FAMBF · СПРАВОЧНЫЙ ДОКУМЕНТ

# Чек-лист безопасности бота.

14 вопросов, которые решают, выживет ли ваша торговая автоматизация в реальном рынке.

**Pavlo Filianov**

Основатель FAMBF — Framework for Automated, Mandate-Backed Finance

~30 МИН ЧТЕНИЯ
14 ВОПРОСОВ · 0–14 БАЛЛОВ

00 · ЗАЧЕМ ЭТО

# Введение.

Я начал писать этот чек-лист после того, как третий лично знакомый мне трейдер потерял большую часть счёта из-за бага в собственном боте. Никто из них не отдал деньги рынку. Они отдали их чему-то в автоматизации, что должно было быть отловлено до того, как система вообще была подключена к реальному капиталу.

Сценарий всегда один и тот же. Стратегия в порядке, код работает в нормальных условиях, а потом случается что-то непривычное. Reconnect в неудачный момент. Сигнал, пришедший дважды. Webhook, который опоздал на двадцать минут. Бот делает то, чего трейдер никогда не имел в виду, а к моменту, когда кто-то наконец заглядывает в логи, ущерб уже понесён.

Это список тех вещей, которые, по моему опыту, решают, выживает ли автоматизированная торговля в принципе или медленно разрушает счёт изнутри.

Часть из них очевидна задним числом. Часть становится очевидной только после того, как наблюдаешь, как знакомый теряет шестизначную сумму. Я постарался уложить весь документ примерно в полчаса чтения и без необходимости в каких-то специальных инструментах.

## КАК ИМ ПОЛЬЗОВАТЬСЯ

Ставьте себе ноль или один балл за каждый вопрос. Ноль означает, что ваша система этого не делает, либо вы не уверены. Один означает, что делает, причём так, что вы можете это описать, указать в коде и при необходимости продемонстрировать.

В конце сложите баллы. Шкала оценки находится в самом конце документа.

Два коротких замечания перед стартом. Будьте честны с собой; это инструмент для вас, а не маркетинговое упражнение. Если вы поставите «да» там, где сами не уверены, то оптимизируете под хорошее самочувствие сегодня и под потери позже.

И помните, что этот чек-лист на самом деле измеряет. Он смотрит на автоматизацию, а не на саму стратегию. Идеальный балл не сделает плохую стратегию прибыльной. Что он сделает: когда ваша стратегия работает, автоматизация вокруг неё не будет тем самым местом, где прибыль тихо уходит обратно.

ВОПРОС 01 · ДНЕВНОЙ CAP НА УБЫТОК

# Есть ли у вашего бота жёсткий дневной cap на убыток, который он сам не может обойти?

### ПОЧЕМУ ЭТО ВАЖНО

Самый надёжный способ, которым автоматизация уничтожает счёт, — это продолжать торговать в плохой день. У большинства стратегий есть несколько дней в году с аномальными условиями, не совпадающими с тем, под что стратегия изначально проектировалась. Без жёсткого лимита бот продолжает применять нормальную логику к ненормальным условиям, и убытки накапливаются быстрее, чем человек позволил бы им накопиться.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Настраиваемый порог (в долларах или в процентах от собственного капитала счёта), который проверяется перед отправкой каждой заявки. Когда лимит превышен, бот останавливается. Дальше поведение зависит от того, что заранее задано: открытые ордера могут быть отменены, позиции могут быть закрыты или удержаны, и трейдеру отправляется уведомление. Стоп держится до ручного сброса либо до следующей торговой сессии.

### ТИПИЧНАЯ ОШИБКА

> *Лимит существует как переменная в файле стратегии, но никогда не применяется на уровне отправки ордеров. Бот проскакивает его в быстром рынке именно тогда, когда это критично.*

ВОПРОС 02 · CAP НА РАЗМЕР ПОЗИЦИИ

# Есть ли жёсткий cap на размер позиции, на сделку и на символ?

### ПОЧЕМУ ЭТО ВАЖНО

Стратегии часто рассчитывают размер позиции динамически, исходя из волатильности или собственного капитала счёта. Это работает, пока входной параметр не начнёт вести себя странно. Значение волатильности, обнулившееся из-за пропуска в дата-фиде, может произвести из динамической формулы огромный лот, и биржа спокойно его исполнит.

Простой абсолютный cap, применяемый поверх собственной sizing-логики стратегии, перехватывает все такие случаи. Cap не заменяет sizing-логику стратегии. Он существует для того, чтобы при сбое этой логики, по какой бы то ни было причине, ущерб был ограничен.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Два потолка. На сделку: не больше X единиц в одном ордере. На символ: не больше Y единиц общего exposure по одному инструменту, независимо от того, сколько ордеров потребовалось для построения позиции. Оба проверяются на уровне отправки, а не только в логике стратегии. Настраиваются отдельно для каждого инструмента, потому что разумное для major-пары — безрассудно для small-cap альткоина.

### ТИПИЧНАЯ ОШИБКА

> *Cap существует на уровне стратегии, но не учитывает частичные исполнения, повторы и повторные входы после stop-out. На третьем повторном входе реальная экспозиция в несколько раз превышает заявленный лимит.*

ВОПРОС 03 · WITHDRAWAL API

# Создан ли API-ключ с явным отключением права на withdrawal?

### ПОЧЕМУ ЭТО ВАЖНО

У торгового бота нет ни одной законной причины выводить средства. Ни одной. Если систему каким-то образом скомпрометируют, будь то утечка ключа, атакующий на вашей машине или вредоносное обновление библиотеки, единственное, что стоит между атакующим и вашими деньгами, — это набор прав на этом ключе.

Отключённый withdrawal означает, что худший сценарий — нежелательные позиции, и это поправимо. Включённый withdrawal означает, что средства уходят за считанные минуты.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Каждый ключ, который использует автоматизация, создан с отключённым правом на withdrawal на уровне биржи. IP-allowlisted там, где биржа это поддерживает. Ротируется по известному графику, разумно — раз в 90 дней. Хранится в нормальном secret manager, а не в конфиг-файле и не в чате.

### ТИПИЧНАЯ ОШИБКА

> *Изначальный ключ был создан с включённым withdrawal «на всякий случай» и теперь живёт в dotfile на вашем ноутбуке, на облачном сервере и в трёх заброшенных папках проектов.*

ВОПРОС 04 · ДУБЛИКАТЫ ОРДЕРОВ

# Если бот переподключается после разрыва, корректно ли он распознаёт ордер, который отправил, но подтверждения по которому не получил?

### ПОЧЕМУ ЭТО ВАЖНО

Это режим отказа, который я в реальной жизни встречаю чаще всего. Бот отправляет ордер. Связь рвётся до того, как ответ дойдёт. Бот переподключается, запрашивает открытые ордера, и того ордера там нет — потому что он уже исполнился. Бот трактует «открытых ордеров нет» как «ордер не был отправлен» и шлёт ещё один. Трейдер оказывается в позиции вдвое больше задуманной, с логикой выхода, написанной под одну единицу.

Разрывы соединения — не редкость. Они случаются каждые несколько часов в нормальных условиях, чаще через домашний интернет или дешёвый VPS. Любой бот, работающий дольше пары недель, через это пройдёт.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Каждый ордер несёт детерминированный client_order_id, по которому биржа отклоняет дубликаты на своей стороне. При переподключении бот запрашивает исполненные ордера с последней известной метки времени (а не только открытые) и сверяет ожидаемое состояние с фактическим состоянием биржи. Там, где есть неопределённость, бот делает паузу в 30–60 секунд, прежде чем размещать что-либо новое.

### ТИПИЧНАЯ ОШИБКА

> *Бот доверяет тому, что видит в «открытых ордерах» при переподключении, без сверки с историей исполнений. Первый же сетевой провал тихо удваивает позицию.*

ВОПРОС 05 · УСТАРЕВШИЕ СИГНАЛЫ

# Отбрасывает ли бот сигнал, пришедший слишком поздно, чтобы быть полезным?

### ПОЧЕМУ ЭТО ВАЖНО

Торговые сигналы валидны только в пределах окна. TradingView-алерт, который говорит «купить на открытии часовой свечи», имеет смысл на открытии этой свечи. Через три часа, на другой свече, в другом ценовом режиме, тот же сигнал — это уже случайная сделка.

Задержки webhook'ов происходят постоянно. У самого TradingView в волатильные периоды бывали многоминутные задержки. Cloud-функции делают cold-start. Notification-сервисы накапливают очередь. Бот, который обрабатывает каждый поступивший сигнал независимо от его возраста, рано или поздно совершит сделку по инструкциям двадцатиминутной давности.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Каждый сигнал несёт метку времени с источника. Бот проверяет возраст сигнала в момент, когда собирается действовать. Если сигнал старше заданного порога (обычно секунды для интрадея, минуты для swing-сетапов), он логируется, по нему отправляется alert, и сигнал отбрасывается.

### ТИПИЧНАЯ ОШИБКА

> *Бот обрабатывает сигналы в порядке поступления без проверки возраста. Двадцатиминутный накопленный backlog после сбоя webhook'а порождает двадцать минут устаревших сделок, как только очередь разгребётся.*

ВОПРОС 06 · KILL SWITCH

# Можете ли вы остановить систему меньше чем за пять секунд с телефона, не заходя в кабинет биржи?

### ПОЧЕМУ ЭТО ВАЖНО

Когда что-то идёт не так с живым ботом, дорога каждая секунда. Если единственный способ его остановить — это зайти по SSH на сервер и убить процесс, или зайти в кабинет биржи и начать вручную отменять ордера, трейдер либо застынет, либо сделает не то движение. В первые тридцать секунд, наблюдая за необъяснимым поведением своего счёта, люди не принимают хороших решений.

Kill switch должен быть одним осознанным действием, доступным оттуда, где вы в данный момент находитесь.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Простой интерфейс, который можно вызвать с телефона меньше чем за пять секунд. Команда Telegram-боту, кнопка на дашборде, SMS-код — что угодно, что не требует залезания в UI биржи. Срабатывание kill switch логируется с меткой времени. После срабатывания бот не может возобновиться без явного ручного перезапуска, в идеале с подтверждением, что трейдер просмотрел состояние.

### ТИПИЧНАЯ ОШИБКА

> *«Kill switch» требует зайти в облачную консоль, найти нужный сервис и остановить контейнер. Трейдер возится с двухфакторкой, пока позиция уходит против него.*

ВОПРОС 07 · PAPER-РЕЖИМ

# Когда бот работает в paper-режиме, идёт ли он по тому же code path, что и live?

### ПОЧЕМУ ЭТО ВАЖНО

Распространённый паттерн — держать paper-режим как отдельную ветку или отдельный скрипт. Со временем paper-версия расходится с live-кодом. Новые фичи добавляются в live и забываются в paper. Bugfix'ы применяются в одном месте и не применяются в другом.

К моменту, когда вы хотите проверить изменение в paper, вы тестируете систему, уже не похожую на то, что реально торгует. Ложное чувство безопасности хуже, чем полное отсутствие paper-режима.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Всё, что выше слоя исполнения, общее у paper и live: risk engine, логика стратегии, order builder, реконсиляция. Единственное, что реально отличается, — это адаптер на самом краю. В paper-режиме он говорит с симулятором (testnet, внутренний симулятор или повторно проигранные live-данные). В live-режиме он говорит с реальной биржей. Переключение между ними — это конфигурационный флаг, а не изменение в коде.

### ТИПИЧНАЯ ОШИБКА

> *Paper и live — это два разных скрипта. Последний раз paper-версию открывали полгода назад, и она даже не собирается под текущую схему данных.*

ВОПРОС 08 · ЛОГИ РЕШЕНИЙ

# Записывается ли каждое решение бота с меткой времени?

### ПОЧЕМУ ЭТО ВАЖНО

Когда бот делает что-то, чего вы не ожидали, первый вопрос всегда «почему». Единственный способ на него ответить — логи, и эти логи должны покрывать не только отправленные ордера и исполнения. Каждый поступивший сигнал, каждый фильтр, который прогнался против него, каждая риск-проверка, которая прошла или не прошла, каждая причина, по которой сделка не была взята: всё это должно быть зафиксировано. Без этого post-incident анализ — это гадание.

Логи также ловят медленный дрейф. Фильтр, который тихо стал слишком узким. Постепенно растущий slippage. Падающий месяц за месяцем win rate. Ничего из этого не видно по дневному P&L, но всё это имеет значение.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Структурированное логирование (JSON или подобное) для каждого значимого события. UTC-метки времени с миллисекундной точностью. Чёткие типы событий: signal_received, signal_rejected, order_submitted, order_filled, risk_breach, kill_activated. Хранение минимум 90 дней. Доступны для запросов без grep'а по гигабайтам текста. Даже простая таблица в Postgres с нормальными индексами справится с этим.

### ТИПИЧНАЯ ОШИБКА

> *Бот пишет в текстовый log-файл где-то на сервере. Никто туда не смотрит, пока что-то не сломается. К этому моменту файл уже отротировался, и нужных записей в нём нет.*

ВОПРОС 09 · ГИГИЕНА API-КЛЮЧЕЙ

# Хранятся ли API-ключи зашифрованно, отдельно от кодовой базы, и ротируются ли они по известному графику?

### ПОЧЕМУ ЭТО ВАЖНО

API-ключи — это учётные данные к вашим деньгам. Большинство утечек, о которых я слышал, не были изощрёнными атаками. Это были ключи, закоммиченные в публичный Git-репозиторий, скопированные в чат при просьбе о помощи с отладкой, оставленные на скриншоте, загруженном в саппорт, или сохранённые в dotfile, синхронизированной в облако.

Ротация важна, потому что компрометация не всегда известна. Утёкший ключ, лежащий без дела месяцами, — это безвредно. Тот же ключ в чужих руках во время волатильного дня обходится дорого. Ротация ограничивает окно, в которое любая утечка может быть использована.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Ключи живут в выделенном secret store: в managed-сервисе, в self-hosted vault или в зашифрованных переменных окружения, которые предоставляет хостинг-платформа. Никогда в кодовой базе. Никогда открытым текстом на диске. Ротируются по графику (90 дней — разумно), и процесс ротации заранее протестирован, чтобы он не сломал бот, когда сработает реально.

### ТИПИЧНАЯ ОШИБКА

> *Трейдер знает, что ключи «где-то в надёжном месте», но не может конкретно показать, где именно. А последняя ротация была в день, когда бот был развёрнут впервые.*

ВОПРОС 10 · INCIDENT-ПРОТОКОЛ

# Есть ли у вас письменная процедура на случай, когда биржа отклоняет ордер или не подтверждает исполнение?

### ПОЧЕМУ ЭТО ВАЖНО

Биржи — не идеально надёжные системы. Они отклоняют ордера по причинам, в которых не всегда есть смысл. Иногда они принимают ордер, а потом сообщают, что отклонили. Иногда они теряют исполнения и требуют сверки. Бот, который исходит из того, что биржа всегда отвечает корректно, рано или поздно окажется в состоянии, в котором его внутреннее представление расходится с тем, что биржа показывает на самом деле.

Incident-протокол — это ответ на вопрос «что делает бот, когда реальность и его ожидания расходятся».

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Документированный список сценариев ошибок, каждый со своей определённой реакцией. На каждый тип ошибки есть чёткий ответ: когда безопасно делать retry, когда нужно поднять алёрт трейдеру вместо тихой обработки, и когда вся система должна встать на паузу, пока человек не подтвердит, в каком состоянии всё на самом деле находится. Протокол записан на бумаге, а не просто реализован в коде, чтобы трейдер мог его читать и обновлять по мере изменения условий.

### ТИПИЧНАЯ ОШИБКА

> *Обработка ошибок — это то, что разработчику пришло в голову обработать в моменте. Неожиданные ошибки роняют процесс, его автоматически перезапускают, и бот возобновляет торговлю без того, чтобы кто-то заметил, что состояние сбросилось.*

ВОПРОС 11 · ПОЭТАПНЫЙ ЗАПУСК

# Запускалась ли эта система поэтапно, или первый день уже был развёртыванием в полный размер?

### ПОЧЕМУ ЭТО ВАЖНО

Стратегии в backtest'ах выглядят лучше, чем перформят live. Это не предмет спора. Slippage в реальности больше. Исполнения медленнее. Какие-то сетапы вообще не срабатывают, потому что данные, на которых строился backtest, были чище, чем live-feed. У любой автоматизации есть баги, которые не проявляются, пока она не побежит против настоящего поведения биржи.

Поэтапный запуск даёт возможность найти эти проблемы на маленьких деньгах, а не на полном размере. Стандартная последовательность: сначала paper, затем shadow-режим (live-данные, но без реальных ордеров), затем micro-live на минимальном размере, который ещё что-то говорит, и только затем постепенно крупнее, по мере того как доверие к системе реально нарастает.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Заранее согласованный план запуска с явной длительностью и критериями успеха для каждой стадии. Размер позиции в micro-live достаточно мал, чтобы полная потеря тестового капитала не имела значения. Переход на следующую стадию требует положительного ревью, а не просто истёкшего времени. План записан до того, как бот пошёл в live.

### ТИПИЧНАЯ ОШИБКА

> *Бот «потестировали в paper» пару дней, потом подключили к живому счёту в обычном размере, потому что paper-результаты «выглядели хорошо». Первый реальный баг проявляется на реальной позиции.*

ВОПРОС 12 · ДАШБОРД

# Есть ли дашборд, отдельный от интерфейса биржи, в который вы реально регулярно заходите?

### ПОЧЕМУ ЭТО ВАЖНО

Большинство трейдеров проверяют бот, заходя в кабинет биржи и глядя на позиции. Это говорит вам, что считает биржа, а не что считает бот. Расхождение этих двух представлений — это именно то, что должно быть пойманно рано, и единственный способ это поймать — смотреть на представление бота независимо.

Дашборд — это ещё и место, где становится виден медленный дрейф. Падающий неделя за неделей win rate. Постепенно растущий slippage. Повышающиеся отказы по сигналам, потому что фильтр стал слишком узким. Ничего из этого не видно на дневном P&L, но всё это имеет значение.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Простой веб-интерфейс (необязательно красивый), показывающий текущее состояние: активные позиции, недавние исполнения, недавние сигналы, недавние отказы, текущая загрузка риск-лимитов, последний статус kill switch. Историческое представление минимум за 30 дней. Доступен с телефона. Проверяется по чёткому графику, минимум ежедневно.

### ТИПИЧНАЯ ОШИБКА

> *Дашборда нет. Трейдер изредка проверяет приложение биржи и доверяет тому, что у бота всё в порядке, потому что кривая капитала «примерно плоская».*

ВОПРОС 13 · SLIPPAGE

# Отслеживает ли бот slippage по каждому исполнению и ставит ли торговлю на паузу при превышении порога?

### ПОЧЕМУ ЭТО ВАЖНО

Slippage — это разница между ценой, которую ожидал бот, и ценой, которую он реально получил. В нормальных условиях slippage невелик и предсказуем. В ненормальных условиях slippage может стать огромным, иногда на порядки хуже того, что предполагал backtest. Эти ненормальные условия бывают разными: быстрые рынки, тонкая ликвидность, деградация биржи, регуляторные новости в середине сессии.

Бот, который игнорирует slippage, спокойно продолжает торговать через эти условия, получая исполнения по всё худшим ценам, пока edge стратегии не съедается стоимостью исполнения.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Slippage измеряется по каждому исполнению в базисных пунктах относительно ожидаемой цены. Скользящее среднее по короткому окну. Когда среднее превышает порог (всё, что выше 5x обычного, подозрительно), бот ставит торговлю на паузу и шлёт alert. Порог настраивается отдельно для каждого инструмента.

### ТИПИЧНАЯ ОШИБКА

> *Slippage вообще не измеряется. Backtest стратегии предполагал один базисный пункт slippage. Live-условия во время стресс-события дают пятьдесят, а бот продолжает торговать.*

ВОПРОС 14 · САР НА УСРЕДНЕНИЕ

# Принудительно ли ограничено максимальное число шагов усреднения или DCA в коде, а не только в документе стратегии?

### ПОЧЕМУ ЭТО ВАЖНО

Многие стратегии используют усреднение, то есть докупание в позицию по мере её движения против изначальной точки входа. В нормальном рынке это работает. Это же даёт некоторые из самых сильных blow-up'ов в розничном трейдинге, потому что представление стратегии о том, «сколько раз можно усредниться», как правило больше того, что счёт реально может вынести во время серьёзного движения.

В документе стратегии может быть написано «усредняться до пяти раз». Код, если ему явно не сказано иначе, усредняется столько раз, сколько срабатывает сигнал. Во время быстрого встречного движения это может быть десять или двадцать раз.

### КАК ЭТО ВЫГЛЯДИТ ПРАВИЛЬНО

Жёсткий счётчик в слое исполнения, который отслеживает шаги усреднения по каждой позиции. После настроенного лимита больше никаких ордеров на усреднение не принимается, независимо от того, что говорит сигнал. Счётчик сбрасывается только при полном закрытии позиции, а не при частичном уменьшении. Лимит консервативный, ниже того, что стратегия «могла бы» вынести в нормальном рынке, потому что сар существует для рынков ненормальных.

### ТИПИЧНАЯ ОШИБКА

> *Лимит усреднения живёт в файле стратегии как переменная, которую стратегия должна уважать. В быстром движении логика стратегии не успевает её проверить, и бот продолжает усредняться в свободном падении.*

15 · ОЦЕНКА

# Оценка.

Сложите ваши нули и единицы по 14 вопросам. Результат скажет, где находится ваша система.

**0–5**

КРИТИЧЕСКИЙ РИСК

Система в одном плохом дне от серьёзной потери, не имеющей отношения к стратегии. Рекомендация: остановить live-торговлю, пока пробелы не закрыты.

**6–9**

СУЩЕСТВЕННЫЕ ПРОБЕЛЫ

Система будет работать большую часть времени, но непокрытые режимы отказа — те, что наносят больше всего ущерба. Фокусный проект на одну-две недели поможет закрыть непроверенные пункты.

**10–12**

КРЕПКО

Основные риски закрыты. Оставшиеся пункты обычно касаются качества мониторинга, операционной дисциплины или граничных случаев, которые трейдер сознательно принял.

**13–14**

INSTITUTIONAL-GRADE

Система собрана на уровне того, как должна выглядеть корректно поставленная торговая операция. Главная оставшаяся забота — дрейф во времени: операционные практики, которые были хороши на старте, тихо ослабевают, пока система работает годами.

16 · СЛЕДУЮЩИЕ ШАГИ

# Если нужно второе мнение.

Если у вас меньше 10 баллов и хочется второго мнения по тому, какие пробелы важнее всего для вашего конкретного сетапа, напишите мне. Я провожу платные hardening-аудиты существующей автоматизации. Формат — 30-минутный звонок и письменное ревью против этого чек-листа и против вашего реального кода и конфигурации. На выходе вы получаете приоритизированный список: что чинить сейчас, что нормально как есть, чего не стоит вообще трогать.

Если у вас больше 10 и вы думаете о расширении того, что покрывает ваша автоматизация (новые рынки, дополнительные стратегии, более жёсткие риск-контроли), это другой разговор, и я тоже рад его провести.

## Pavlo Filianov

Основатель FAMBF — Framework for Automated, Mandate-Backed Finance

25 лет на рынках, из них первые 13 — частично через лицензированную брокерскую компанию, которую я основал в Украине, а последнее десятилетие — преимущественно в крипте. Я строю автоматизацию для самостоятельных трейдеров, которые хотят, чтобы их правила реально работали на их собственном счёте.

→ fambf.com
→ pavlo@fambf.com
→ Записаться на 30-минутный звонок
→ LinkedIn