Интервью с белыми хакерами. Как выглядит их работа изнутри и считается стоимость взлома

Антон Бочкарёв:
О профессии белого хакера и устройстве рынка кибербезопасности

Егор Богомолов:
Как белые хакеры помогают бизнесу и формируют культуру кибербезопасности

Павел Чернышев:
Чем чревата атака на бизнес и какие ошибки допускают в сфере информационной безопасности

Антон Бочкарёв

сооснователь компании «Третья Сторона» и эксперт по кибербезопасности

О профессии белого хакера и устройстве рынка кибербезопасности

Как становятся белыми хакерами

Люди приходят в индустрию после профильного высшего образования или курсов. Значительную долю составляют самоучки из смежных областей. Важно, чтобы мышление человека подходило для этой профессии — помогает желание что-то постоянно искать и тестировать весь мир вокруг нас.

Какая мотивация у белых хакеров

Все, кто работает в кибербезопасности, понимают, что взломать можно абсолютно любую систему. Невозможно создать стопроцентную защиту — ее делают люди, а люди ошибаются.

У белого хакера в крови вызов самому себе и неуемное любопытство сделать что-то экстраординарное. А еще такие исследования дают возможность выступить на конференции, поделиться результатами на профильном блоге, попасть в виртуальный «зал славы».

Конечно, взлом — это и заработок тоже. Компании платят большие деньги за особо важные исследования и уязвимости нулевого дня, от которых не существует защиты. Некоторые исследователи занимаются поиском только чего-то экстраординарного, тратят значительное время и ресурсы и получают за это хорошее вознаграждение.

Исследователю важна свобода действия, широта охвата и профиль проекта: для белого хакера важно, чтобы сложность и особенности задачи всегда отличались.

Как устроена работа белого хакера

Небольшая компания, которая платит за выявление уязвимости до 1 млн ₽, обычно имеет ограниченный периметр, где мало что можно сломать. При таком бюджете белые хакеры проверяют компанию стандартными методами. Это социальная инженерия, то есть вредоносные письма и звонки сотрудникам, а также отслеживание случайных ошибок.

С бюджетом в 10 млн ₽ можно потратить на исследования значительное время, организовать детальную проработку социальной инженерии и технических атак.

С бюджетом от 50 млн ₽ появляется возможность купить то, что дорого ценится на черном рынке. Например, фрагменты вредоносного кода или последовательности команд для самых современных уязвимостей, которые пока не используются массово и публично.

Сходства и отличия черных и белых хакеров

Черные и белые хакеры атакуют одними и теми же способами, но цели у них разные. Обмен опытом у белых — на конференциях, у черных — на форумах и каналах в даркнете. Главное отличие — это образ мысли. Черные хакеры уверены, что можно нарушать законы и делать что угодно безнаказанно.

Существует серая зона, где работают исследователи и аналитики угроз. Они развивают свои учетные записи на черных форумах, чтобы следить за утечками и за продажами доступов к компаниям. Правоохранительные структуры также ведут агентурную работу в серой зоне.

Сколько зарабатывает белый хакер

Если грубо оценивать в годах активной работы в крупных компаниях, то можно взять зарплату ИТ-специалиста, вычесть 30% и получить деньги в кибербезе. Помимо основной работы можно делать сторонние проекты, брать подработки по знакомству либо через агрегатор — и на этом зарабатывать больше.

Например, с утра до вечера специалист защищает периметр своего работодателя, а после работы или по выходным с собственной командой пытается реализовать недопустимое событие другой компании за вознаграждение в несколько миллионов рублей.

Недопустимое событие как основа стратегии

Для бизнеса не всегда понятно, в чем ценность отдельно найденной уязвимости. Другой вопрос, когда тебе могут наглядно показать, как можно остановить твое производство, украсть персональные данные клиентов или выкрасть со счета деньги.

В этом случае на кибербезопасность обращают внимание не только технические специалисты, но и весь менеджмент, на глазах которого произошло событие, которое может нанести бизнесу неприемлемый ущерб.

Концепция киберисптаний взяла все лучшее из предыдущих подходов и максимально приблизила это к реальным атакам черных хакеров с пользой для бизнеса. В этом случае исследователи могут показать, как можно фактически остановить бизнес, но сделает это в доверенной среде и без реальных рисков. Компания в этом случае поймет, какие проблемы у нее в ИТ-инфраструктуре и исправит их, чтобы ими не смогли воспользоваться злоумышленники.

Какие ошибки допускают компании в построении защиты

Самая распространенная ошибка — защищаются не от того, от чего нужно. В России концепция недопустимых событий появилась всего пару лет назад. Бизнесу начали объяснять, что нужно не защищаться от всех рисков на свете — это грозит потерей денег впустую — а покрывать самое важное и проверять полученный результат.

Во-вторых, компании часто тратят огромный бюджет на то, что им в действительности не требуется. Это только увеличивает строку расходов, что в условиях экономической нестабильности вызывает дополнительную напряженность для компании.

В-третьих, компании сращивают ИТ и информационную безопасность (ИБ). Это большая проблема, потому что одно должно контролировать другое. ИТ-специалист должен думать о том, чтобы все работало и было удобно. А представитель ИБ должен думать о безопасности — это разные задачи.

И последняя ошибка — компании не используют все возможности рынка внешних подрядчиков и кибербезопасности. Многие думают, что обязательно нужно нанимать людей в штат и это очень дорого — хотя на деле это необязательно.

Что бизнес может перенять у хакеров

Белые хакеры и их работа помогает бизнесу задуматься, что конкретно для него станет тем самым недопустимым событием, которое полностью остановит функционирование компании. Так можно по-новому взглянуть на выстроенные процессы, ИТ-инфраструктуру и трансформироваться во что-то более защищенное. А это позитивно отразится не только на самой компании, но и на клиентах, и на всей экономике страны.

Получите грант и узнайте, можно ли вас взломать за 1 млн ₽

Егор Богомолов

генеральный директор компаний CyberEd и Singleton Security

Как белые хакеры помогают бизнесу и формируют культуру кибербезопасности

Кто такие белые хакеры и как ими становятся

Белый хакер — это специалист, которого нанимает бизнес, чтобы сделать систему более защищенной. Решив стать хакером, в течение первого года вырабатываешь понимание виртуального мира и его законов. Во второй год набиваешь руку и закрепляешь результат. Лет через пять, наконец, понимаешь, что нужно делать.

Какие черты отличают белого хакера

Это очень трудолюбивый и усидчивый человек. Хакер может месяц сидеть, чтобы найти первые пути ко взлому компании. Ему нужна только победа, а потом сразу приходится искать другую, еще более сложную уязвимость.

Второе — это сильная техническая эрудиция и скорость обучения. И третье — это творческая гибкость ума, умение сложить какие-то вещи, которые никто не складывал до тебя.

Почему белый хакер — помощник бизнеса, а не враг

У белых и черных хакеров совершенно разная мотивация. Белые хакеры — это популяризаторы, пассионарии, которым любопытно что-то найти; они этим живут. В эту профессию очень высокий порог входа, и люди просто так тут не задерживаются. Поэтому если вы видите белого хакера, который давно на рынке, то это человек, который предан своему делу.

У белого хакера в мотивации чаще всего интерес к победе. У черного — просто деньги, которые могут быть добыты самым простым способом. Поэтому квалификация белых хакеров выше, ведь у них в голове больше вариантов и сильнее набита рука.

Как белые хакеры взламывают системы

Самый простой способ — искать ошибки, допущенные из-за человеческого фактора. Можно взломать банковского оператора, его компьютер или доступ в удаленный бэк-офис, можно взломать компьютер оператора телефонной связи и получить доступ ко всем телефонам или выпустить себе дубль сим-карты.

А если взять дистанционное банковское обслуживание, то это достаточно монструозная система. Нужно препарировать ее по слоям, найти способ ее сломать, сшив разные недостатки в общий сценарий. Попытка связать это воедино длится дни и недели. Если это проектная работа, срок варьируется от двух недель до полутора-двух месяцев.

На киберучениях ограничений по времени нет: ты говоришь всем командам, что можно пробовать сломать систему в любое время в течение полугода. В этом случае бизнес подвергается испытаниям разных умов, что очень важно. Такой подход более эффективен и дает объективную картину того, какая защита выстроена в выбранной компании.

Какие затраты берет на себя хакер

Никто не будет взламывать систему, если вознаграждение едва превышает стоимость взлома. Нужно потратить трудочасы, возможно, купить за определенную сумму отдельные хакерские программы, эксплуатирующие уязвимости нулевого дня, неизвестные ранее.

Сделать так, чтобы стоимость взлома была для злоумышленников неприемлемой, чтобы им не хотелось тратить деньги на взлом, — это базовая формула, на которую нужно опираться при выстраивании защиты.

Сложнее ли черному хакеру взломать бизнес после белого хакера

Определенно. Черные хакеры не изучают компанию, чтобы сломать систему, для них это сложно. Проще взять тысячу компаний и на всех попробовать что-то одно. Если компания позвала белого хакера, чтобы он сделал хотя бы минимальные вещи, возможность веерной атаки исключается.

Сколько зарабатывает белый хакер

Оклад в этой сфере 300–500 тысяч ₽, но люди больше зарабатывают побочными активностями. Можно вечером обучать кого-то кибербезопасности, искать уязвимости, участвовать в киберучениях со своей командой, ездить на турниры. Экспертиза растет очень быстро: изучаешь что-то за месяц, и у тебя уже совершенно другой уровень дохода и роль в проектах.

Как оценивается кибербезопасность в деньгах

Здесь вопрос в ключевом субъекте взлома. Представим себе компанию, у которой есть рекламный лендинг и CRM-система какого-нибудь большого поставщика. Здесь нечего ломать: процесс не будет стоить дорого, он не выглядит сложным или масштабным.

А теперь посмотрим на банковские процессы и архитектуру банка. Это финансовый контроль, огромное количество этапов работы с транзакциями и персональными данными — невероятно богатая и передовая инфраструктура. Конечно, взлом банковской системы будет стоить гораздо дороже.

Равны ли деньги, вложенные в безопасность, стоимости взлома

Давайте посчитаем экономику. Стоимость защиты — это совокупность средств, которые компания вкладывает в информационную безопасность (ИБ). Сюда входят зарплаты сотрудников, бюджет на закупку продуктов и лицензий, а также услуги третьих лиц — например, интеграторов.

Стоимость взлома строится аналогичным образом. Сюда также входят зарплаты специалистов и технологии, которые команда исследователей использует, чтобы оценить защищенность бизнеса. Зачастую у хакеров затраты в разы меньше — на этом сказываются размер команды и стоимость их вознаграждения: фонд оплаты труда никто не отменял. Также на цену влияют используемые технологии, которые разрабатывают самостоятельно или полулегально приобретают.

Отсюда следует логика, которая и позволяет найти экономическую эффективность защиты: чем более ты защищен, тем дороже для хакеров должен стоить взлом.

Бывают обратные ситуации: ты вкладываешь тонну денег, а компанию ломают за миллион. Значит, ты что-то делаешь не так.

Чему бизнес может научиться у хакеров

Важно понимать: стоимость взлома может быть копеечной, потому что злоумышленники атакуют тысячи компаний и для них это почти автоматический процесс. Можно вкладывать в безопасность десятки миллионов ежегодно, а тебя взломает какой-нибудь начинающий злоумышленник, который просто запустил два инструмента и пробил периметр. Киберучения показывают бизнесу, как быстро все может рассыпаться. Поэтому нужно себя проверять — это как прививка для бизнеса.

Получите грант и узнайте, можно ли вас взломать за 1 млн ₽

Павел Чернышев

**специалист
по кибербезопасности
Совкомбанка и участник
команды Dream Team**

Чем чревата атака на бизнес и какие ошибки допускают в сфере информационной безопасности

Как становятся белыми хакерами

Белый хакер предпочитает большим и быстрым деньгам стабильность. Он понимает, что нужно наращивать экспертизу, становиться известным и развивать личный бренд. По своим навыкам и умениям белый хакер выше, чем специалисты, которые строят ИТ: ему нужно не просто сломать систему, а быстро разобраться в том, как она была построена, проконтролировать закрытие уязвимостей, формализовать их, сделать техническую, рекомендательную и рисковую часть для бизнеса. Это оценивается очень высоко. Случайных людей здесь быть не может.

В чем отличие белых и черных хакеров

Черными хакерами движут негативные эмоции или деньги. Это люди, которые разочаровались в рабочих процессах и обиделись на весь мир, либо идейные активисты. Они находятся в тени и могут зарабатывать огромные деньги в составе группировок, но рано или поздно их все равно находят. Технологии поиска таких людей совершенствуются, существует и киберразведка, и киберконтрразведка.

Белый хакер — это человек, который соблюдает кодекс чести. Если он его нарушит, то попадет везде в черный список и загубит свою карьеру. Ради чего — ради ста тысяч украденных строк с данными?

Недопустимое событие как основа стратегии

Недопустимое событие – это конкретный риск, реализация которого приведет к измеримым финансовым и репутационным потерям. Для маркетплейса или другого игрока онлайн-торговли таким риском может быть остановка продаж, для банка — кража денег, для производственной компании — остановка оборудования на несколько дней. Такие события могут обойтись крупным компаниям в сотни миллионов рублей и более.После реального взлома в компании полностью пересматривается подход к информационной безопасности (ИБ), увольняют ответственных за это сотрудников — вплоть до генерального директора.

Такие риски можно минимизировать через проверку силами белых хакеров, которые используют аналогичные методы и инструменты, что и «черные» специалисты. Проблем в этом случае гораздо меньше: процесс контролируется третьей стороной, в случае найденной уязвимости, команда может вовремя ее исправить. Максимальный риск — сотрудника ИБ лишат премии.

Ключевые ошибки бизнеса в построении ИБ

Главная ошибка — не тестировать свою защищенность на реальной инфраструктуре или проводить такие исследования с большими ограничениями. Из-за этого компания не может понять, реально ли она защищена. И не тренирует своих ИБ-специалистов, кто должен такие атаки отражать.

Другая ошибка — использовать устаревшее или нелицензионное программное обеспечение (ПО), не соблюдать парольную политику. Уязвимостями в этой сфере чаще всего пользуются злоумышленники, чтобы проникнуть в инфраструктуру компании.

Еще одна ошибка — отсутствие защищенных резервных копий. Как бы ни работала ИБ, если у бизнеса нет резервных копий, в любой момент найдется брешь. Однажды сотрудник нажмет что-то не то, и бизнес остановится.

Как оценивается кибербезопасность в деньгах

Бесценна только репутация; все остальное имеет цену. Мы можем посчитать экономику взлома. На черном рынке реально найти стоимость каждой базы — мы берем эту цену, умножаем на количество потерянных данных при той или иной уязвимости и получаем финансовый эквивалент уязвимости.

При эксплуатации уязвимости мы не просто компрометируем сервер, этого мало. Нужно понять, что это за сервер и какие данные на нем хранятся. Если там содержится база данных клиентов с их персональными данными, считаем, сколько таких клиентов, умножаем на цену на черном рынке за штуку и получаем цену взлома.

Но это только начало — у нас еще есть цена ресурсов. Это стоимость сервера, потому что он сколько-то времени живет в интернете, его купили в какой-то конфигурации. Для серьезной задачи там может стоять лицензированное ПО, которое для корпораций стоит десятки миллионов. Для его восстановления потребуются время ИТ-специалистов, которые вместо решения актуальных задач потратят недели и месяцы на возобновление процессов, которые можно было защитить.

Можно провести разведку по открытым источникам, собрать информацию о компании и о том, что ее главный актив — это, например, какой-то сервер. Если понятно, что там есть база данных и установлены конкретные программы, значит, явно есть лицензии на это и обученные эксперты. Средняя цена этих экспертов на рынке тоже известна. Суммируешь все это — получается стоимость потери бизнеса.

Что может перенять бизнес у хакеров

Бизнес должен понять, какие существуют риски. Эта роль отчасти возлагается на генерального директора, а также отдельного специалиста, который занимается риск-менеджментом. Последний формирует сценарии угроз: что может произойти и к каким последствиям это приведет, взвешивает ситуацию и дает советы, на что необходимо потратить ресурсы.

По умолчанию черному хакеру платить нельзя, потому что нет гарантии, что он что-то вернет. Мало того: существует риск, что проблема глубже, чем просто компрометация одного сервера и шифрование какого-то одного сегмента. Если хакер что-то скомпрометировал, то он уже украл персональные данные и серверные учетные записи.

Их нужно менять и смотреть, есть ли пробития в других местах, остались ли резервные копии, можно ли восстановить данные или нет. Когда все это разложится по полочкам, тогда будет понятен план действий.

Получите грант и узнайте, можно ли вас взломать за 1 млн ₽