать нестандартный случай.

Как войти без опыта

Это одна из самых доступных точек входа: вакансии в поддержке и операционных отделах банков и платёжных систем открыты постоянно. Достаточно внимательности, грамотной речи и готовности учиться. Через год-два человек может перейти в антифрод, расследования или комплаенс.

5. Баг-баунти-хантер

Чем занимается

Компании официально публикуют правила, по которым исследователи могут искать уязвимости в их сервисах и получать за найденные вознаграждение. Эти программы называются баг-баунти. Работа идёт строго в рамках правил программы: что можно проверять, а что нельзя, как сообщать о находке и сколько за неё платят.

Один день хантера

У него нет расписания в привычном смысле. Он выбирает программу, внимательно читает её правила и начинает методично изучать сервис: как устроена авторизация, что происходит при смене пароля, как приложение обрабатывает необычные данные. Основная часть времени уходит не на яркие находки, а на рутину: чтение документации, повторение проверок с небольшими изменениями, ведение записей о том, что уже проверено.

Отчёт об уязвимости пишется по строгой форме: как воспроизвести, что происходит, к чему это может привести, как исправить. Отчёт без чёткого воспроизведения отклоняют, и

потраченное время не оплачивается. Поэтому качество описания здесь не менее важно, чем сама находка.

Какие навыки ценятся

- Техническая сообразительность и терпение.
- Знание типовых классов уязвимостей веб-приложений и способов их проверки на разрешённых системах.
- Умение чётко и коротко писать отчёты.
- Дисциплина: соблюдать правила программы, не выходить за её рамки.

Как войти без опыта

Начните с обучения на учебных площадках и соревнованиях, потом переходите к публичным программам российских и международных платформ. Выплаты за находки нерегулярны, поэтому на старте это дополнение к основной работе, а не источник стабильного дохода. Хантеры, показавшие себя, часто получают предложения о работе от самих компаний.

6. Комплаенс и AML

Чем занимается

Эти специалисты смотрят на операции с точки зрения закона о противодействии отмыванию денег (AML, от «anti-money laundering»). Они строят правила, по которым банки и финтех-компании распознают подозрительные цепочки переводов, и следят, чтобы компания соблюдала требования регуляторов.

Один день специалиста

Его рабочий день состоит из очереди операций, которые система отметила автоматически: слишком крупный перевод для профиля клиента, серия операций чуть ниже порога обязательного контроля, деньги из страны с высоким риском. По каждой нужно решить: обычная активность или признак схемы, о которой следует сообщить регулятору.

Ошибка в любую сторону стоит дорого: пропущенная схема означает штраф для банка, а лишняя блокировка честного клиента вредит репутации сервиса. Поэтому AML-специалисты с опытом ценятся высоко: способность быстро различать пятьдесят похожих операций это тот же навык распо-

знавания паттернов, что и в антифроде, только применённый к другому типу данных и юридическому контексту.

Какие навыки ценятся

- Внимательность и аналитическое мышление.
- Понимание нормативной базы или готовность её изучать.
- Умение обосновать решение письменно и в разговоре с регулятором.
- Знание Excel, базовый SQL на следующем уровне.

Как войти без опыта

Часто через юридический, финансовый или операционный отдел банка. Подходят и люди из смежных профессий: бухгалтеры, юристы, аудиторы. Помогают профильные курсы по AML и комплаенсу.

Как выбрать направление

Вернитесь к профилю из первой главы и сопоставьте его с направлениями.

- Детектив (внимание к деталям): антифрод, комплаенс и AML.
- Исследователь (техническая сообразительность): пен-тест, баг-баунти, QA.
- Оператор (скорость и выдержка): SOC, поддержка платёжных систем.
- Психолог (понимание людей): социальная инженерия, обучение сотрудников, расследования.

Ничто из этого не выбирается навсегда. Большинство специалистов за карьеру меняют направление внутри отрасли несколько раз: QA уходит в безопасность, поддержка в антифрод, антифрод в риск-менеджмент. Границы между направлениями тоньше, чем в большинстве профессий.

С чего начать, если нет технического образования

Большинство этих направлений не требуют диплома программиста на старте. Антифрод и комплаенс часто берут людей из поддержки и операционных отделов банков, QA из любой внимательной к деталям профессии. Вот пошаговый план.

- Месяц 1. Выберите одно-два направления по профилю. Прочитайте по 10 вакансий на каждое и выпишите повторяющиеся требования.

- Месяц 2. Пройдите базовый курс по выбранному направлению: основы информационной безопасности, тестирования или аналитики. Параллельно подтяните Excel или таблицы.

- Месяц 3. Сделайте один практический проект: например, разберите открытый набор данных на предмет аномалий, найдите баги в демонстрационном приложении или пройдите несколько заданий на учебной платформе. Опишите результат в одном-двух абзацах.

- Месяц 4. Подготовьте резюме и откликайтесь на входные позиции: поддержка, операции, джуниор-аналитик, стажёр.

Это ориентир, а не жёсткий график. Главное не ждать идеального момента: входные позиции в этой отрасли открываются постоянно.

Как читать реальные вакансии

Откройте любой сайт с вакансиями и введите «антифрод-аналитик», «SOC-аналитик», «QA-инженер» или «AML-специалист». В большинстве объявлений видны вилка зарплат, требования и обязанности. Сравните несколько:

- Какие требования повторяются во всех вакансиях? Это обязательный минимум.
- Какие встречаются реже? Это то, что вы можете подтянуть позже.
- Какие формулировки означают «знаю основы»: чаще всего это работа с таблицами, базовый SQL, понимание процессов.

Зарплатные вилки зависят от города, компании и уровня, поэтому ориентируйтесь на актуальные объявления на момент чтения. Порог входа обычно заметно ниже, чем кажется со стороны.

Что видят работодатели в резюме

Рекрутер в антифродде или кибербезопасности редко ищет в резюме просто слово «опыт». Гораздо больше его интересуют конкретные примеры: как человек самостоятельно разобрался в незнакомом сервисе, нашёл в нём ошибку, которую никто не заметил, выучил основы анализа данных по открытым курсам и применил их.

Что писать

- Результаты, а не обязанности: «нашёл и описал 12 ошибок в демо-приложении» лучше, чем «занимался тестированием».
- Учебные проекты и участие в соревнованиях CTF: они показывают инициативу.
- Курсы и сертификаты с датами.
- Опыт из других профессий, где вы применяли внимательность, аналитику или работу с людьми.

Чего избегать

- Общих слов «ответственный, внимательный, быстро обучаюсь» без примеров.
- Перечня технологий, которых вы не знаете: на собеседо-

вании это быстро выясняется.

- Описания любых действий в чужих системах без разрешения: для работодателя это тревожный сигнал.

Тестовое задание и собеседование

Каких кандидатов реально берут

Диплом по профильному направлению важен гораздо меньше, чем способность пройти тестовое задание на логику и внимательность. Типичное задание для джуниора-аналитика: дают таблицу с несколькими десятками транзакций и просят найти подозрительные без подсказок. Задача не в том, чтобы угадать «правильный» ответ, а в том, чтобы показать ход мысли: почему именно эти строки вызывают вопросы. Многие компании берут людей из других сфер, например бывших бухгалтеров, юристов, даже учителей, если у человека видна склонность думать системно.

Как проходит собеседование

Обычно оно состоит из трёх этапов. Сначала короткий звонок с HR на пятнадцать минут: мотивация, ожидания по зарплате. Затем техническое или кейс-интервью с будущим руководителем: нужно разобрать практический случай вслух и объяснить своё решение. Здесь важнее логика рассуждения, чем единственно верный ответ. Наконец, финальное собеседование с руководителем отдела или директором по без-

опасности, где обсуждают направление развития и команду. Вся цепочка занимает от двух до четырёх недель.

Ошибки, которые стоят дорого

Самая частая ошибка кандидата без опыта — пытаться звучать увереннее, чем он есть. Опытный интервьюер сразу слышит, когда незнание прикрывают уверенной интонацией. Гораздо лучше работает честность: сказать, чего вы не знаете, и показать, как стали бы разбираться. Это качество часто важнее для найма, чем знание терминов наизусть.

Вопросы, которые стоит подготовить

- Расскажите о случае, когда вы заметили то, чего не заметили другие.
- Как вы поступите, если не уверены в решении, а время ограничено?
- Почему вам интересно именно это направление?
- Как вы будете учиться в первые полгода?

Чего ждать на испытательном сроке

Первые три-шесть месяцев новый сотрудник чаще всего работает в паре с наставником: смотрит, как тот ведёт реальные кейсы, задаёт вопросы, постепенно берёт простые случаи сам. Главный показатель этого периода не то, сколько случаев вы закрыли, а насколько точно вы умеете признать, что не уверены, и попросить второе мнение. Привычка проверять себя, а не действовать вслепую, отличает тех, кто остаётся в отрасли надолго.

Частые заблуждения о работе в антифродде

- «Это скучная работа без творчества». На самом деле значительная часть времени уходит на поиск новых паттернов, которые никто ещё не описал; это творческая задача, просто в другой форме.
- «В отрасль попадают только те, кто работал в IT». Большинство начальных позиций не требуют программирования: нужны умение читать таблицы и сохранять концентрацию при монотонной работе.
- «Работа только за компьютером». Аналитики в крупных банках выступают на внутренних тренингах, встречаются с клиентами и участвуют в расследованиях вместе со службой безопасности.
- «Нужно постоянно держать себя в напряжении». Окно реагирования короткое, но рабочий день устроен ритмично: алерты, разбор, обновление правил, отчёты.

Что сделать после этой главы

- Выбрать одно-два направления, которые соответствуют вашему профилю из главы 1.
- Прочитать по десять вакансий для каждого и выписать повторяющиеся требования.
- Найти один бесплатный вводный курс по выбранному направлению и пройти первый урок на этой неделе.
- Набросать абзац для резюме о случае, когда ваша внимательность или смекалка принесли результат.
- Записать три вопроса, которые вы хотели бы задать специалисту этой профессии, и найти способ их задать: отраслевое сообщество, конференция, профессиональный чат.

Коротко о главном

- Хакерское мышление востребовано в шести доступных направлениях: антифрод, кибербезопасность, QA, поддержка платёжных систем, баг-баунти и комплаенс с AML.
- Большинство входных позиций не требуют технического диплома и программирования.
- Самые доступные точки входа: поддержка и операционные отделы банков, курсы по QA и основам безопасности.
- Работодатели оценивают ход мысли и примеры реальных действий, а не количество терминов.
- Направление можно менять: переходы внутри отрасли нормальны и открывают новые возможности.