

18+
Гудик

Багдасарян

Телохранитель

Инструкция побеждать

Часть 2

Рудик Багдасарян

**Телохранитель. Инструкция
побеждать. Часть 2**

«Издательские решения»

Багдасарян Р.

Телохранитель. Инструкция побеждать. Часть 2 / Р. Багдасарян —
«Издательские решения»,

ISBN 978-5-00-695041-2

Второй том «Телохранитель. Профессиональный стандарт». Вы узнаете, как интегрировать кибербезопасность в физическую охрану, работать в зонах вооруженных конфликтов и юридически безупречно защищать свои действия. А также это руководство по переходу от роли исполнителя к роли руководителя службы безопасности. Эта книга о том, как сделать качественный скачок в профессии, где холодный расчет и стратегическое видение ценятся выше сиюминутной храбрости.

ISBN 978-5-00-695041-2

© Багдасарян Р.
© Издательские решения

Содержание

ТЕЛОХРАНИТЕЛЬ. ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ	6
Часть 2-я:	6
РАЗДЕЛ VII: КИБЕРБЕЗОПАСНОСТЬ И OSINT-РАЗВЕДКА	7
Конец ознакомительного фрагмента.	14

Телохранитель. Инструкция побеждать Часть 2

Рудик Багдасарян

© Рудик Багдасарян, 2026

ISBN 978-5-0069-5041-2 (т. 2)

ISBN 978-5-0068-7761-0

Создано в интеллектуальной издательской системе Ridero

ТЕЛОХРАНИТЕЛЬ. ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Часть 2-я: ЭКСПЕРТНЫЙ УРОВЕНЬ И СПЕЦИАЛИЗАЦИЯ

Вступление: От управления рисками к их предвосхищению

В первой части мы заложили фундамент: научились замечать угрозу, управлять пространством и действовать по алгоритму в критической ситуации. Мы ответили на вопрос «что делать» и выстроили каркас личности — этический кодекс и психологическую устойчивость.

Вторая часть посвящена переходу от реактивного мышления к проактивному.

Это уровень, на котором телохранитель перестает быть просто живым щитом и становится архитектором безопасности.

Здесь важно уметь работать не только с физическим пространством, но и с цифровым следом, понимать геополитические риски, выстраивать службу безопасности с нуля в любой точке мира и, главное, юридически безупречно защищать свои действия, если предотвратить угрозу не удалось.

Главное изменение парадигмы 2026 года

Больше нет разделения на кибер и физику. Репутацию клиента или сделку теперь можно уничтожить без единого выстрела — через взлом почты, слив переписки или публикацию компромата в Telegram.

Современная угроза всегда гибридна:

дрон ведет слежку, инфостилер сливает геолокацию, а поддельное сообщение может сорвать операцию. Значит, и подход к безопасности должен быть таким же гибридным.

РАЗДЕЛ VII: КИБЕРБЕЗОПАСНОСТЬ И OSINT-РАЗВЕДКА



Цель раздела: научить телохранителя выявлять цифровой след клиента, устранять слабые места в виртуальном пространстве и находить открытую информацию раньше злоумышленников.

Введение

Раньше мы разбирали уличные угрозы: подозрительных прохожих, автомобили наблюдения и потенциальных преступников. Теперь акцент смещается в цифру. Любой профессиональный злоумышленник начинает с изучения онлайн-информации. Задача телохранителя — закрыть пробелы в цифровой защите, не допустить утечек чувствительных данных и надежно охранять клиента как в офлайне, так и в онлайн.

Глава 27. Киберугрозы для VIP-клиентов в 2026 году

27.1. Инфостилеры

Инфостилеры воруют личные данные клиента с помощью вредоносного ПО. Достаточно одного неосторожного клика по ссылке в мессенджере — и устройство оказывается под контролем злоумышленников. Программа скрытно собирает пароли, файлы, фотографии и передает их третьим лицам.

По статистике за первое полугодие 2025 года, инфостилеры украли свыше 1,8 миллиарда учетных записей пользователей. Среди жертв — и клиенты VIP-уровня: конфиденциальные данные продаются в теневом сегменте интернета за сравнительно небольшие деньги. Получив доступ к личным фото, банковским реквизитам и семейным чатам, злоумышленники наносят не только материальный ущерб, но и создают прямую угрозу физической безопасности клиента.

27.2. Синтезированные атаки

Сочетание хакерской активности и физической преступности — один из ключевых трендов 2025—2026 годов. Современные злоумышленники собирают сведения о распорядке дня клиента через домашние устройства, сервисы доставки и цифровые следы повседневной жизни. Затем эти данные передаются физическим преступникам, которым гораздо проще действовать, когда они знают привычки, маршруты и слабые места цели.

Например, хакеры могут выяснить расписание работы камер видеонаблюдения, и это уже облегчает проникновение в дом.

27.3. Дипфейки

Технологии синтеза изображения и речи стали доступны практически любому человеку. На их основе создаются поддельные видео, компрометирующие VIP-персону, или фальшивые распоряжения от имени руководителя. Такие манипуляции способны нанести бизнесу финансовый и репутационный ущерб за считанные часы.

Кейс: взлом умного дома в Москве

Бизнесмен заметил странности в работе домашней автоматизации: ночью сами включались шторы, а по расписанию без причины запускалась громкая музыка. Специалист обнаружил устаревшую прошивку роутера, через которую злоумышленники получили доступ к камерам и начали наблюдение за жильцами. Выяснилось, что готовилась не только цифровая атака, но и возможное физическое преступление: преступники изучали ежедневный график владельца дома.

Решение было простым и жестким: заменить старый роутер, обновить программное обеспечение, изолировать домашнюю сеть от гостевой и взять устройства под постоянный контроль.

Вопросы для самопроверки

Что такое инфостилер и какие данные он может украсть?

Чем опасны синтезированные атаки?

Как дипфейки могут быть использованы против клиента?

Какие меры были приняты в кейсе с взломом умного дома?

Практическое задание к главе 27

Проверьте электронную почту на наличие утечек через сервис вроде HaveIBeenPwned. Узнайте, участвовал ли ваш email в известных утечках данных. Подготовьте краткий отчет с рекомендациями сменить пароли и усилить информационную безопасность.

Глава 28. OSINT: чтобы бить первым

В предыдущей главе мы разобрали основные виды киберугроз. Теперь переходим к инструменту, который позволяет обнаруживать угрозы еще на стадии подготовки. Эта глава посвящена открытому поиску информации, который помогает выявлять риски и предотвращать неприятности до того, как они станут проблемой.

28.1. Протокол OSINT-мониторинга

Мониторинг должен быть регулярным. Одной проверки недостаточно. Угрозы появляются ежедневно, поэтому каждую неделю нужно проходить по четкому плану.

Шаг первый. Мониторинг утечек

Проверяйте электронную почту и телефоны клиента, а также членов его семьи, в базах утекших данных. Если обнаружена новая утечка, немедленно меняйте пароли.

Шаг второй. Анализ социальных сетей семьи

Дети и супруги клиентов часто невольно становятся источником утечек. Обращайте внимание на геотеги, номера домов, названия улиц, фото возле школы, ресторана или дома. Все это может лечь в основу карты маршрутов для потенциальных преступников.

Шаг третий. Мониторинг Telegram-каналов и форумов

В криминальной среде Telegram давно заменил даркнет. Отслеживайте каналы и форумы, где появляются упоминания клиента, его семьи, фирмы или привычных маршрутов.

Шаг четвертый. Анализ цифровой инфраструктуры

Проверьте, не используется ли личный номер телефона клиента для привязки к рабочим аккаунтам. Личный номер должен оставаться личным, а рабочие контакты — быть изолированы. Смешение этих контуров создает ненужные риски.

28.2. Арсенал инструментов для OSINT

Не нужно быть хакером или покупать дорогие программы. Есть простой и доступный набор инструментов, который можно использовать уже сейчас.

Сервисы проверки утечек

Платформы вроде HaveIBeenPwned и Dehashed помогают быстро понять, попадали ли данные в известные утечки. Достаточно ввести email или номер телефона.

Сервисы обратного поиска изображений

Google Images и Yandex Images позволяют проверять, где еще используется фото клиента или его семьи. Это помогает выявлять фейковые аккаунты и поддельные страницы.

Программы для анализа метаданных

ExifTool позволяет извлекать из фотографий модель камеры, дату съемки и GPS-координаты. Многие не знают, что снимок может содержать точное место съемки. Поэтому перед публикацией такие данные нужно удалять.

Кейс: предотвращение похищения через Telegram

Накануне отпуска семьи клиента служба безопасности проводила обычный еженедельный мониторинг. В одном из Telegram-каналов всплыло объявление о продаже доступа к приватному чату известного бизнесмена. В посте были скриншоты переписки супруги клиента с подругой, где обсуждались точные даты перелета и место отдыха.

Старший группы безопасности сразу оценил угрозу как критическую.

Аккаунт был заблокирован, все пароли немедленно сменены. Решили полностью изменить план поездки: выбрали другой рейс, сдвинули дату вылета на пять дней, купили билеты другой авиакомпания и на другие имена.

Дополнительно распространили ложную информацию о старом плане и заранее организовали охрану в аэропортах вылета и прилета.

Если засада и планировалась, преступники столкнулись с пустотой. Угроза была сорвана на этапе подготовки благодаря своевременному мониторингу.

Вопросы для самопроверки

Каков порядок шагов в протоколе еженедельного OSINT-мониторинга?

Почему анализ соцсетей членов семьи так же важен, как и анализ профиля самого клиента?

Для чего нужен сервис обратного поиска изображений?

В чем риск геотегов на фотографиях?

Чек-лист: еженедельная OSINT-сводка

Пункт проверки: email клиента проверен в базах утечек

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Пункт проверки: телефоны клиента проверены в базах утечек

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Пункт проверки: соцсети супруги проверены на наличие геотегов и опасных публикаций

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Пункт проверки: соцсети детей проверены на наличие геотегов и опасных публикаций

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Пункт проверки: Telegram-каналы проверены на упоминания клиента и его семьи

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Пункт проверки: новые фото клиента и семьи найдены в поисковиках

Статус: выполнено / не выполнено

Оценка риска: низкий / средний / высокий

Комментарий:

Практическое задание к главе 28

Выберите публичную личность для учебной тренировки.

Исследуйте ее аккаунты и аккаунты ближайших родственников только в открытых источниках.

По открытым данным восстановите примерный график перемещений за последнюю неделю.

Подготовьте отчет на одну страницу: какие данные найдены, какие из них создают риск, и три рекомендации по повышению приватности.

Глава 29. Цифровая гигиена и защита от технической слежки

Обнаружить угрозу — это половина дела. Вторая половина — научить клиента и его семью правилам безопасности, которые сделают их невидимыми для цифрового наблюдения.

29.1. Правила чистой работы с телефоном

Постоянно поддерживайте чистоту цифрового пространства клиента. Эти правила должны стать его привычкой.

Правило первое. Запрет на открытый Wi-Fi без VPN

Ни в коем случае не используйте общественные сети без защиты VPN. Особенно это касается кафе, аэропортов, вокзалов и гостиниц. Открытые сети — это идеальные ловушки для перехвата трафика.

Правило второе. Раздельные SIM-карты и телефоны

Держите отдельно личные и рабочие сим-карты. Идеально — использовать разные устройства для семейных нужд и деловых целей. Если телефон для бизнеса взломают, данные семьи останутся в безопасности.

Правило третье. Двухфакторная аутентификация и аппаратные ключи

На всех критически важных аккаунтах должна быть включена двухфакторная аутентификация. Применяйте аппаратные ключи. Они надежнее SMS, которые можно перехватить. Храните сложные и уникальные пароли в специальном менеджере.

Правило четвертое. Регулярная смена паролей

Установите периодичность обновления паролей. Раз в три месяца — для особо важных аккаунтов. Раз в полгода — для остальных. Пароли должны быть разными для разных сервисов.

29.2. Физическая борьба с техническими средствами слежки

Цифровая гигиена не отменяет физического контроля. Техническая слежка часто дополняет цифровую.

Проверка автотранспорта

Каждую неделю проводите осмотр автомобиля клиента. Особое внимание уделяйте:

Днищу. Магнитные трекеры часто крепятся именно туда.

Колесным аркам. Удобное место для быстрой установки.

Багажнику и салону. Под сиденьями, в бардачке, за обшивкой.

Проверка помещений

Перед важными переговорами или размещением клиента в новом отеле проводите осмотр помещения. Используйте специальные приборы:

Детекторы электромагнитного излучения для поиска работающих камер и микрофонов.

Спектральные анализаторы для выявления сложных закладок.

Контроль за умными устройствами

В процессе секретных переговоров отключайте всю технику от электропитания. Недостаточно просто сказать голосовому помощнику «выключись». Нужно выдернуть шнур питания. Любое устройство, подключенное к сети, может быть скомпрометировано.

Кейс: GPS-трекер под бензобаком

Ситуация:

Водитель-телохранитель московского бизнесмена проводил стандартную проверку автомобиля. Осматривая днище с помощью телефона на палке, он заметил небольшую коробочку, скрытую под бензобаком внедорожника. Коробочка была примотана пластиковыми стяжками.

Обнаружение:

Внутри оказался GPS-трекер с встроенной SIM-картой, обеспечивавший передачу координат автомобиля в режиме реального времени. Автономность устройства составляла примерно 30 суток. Трекер был закреплен так, чтобы его невозможно было заметить при обычном беглом осмотре.

Расследование:

Трекер не трогали руками, чтобы сохранить отпечатки. Вызвали полицию. Анализ данных вывел на группу, которая уже несколько недель следила за перемещениями бизнесмена.

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.