Брюс Шнайер

МЫСЛИТЬ КАК ХАКЕР

КАК СИЛЬНЫЕ ЛОМАЮТ
ОБЩИЕ ПРАВИЛА
И КАК ДАВАТЬ ИМ ОТПОР

ЦЕЛЬ: ВЗЛОМАТЬ МЫСЛИТЕЛЬНЫЙ ПРОЦЕСС

Мы привыкли считать хакеров компьютерными преступниками, взламывающими системы ради выгоды или хаоса. Но что, если хакерство — это нечто большее, чем атаки на серверы и утечки данных? Книга «Мыслить как хакер» приглашает читателя взглянуть на хакерство как на способ анализа систем и феномен, который определяет нашу реальность и пронизывает все сферы жизни — от финансовых рынков и политики до технологий и повседневных решений.

Автор исследует истоки хакерства и показывает, что в современном мире взлом — это не всегда незаконное действие, но почти всегда — инструмент власти. Корпорации и элиты используют лазейки в законах, обходят правила и манипулируют системами в своих интересах, оставаясь безнаказанными. Хакинг становится частью механизма работы общества, и, если его контролируют только привилегированные группы, это приводит к неравенству и несправедливости.

Но может ли хакинг служить во благо? Автор убежден, что да. При правильном подходе хакерское мышление полезно и обществу, и личности. Именно через поиск слабых мест и их исправление мы можем сохранить способность к независимому мышлению, а общество — стать устойчивее и эффективнее. Однако важно научиться различать «конструктивный» и «разрушительный» хакинг, чтобы использовать силу взлома для улучшения мира, а не его разрушения.

В эпоху искусственного интеллекта границы между хакингом и управлением становятся еще более размытыми. ИИ может сделать хакинг опаснее, чем когда-либо, но также может помочь защитить системы и предсказывать уязвимости. Эта книга — о будущем, в котором хакинг может стать инструментом создания или разрушения, и о том, как можно научиться контролировать эту силу.

ХАКЕРСКОЕ МЫШЛЕНИЕ

ВЗЛОМ — НЕ ВСЕГДА ПРЕСТУПЛЕНИЕ

Слово «хакерство» появилось в 1955 году, быстро войдя в обиход в зарождающейся компьютерной среде. Изначально оно описывало способ решения проблем, который требовал хороших знаний и стремления действовать нестандартно. Но уже к 1980-м годам термин «хакерство» чаще всего использовали для обозначения взлома систем безопасности компьютеров.

Одно дело — взломать машину и угнать ее. И совсем другое — придумать, как заставить электронику авто открыть дверь и запустить двигатель.

Несмотря на то что сегодня между словами «хакер» и «преступник» часто ставят знак равенства, это далеко не всегда верно. Мыслить как хакер — значит понимать, как работают системы, как они выходят из строя и как сделать их более надежными.

Взлом системы — далеко не всегда противозаконный акт.

Хакер находит изъяны в действующих правилах. Это своего рода «игра с системой», деятельность на границе мошенничества и инноваций.

ХАКЕРСТВО КАК СИСТЕМА

Любой компьютерный код содержит ошибки. Но в норме их цена не слишком высока: программное обеспечение все равно большую часть времени работает идеально. Однако некоторые ошибки создают так называемые «уязвимости», то есть дыры в безопасности, через которые злоумышленник может намеренно вызвать сбой в работе системы.

Взлом компьютерного кода похож на уклонение от налогов. В Налоговом кодексе также присутствуют неточные формулировки, непреднамеренные упущения, неоднозначность в интерпретации — только в контексте налогов их называют «лазейками». Если в совершенстве изучить систему, можно сэкономить большие деньги.

Иногда Налоговый кодекс меняют и уточняют, чтобы закрыть возможность злоупотреблений. Но это долгий и сложный процесс, которому противостоят лоббисты. Поэтому некоторые налоговые «лазейки» остаются неисправленными и со временем становятся частью обычного бизнеса.

Автор сравнивает хакерство с деятельностью вирусов COVID-19 и ВИЧ, которые внедряются в иммунную систему и меняют цели ее работы. Организм начинает разрушать сам себя, вплоть до полной гибели.

Например, известны случаи, когда американские компании уклоняются от налогов, передавая права интеллектуальной собственности дочерним компаниям за рубежом. «Дочки» зарабатывают деньги на том же продукте и затем выводят их в офшоры, не уплачивая часть налогов. Схемы «двойная ирландская лазейка» и «голландский сэндвич» применяют, например, Facebook, Pfizer и Coca-Cola.

НЕИЗБЕЖНОСТЬ ОШИБОК

В сложных технических системах действуют различные наборы правил, и в конечном счете ошибки неизбежны. Если взлом произошел, значит, система его допустила. Хакер, взломавший компьютерную систему, перехитрил ее разработчиков.

Если кто-то смог успешно обойти социальные нормы, значит, он перехитрил разработчиков общественной системы, сумел найти и использовать ошибки, связанные с историей развития общества, или нерегулируемые лакуны в нормах, в соответствии с которыми общество действует.

Отличное знание системы избавляет от необходимости играть по правилам, которым подчиняются все остальные.

Главное в хакерском мышлении — это гибкость. Наша когнитивная система живет по тем же законам, которые руководят эволюцией: старые системы перепрофилируются, ненужные системы атрофируются. Это постоянное развитие происходит под влиянием среды, а не по воле некоего разработчика. Хакером буквально может стать каждый из нас.

Когда в некоторых американских школах ввели запрет на пользование мессенджерами, ученики стали общаться в общем файле Google Doc.

А бывший директор ЦРУ генерал Дэвид Петреус, которого обвинили в передаче секретной информации, пользовался тем же способом коммуникации, что и политический лоббист Трампа Пол Манафорт. Они делились с сообщниками учетной записью электронной почты и писали сообщения, сохраняя их как черновики без последующей отправки.

Чтобы мыслить как хакер, вы ищете упущения в правилах. Обнаруживаете, где перестают работать ограничения, которые система накладывает на вас. Вы начинаете естественным образом взламывать систему.

КОМУ ВЫГОДНО

Взлом системы состоит из двух элементов: уязвимости и эксплойта, то есть использования. Пользоваться обнаруженной уязвимостью могут как киберпреступники, так и вполне респектабельные институты.

Когда в протоколе Microsoft была обнаружена уязвимость в системе связи клиент-сервер, позволяющая получить контроль над удаленным компьютером через отправку определенного пакета данных, этим воспользовалось Агентство национальной безопасности США (АНБ).

В технических системах взломы чаще всего исправляют сразу же после обнаружения. Обычно это можно сделать довольно быстро, хотя для крупных организаций внедрение во все уязвимые системы может представлять проблему.

В 2017 году в микропроцессорах Intel были обнаружены неполадки Spectre и Meltdown, возникшие в процессе оптимизации производительности. Они создавали угрозу безопасности и к тому же затрагивали не ПО, а аппаратное обеспечение. Устранить эти уязвимости программными средствами было очень сложно и до конца это сделать так и не удалось.

ЗАЩИТА ОТ ХАКЕРСТВА В ТЕХНИЧЕСКИХ СИСТЕМАХ

Автор выделяет четыре уровня защиты кибербезопасности:

1. Прогнозирование угроз на этапе проектирования.
2. Перепроектирование существующих систем для усложнения взлома.
3. Отработка реакции на угрозы — например, обучение сотрудников распознавать мошеннические письма или сознательная тренировка по распознаванию приемов когнитивных взломов.
4. Создание дополнительных систем безопасности, таких как двухфакторная идентификация или двойное подтверждение крупных переводов.

ПРЕДУПРЕЖДЕНИЕ ПОТЕНЦИАЛЬНЫХ ВЗЛОМОВ НА ЭТАПЕ ПРОЕКТИРОВАНИЯ

Принципы проектирования для минимизации уязвимостей:

- **Простота:** чем проще устроена система, тем меньше потенциальных точек для атак и ошибок. Сложные архитектуры могут содержать скрытые уязвимости, поэтому минимизация избыточности и упрощение процессов повышают безопасность.
- **Глубокая защита (Defense in Depth):** использование многоуровневых защитных мер, таких как многофакторная аутентификация, шифрование данных и контроль доступа, снижает вероятность компрометации системы. Даже если один из уровней защиты будет взломан, другие слои предотвратят полную компрометацию.
- **Разделение обязанностей и изоляция (Separation of Duties, SoD):** для предотвращения злоупотреблений и ошибок критически важные задачи распределяются между разными пользователями или системами. Например, один сотрудник не должен иметь права одновременно создавать и утверждать платежи. Также важно ограничивать доступы к различным частям системы друг от друга, чтобы компрометация одной не приводила к взлому всей системы.
- **Минимальные привилегии (Principle of Least Privilege, PoLP):** пользователи и системы должны получать только тот уровень доступа, который необходим для выполнения их задач. Это снижает вероятность утечки информации, несанкционированного доступа и минимизирует потенциальный ущерб в случае компрометации учетной записи.

- **Отказоустойчивость (Fail-Safe Mechanisms):** система должна быть способна безопасно отключаться или переходить в защищенное состояние в случае ошибки, сбоя или атаки. Это позволяет минимизировать риски повреждения данных, потери контроля и дальнейшего распространения угроз.

МОДЕЛИ УГРОЗ И УСТОЙЧИВОСТЬ ЗАЩИТЫ

Технические системы становятся небезопасными, когда изменяется модель угроз. Для поддержания безопасности в динамично меняющемся мире важно опережать хакеров, отслеживать изменения угроз и проводить исследования для разработки лучших методов защиты. Законодательство также должно быть гибким и адаптироваться к новым угрозам. Так, в области компьютерной безопасности в 1986 году был разработан закон о компьютерном мошенничестве и злоупотреблениях.

Моделирование угроз — важный аспект системного проектирования, который позволяет прогнозировать риски и предотвращать их. При моделировании угроз учитывают стоимость защиты, эффективность мер безопасности и возможные последствия взломов.

В процессе разработки нередко применяют метод Red-teaming — поиск уязвимостей через моделирование атак, который помогает устранить слабые места до того, как их обнаружат настоящие хакеры.

Недостаточно тщательное проектирование угроз способно нанести существенный урон.

Устойчивость системы, то есть ее способность адаптироваться и восстанавливаться после разрушений, включает такие аспекты, как избыточность и гибкость, которые помогают системе сопротивляться атакам.

ХАКИНГ ВЕЗДЕСУЩИЙ

Сложно назвать сферу, в которой не было бы зафиксировано успешных взломов системы. Хакеры всегда оказываются на шаг впереди: сначала происходит взлом, и лишь когда жертва обнаружит ущерб, она может попробовать защититься на будущее. Это касается и финансовой, и технической, и социальной сферы.

Но если в технической сфере распознание взломов и борьба с ними довольно логичны, там, где дело касается законов или общественных норм, борьба с хакерством сильно осложняется. Те, кто с выгодой для себя использует лазейки, могут активно противодействовать их устранению. Причем выгоды могут быть не только финансовыми, но и моральными, этическими или политическими.

ХАКЕРСТВО В КАЗИНО

Попытки игроков обмануть казино имеют длинную историю. Еще в 1950-х годах появилась идея предсказывать результаты рулетки, основываясь на вычислениях скорости вращения колеса и шарика. В 1960-х годах был разработан персональный компьютер, который помогал игрокам вычислять вероятные числа для выигрыша.

24 ноября 1971 года Дэн Купер угнал Boeing 727 авиакомпании Northwest Orient Airlines. Получив $200 000 выкупа и четыре парашюта, он приказал экипажу снова взлететь. Затем он открыл кормовую лестницу и выпрыгнул с парашютом где-то над Тихоокеанским Северо-Западом. Купера так и не нашли. После этого инцидента дизайн Boeing изменили, добавив предохранитель для открытия хвостовых лестниц. Это устройство названо в честь угонщика — Cooper Vane. Функция AutoRun, представленная в Windows 95, изначально предназначалась для упрощения установки программ, но стала уязвимостью, приведшей к распространению вирусов через CD и USB-устройства. В 2011 году Microsoft отключила AutoRun для флеш-накопителей и сетевых дисков, оставив его только для устаревших носителей.

Однако в 1985 году использование таких устройств запретили, и казино начали менять правила игры, чтобы предотвратить прогнозирование результатов.

В настоящее время законным методом хакнуть казино остается только подсчет карт. В 1980-х годах ученые даже разработали командную стратегию, позволяющую группе игроков более эффективно считать карты и избегать обнаружения.

Казино борются с этим, стараясь максимально усложнить подсчет: используют автоматические тасовщики карт, учащают перетасовку, а в крайнем случае могут отстранить от игры тех клиентов, которых подозревают в попытке взлома системы.

ВЗЛОМЫ КЛИЕНТСКИХ ПРОГРАММ АВИАКОМПАНИЙ

В 1999 году американский инженер Дэвид Филлипс нашел уязвимость в системе лояльности авиакомпании American Airlines. Он потратил $3 150, чтобы купить 12 150 стаканчиков пудинга по 25 центов каждый. Затем с помощью друзей и семьи срезал со всех упаковок UPC-коды, сами десерты передал в Армию спасения, что обеспечило ему налоговый вычет. А в награду за покупку получил 1,2 миллиона бонусных миль, что обеспечило ему пожизненный «золотой» статус в программе лояльности авиакомпании. Когда организаторы — авиакомпания и производитель пудинга — поняли, что произошло, было уже поздно. Филлипс действовал строго по правилам, и аннулировать его мили было нельзя. Он с семьей еще много лет совершенно бесплатно путешествовал по всему миру самолетами American Airlines.

Среди других способов «взлома» программ лояльности авиакомпаний — манипуляции с накоплением миль через маршруты с большим количеством остановок, а также использование кредитных карт для накопления бонусных миль.

Авиакомпании стараются сделать свои программы менее уязвимыми, вводя минимальные требования по расходам и изменяя правила начисления миль так, чтобы клиенты получали бонусы в обмен на реально потраченные деньги. Но схем взлома по-прежнему остается немало.

ХАКЕРСТВО В СПОРТЕ

В спорте игроки часто находят способы обойти правила ради получения преимуществ, и порой такие приемы даже приводят к изменению правил игры.

Некоторые хакерские приемы в спорте — это, по сути, инновационные методы, которые в итоге становятся частью игры. Так произошло в крикете, когда игроки начали использовать перевернутый удар через голову. Сначала этот прием считался спорным, но позже был официально признан и включен в стандартные техники. Благодаря этому крикет эволюционировал, игра стала еще динамичнее и интереснее.

Например, во время баскетбольного матча финала НБА 1976 года игрок «Финикс Санз» Пол Вестфаль намеренно запросил незаконный тайм-аут для своей команды. Это привело к назначению штрафного, после которого команда смогла овладеть мячом, сравнять счет и перевести игру в дополнительное время. Тот матч «Финикс Санз» все равно проиграли, но уловка Вестфаля стала одним из самых известных случаев использования спортивных правил в свою пользу.

ВЗЛОМЫ БАНКОМАТОВ

В 2011 году австралийский бармен Дэн Сондерс случайно обнаружил уязвимость в системе банковских переводов, связанную с ночными операци-

ями банкоматов. Он заметил, что, если в определенное время ночью (обычно между 1 и 3 часами ночи) снять деньги с дебетовой карты, а затем быстро перевести средства между своими счетами, система не фиксировала транзакцию мгновенно. Это означало, что фактический баланс на счетах обновлялся не сразу и можно было снимать больше денег, чем было у него в реальности. Сондерс начал с небольших сумм, но потом увлекся. Банк начал расследование далеко не сразу. Но через несколько месяцев поистине роскошной жизни Сондерс понял, что расплата неминуема, и сам сдался властям. К тому времени он потратил примерно $1,2 млн, и его посадили в тюрьму на 12 месяцев.

Это очень известный случай, но далеко не единственный. В ответ на подобные кражи банки стали улучшать систему безопасности — например, прерывать транзакции клиентов и запрашивать дополнительное личное подтверждение. Но, конечно, этого недостаточно, ведь преступники продолжают изобретать новые способы взлома банкоматов, используя как физические, так и программные методы.

Метод скимминга состоит в том, что преступники устанавливают устройства для считывания информации с карт и PIN-кодов, а затем используют украденные данные.

Метод джекпоттинга связан с установкой на банкомат вредоносного ПО через USB-порт и получением удаленного доступа. Захватив контроль над банкоматом, хакеры заставляют его выбрасывать деньги без необходимости использования карты и ввода PIN-кода.

Атаки такого рода были зафиксированы в разных странах и нанесли многомиллионные убытки.

ОБХОД БАНКОВСКОГО РЕГУЛИРОВАНИЯ

Еще в Средние века церковь торговала индульгенциями, что было своего рода взломом системы христианской этики, а купцы обходили запреты на взимание процентов с помощью конструкций вроде «сухого морского займа», который формально превращал заем в инвестицию, связав его с морскими путешествиями. Такие механизмы в итоге стали основой современного банковского дела.

Финансовые учреждения часто находят способы обойти ограничения, созданные для обеспечения стабильности банковской системы.

Со временем некоторые финансовые манипуляции становятся легализованными практиками и создают постоянные риски для стабильности экономики. Но поскольку эти лазейки позволяют заработать, для них всегда находятся защитники.

Так, в 1933 году в США было введено Положение Q, ограничивающее процентные ставки по вкладам для снижения банковских рисков. Однако к 1970-м годам банки начали использовать схемы, позволяющие формально оставаться в рамках закона, но фактически обходить запреты. Одним из таких инструментов стали счета NOW, позволяющие начислять проценты на депозиты.

ВЗЛОМ ФИНАНСОВЫХ БИРЖ

Финансовые рынки подвержены различным видам атак, когда злоумышленники используют инсайдерскую информацию, ложные данные или манипулятивные схемы для получения прибыли. Основные методы таких взломов:

- **инсайдерская торговля** — использование закрытой (непубличной) информации для совершения прибыльных сделок. Это подрывает принципы честной конкуренции и справедливости на рынке;

- **опережение (Front-running)** — ситуация, когда брокеры или трейдеры, обладая информацией о готовящихся крупных сделках, совершают собственные сделки заранее, извлекая выгоду до того, как рынок отреагирует на официальную транзакцию;
- **дезинформация** — распространение ложных сведений для манипуляции рыночными ценами. Например, преступники скупают дешевые акции, затем создают искусственный ажиотаж с помощью фейковых заявлений, поднимая цену, а после продают активы с прибылью;
- **спуфинг (Spoofing)** — размещение крупных заявок на покупку или продажу, которые затем мгновенно отменяются. Это создает ложное впечатление о спросе или предложении, вынуждая других участников рынка реагировать определенным образом;
- **фейковые новости** — фабрикация и распространение поддельных новостей для искусственного изменения цен активов с последующей спекуляцией на этих изменениях.

Все эти методы подрывают доверие к финансовым рынкам и могут приводить к серьезным экономическим последствиям, включая кризисы и обвалы цен.

ВЫСОКОЧАСТОТНЫЙ ТРЕЙДИНГ КАК ВЗЛОМ БИРЖЕВОЙ СИСТЕМЫ

С развитием компьютерных технологий на финансовых рынках появились новые формы манипуляций, одной из которых стала высокочастотная торговля (HFT — High-Frequency Trading). Она основана на использовании сложных алгоритмов, совершающих сделки в доли секунды, что позволяет извлекать прибыль из малейших ценовых колебаний.

HFT-трейдеры получают преимущество перед другими участниками, нарушая принцип равного доступа к рыночной информации. Кроме того, высокочастотная торговля может усиливать волатильность и приводить к резким рыночным обвалам, как это произошло во время «мгновенного краха» (Flash Crash) 2010 года, когда индекс Dow Jones за считаные минуты потерял почти 1000 пунктов.

Также HFT ставит в невыгодное положение традиционных инвесторов, провоцирует панические распродажи или сознательные манипуляции рынком. Тем не менее регуляторы не вводят жестких ограничений, позволяя HFT оставаться важной, хотя и спорной, частью современной финансовой системы.

ОТМЫВАНИЕ ДЕНЕГ НА РЫНКЕ ЭЛИТНОЙ НЕДВИЖИМОСТИ

Рынок элитной недвижимости давно стал одним из ключевых инструментов отмывания денег. Схема работает так: сначала покупатели приобретают дорогостоящую недвижимость через подставные компании или офшорные структуры. Затем эта недвижимость может использоваться в качестве залога для получения легальных кредитов, позволяя легализовать незаконные средства.

Такие схемы позволяют обходить жесткие требования финансовых учреждений, созданные для борьбы с финансовыми преступлениями. Кроме того,

активное использование элитной недвижимости в качестве инструмента для отмывания денег приводит к росту цен на жилье, ограничивая доступ к рынку для добросовестных покупателей.

ХАКЕРСТВО КОРПОРАЦИЙ

Не только преступники, но и вполне легальные крупные корпорации находят способы манипулировать рыночными механизмами в своих интересах — создавая монополии, скрывая информацию и ограничивая выбор потребителей. Они используют сложные финансовые инструменты и контролируют поставки, чтобы искусственно повышать цены и снижать конкуренцию.

Один из примеров — манипуляции Goldman Sachs с рынком алюминия в 2010–2014 годах. Банк регулярно перемещал крупные партии металла между складами, создавая искусственные задержки в поставках. Это влияло на спотовые цены на алюминий и позволяло извлекать дополнительную прибыль за счет рыночных искажений.

Чем крупнее корпорация, тем большие угрозы для рыночной экономики она способна создать. Гиганты рискуют по-крупному, зная, что государство не допустит их банкротства.

Этот принцип стал очевидным после финансового кризиса 2008 года, когда власти США выделили $700 млрд на спасение крупнейших банков. Вместо того чтобы нести ответственность за свои действия, финансовые институты переложили убытки на налогоплательщиков.

Крупные финансовые игроки часто нарушают или обходят законы, используя свое влияние и ресурсы для легализации сомнительных схем.

Единственный способ бороться с этим — предотвращение чрезмерной концентрации экономической власти, чтобы не допускать появления слишком крупных компаний, которые можно обанкротить.

Логика рыночной экономики требует минимального вмешательства в финансовые рынки, но дерегулирование создает новые возможности для манипуляций и увеличивает риски. В условиях глобальной экономики и мощных технологий последствия таких «взломов» становятся масштабными, что требует более строгого контроля со стороны регулирующих органов.

ВЕНЧУРНОЕ ИНВЕСТИРОВАНИЕ КАК ВЗЛОМ ЭКОНОМИКИ

Многие венчурные компании годами работают, несмотря на огромные убытки. Они искусственно занижают цены, предлагая низкие тарифы и вытесняя конкурентов, которые не могут позволить себе такие расходы. Однако эта стратегия не делает бизнес устойчивым: если финансирование прекратится, цены неизбежно вырастут. Вместо честной конкуренции рынок оказывается под контролем крупных инвесторов, которые временно поддерживают убыточные компании в надежде на будущую монополию.

Компании по доставке еды, такие как DoorDash и Uber Eats, существуют не за счет прибыли, а благодаря многомиллиардным инвестициям венчурных фондов.

Кроме того, венчурные фонды предпочитают краткосрочную прибыль и не вкладывают деньги в инновации и потенциально жизнеспособные бизнес-модели, подрывая устойчивость экономики.

В 2016 году власти США запустили пилотную программу, требующую раскрытия бенефициарных владельцев при покупке недвижимости через подставные компании. В результате резко сократилось количество наличных сделок с элитной недвижимостью. Однако лоббизм и политическая инертность продолжают тормозить более глубокие реформы, позволяя схемам отмывания денег существовать и по сей день.

Так, в 2009 году General Motors объявила о банкротстве, в результате чего рядовые акционеры потеряли все вложения. Однако руководство и крупные инвесторы извлекли прибыль, создав и продав новые акции для привлечения капитала. Этот случай наглядно демонстрирует, как богатые используют финансовые инструменты для защиты собственных интересов, оставляя мелких инвесторов без средств.

ХАКЕРСТВО В ПРАВОВОЙ СФЕРЕ

Законы создаются для регулирования жизни общества, но иногда они содержат пробелы, которыми компании и отдельные люди пользуются для собственной выгоды. Обход законов без формального их нарушения называют юридическим хакингом.

Крупные компании особенно часто занимаются юридическим хакингом, используя тесные связи с регуляторами. Они манипулируют государственным контролем в своих целях и вредят другим участникам рынка и обществу.

Когда регулирующие органы ослабили контроль за безопасностью самолетов и доверили проверки самой компании Boeing, опасные дефекты Boeing 737 MAX остались незамеченными, что привело к авиакатастрофам.

Uber регистрируется как технологическая платформа, а не транспортная компания, что позволяет не платить налоги, не оформлять водителей как сотрудников и избегать регулирования. Это дает Uber преимущество перед традиционными такси, которые обязаны соблюдать правила.

В 2016 году республиканское большинство в Сенате США заблокировало рассмотрение кандидата от демократов на пост судьи Верховного суда. В ожидании прихода Трампа место держали вакантным для другого кандидата на протяжении 10 месяцев, что в принципе законно, но противоречит духу демократии.

Во многих странах мира постоянно ужесточаются требования к проведению забастовок и массовых акций. Право на протест защищено законом, но новые правила постепенно сокращают эту свободу.

Законодательные процедуры также можно «взломать», чтобы добиться результата без нарушения правил.

Иногда нежелательные нормы прячут внутри крупных законов, чтобы их сложнее было заметить и оспорить.

В США к важным законопроектам часто прикрепляют выгодные лоббистам дополнительные пункты, зная, что закон будет принят «в целом», а президент не может наложить вето на его отдельные части.

Нередко государственные органы создают искусственные сложности, чтобы людям было сложнее получать пособия и социальную помощь: усложняют систему подачи заявлений, требуют множество документов, увеличивают время рассмотрения. Это заставляет многих отказываться от своих законных прав, экономя государству деньги.

ХАКИНГ КАК ИНСТРУМЕНТ ПРОГРЕССА В ПРАВОВОЙ СИСТЕМЕ

Сложные системы развиваются через итеративные изменения, и в правовой системе новые прецеденты иногда позитивно влияют на нормы закона.

Случай памфлетиста и издателя Джона Энтика (1762) стал важным прецедентом в защите частной собственности и гражданских свобод. Британские власти без четкого судебного основания ворвались в его дом, изъяли бумаги и разрушили имущество, ссылаясь на общий ордер. Энтик оспорил это в суде, и суд признал действия властей незаконными, постановив, что государство не может произвольно вмешиваться в частную жизнь граждан. Это решение укрепило принцип неприкосновенности собственности, стало основой для будущих законов против незаконных обысков и повлияло на Четвертую поправку Конституции США.

Важно общественное внимание к необходимым изменениям в правовом поле. Защита от злоупотреблений — это не только техническая, но и моральная и практическая задача, требующая координации и гибкости в управлении законодательными органами и регулирующими властями.

Автор уверен, что для предотвращения юридического хакинга нужно улучшать прозрачность законодательного процесса и предоставить больше времени для анализа законопроектов.

ХАКЕРСТВО В ПОЛИТИЧЕСКОЙ СИСТЕМЕ

Манипуляции с избирательным процессом, которые подрывают демократические принципы, не всегда происходят грубо и прямолинейно. Иногда изменяют лишь часть правил, например ограничивают права определенных групп населения.

В 1901 году в Алабаме ввели требования к голосующим гражданам: они должны были пройти тест на грамотность, заплатить избирательный налог и выполнить еще несколько правил. Несмотря на то что меры выглядели невинно, они фактически отсекли от выборов большинство чернокожего населения.

Среди других способов избирательного хакинга автор выделяет:

- **организационный подрыв голосования:** создание сложностей для избирателей, что заставляет их отказаться от голосования (несвоевременное закрытие избирательных участков, отказ от регистрации избирателей в день выборов, нестандартные требования к удостоверениям личности и т. д.);
- **джерримендеринг** — изменение границ избирательных округов с целью усиления контроля за результатами выборов (релевантно для США, где голосование проходит не напрямую, а через институт выборщиков);
- **злоупотребление властью:** политики могут использовать свое влияние для манипуляций с датами выборов, регистрацией голосующих, подсчетом голосов или исключением кандидатов, чтобы достичь выгодных для себя результатов.

РОЛЬ ДЕНЕГ В АМЕРИКАНСКОЙ ПОЛИТИКЕ

Финансовые ресурсы играют ключевую роль в американской политике. Хотя в теории независимые кандидаты способны разрушить монополию партий, на практике они редко добиваются успеха. Политическая система устроена так, что кандидаты без крупных финансовых вливаний почти не имеют шансов на победу.

Избирательные кампании в США — одни из самых дорогих и длительных в мире. Они могут длиться более года, что требует огромных затрат на рекламу, организацию мероприятий и работу штабов. Это делает участие в выборах доступным только для кандидатов с мощной финансовой поддержкой.

В 2010 году Верховный суд США ослабил ограничения на финансирование избирательных кампаний, разрешив корпорациям и частным лицам вкладывать в политику неограниченные суммы. В результате богатые доноры получили еще более широкие возможности влияния, обеспечивая политикам победу в обмен на лояльность.

Внутрипартийная конкуренция на предварительных выборах еще сильнее увеличивает затраты, так как политикам приходится привлекать дополнительные средства для борьбы с соперниками.

Существует мнение, что исправить ситуацию может система рейтингового голосования, которая позволит избирателям ранжировать кандидатов по предпочтению и предотвратит ситуации победы кандидата, набравшего меньше половины голосов.

ХАКИНГ КОГНИТИВНЫХ СИСТЕМ

Когнитивный хакинг — это способ манипуляции восприятием людей, который используется в рекламе, политике, социальной инженерии и даже в законодательстве. С развитием технологий он становится сложнее и эффективнее, влияя на решения людей незаметно для них самих. Хотя полностью избежать такого влияния невозможно, осведомленность о методах манипуляции помогает лучше защищаться.

Когнитивный хакинг может проявляться на разных уровнях — от личных привычек до глобальных политических процессов, влияя на потребительское, экономическое и гражданское поведение людей.

ВНИМАНИЕ СТАНОВИТСЯ ТОВАРОМ

Цифровые платформы и рекламные кампании используют когнитивный хакинг, чтобы привлекать, удерживать и монетизировать внимание пользователей.

- Социальные сети подбирают контент так, чтобы пользователи оставались в ленте как можно дольше.
- В рекламе используют яркие цвета, всплывающие окна и звуки, которые привлекают внимание и заставляют кликнуть.
- Игры и приложения используют переменные вознаграждения (как в азартных играх), создавая привычку и зависимость.
- Сбор личных данных помогает рекламодателям показывать рекламу, от которой сложно отказаться, но при этом ставит под угрозу конфиденциальность пользователей.

МАНИПУЛЯЦИЯ УБЕЖДЕНИЯМИ И ЗЛОУПОТРЕБЛЕНИЕ ДОВЕРИЕМ

Некоторые методы когнитивного хакинга заставляют людей принимать невыгодные решения или верить ложной информации.

- **Капельное ценообразование:** покупателю показывают низкую цену, но на финальном этапе добавляют скрытые сборы.
- **«Темные шаблоны»** (dark patterns) в интерфейсах: дизайн кнопок и меню сбивает пользователей с толку (например, в сервисах подписок сложно найти кнопку отмены, на всплывающем окне — кнопку закрытия, а таймер обратного отсчета создает ложное чувство срочности покупки).
- **Социальная инженерия:** мошенники используют психологические приемы и поддельные сайты, чтобы обманом заставить жертву передать пароли и личные данные.

В 2016 году советник Хиллари Клинтон Джон Подеста ввел свои учетные данные на фальшивой странице Google, созданной российскими хакерами. Это открыло им доступ к электронной почте Подесты, что повлияло на предвыборную кампанию.

СТРАХ КАК ИНСТРУМЕНТ ВЛИЯНИЯ

Люди сильнее реагируют на эмоциональные истории, чем на сухие данные. Это делает страх мощным инструментом манипуляции. Запуганные люди хуже анализируют информацию и склонны сбиваться в группы, что ведет к конфликтам и поляризации общества.

Политики и СМИ могут использовать яркие пугающие образы и тенденциозный сторителлинг, чтобы повысить общий уровень стресса и убедить людей поддержать определенные законы или программы.

КАК ЗАЩИТИТЬСЯ ОТ КОГНИТИВНОГО ХАКИНГА

Хотя осознание манипуляций не всегда помогает избежать их влияния, существуют способы защиты. Узнавая больше о техниках манипулирования, люди повышают шансы на сохранение независимого мышления.

Полезно использовать технические инструменты, такие как блокировщики рекламы, контроль конфиденциальности и настройка уведомлений. А на законодательном уровне — добиваться честной игры: например, обязать продавцов сразу раскрывать полную цену товаров, чтобы предотвратить скрытые платежи.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ХАКИНГ

Искусственный интеллект (ИИ) сегодня становится хакерским инструментом для вмешательства в ключевые сферы общества.

Автор уверен, что ИИ уже сегодня способен манипулировать поведением людей и подрывать социальные и экономические системы. В перспективе он будет самостоятельно находить уязвимости в алгоритмах, взламывая другие системы. Уже сегодня ИИ умеет лучше человека находить и использовать уязвимости, создавая новые угрозы.

На соревнованиях DARPA Cyber Grand Challenge в 2016 году система Mayhem смогла находить и устранять уязвимости быстрее экспертов по кибербезопасности.

ИИ, как и любая цифровая система, имеет уязвимости. Машинное обучение (МО) — одна из самых перспективных, но и наиболее уязвимых технологий. Состязательное машинное обучение позволяет хакерам создавать специальные данные, которые сбивают ИИ с толку.

Например, чат-бот Tay от Microsoft начал писать оскорбительные и расистские сообщения, потому что обучался на нефильтрованных пользовательских данных. Более тонкие манипуляции могут менять решения ИИ незаметно, что делает состязательные атаки особенно опасными.

ИИ уже широко используется для массовых манипуляций. Очеловечивание ИИ делает их все более убедительными: чат-боты имитируют настоящих людей, влияя на пользователей. ИИ в киберпреступности позволяет умным алгоритмам подделывать голоса, видео и тексты, создавая правдоподобные фальшивки, используемые в мошенничестве и кибератаках.

Во время выборов в США в 2016 году и в ходе голосования по Brexit политические боты опубликовали сотни тысяч твитов, формируя искусственное общественное мнение.

ИИ уже сегодня меняет финансовую систему. В будущем, обладая доступом ко всем налоговым и финансовым данным, он сможет находить законные лазейки быстрее, чем любой аналитик. Это может создать новый уровень цифрового хакинга, превосходящий возможности человека. Если ИИ останется неуправляемым, негативные последствия могут быть непредсказуемыми.

Но если ИИ может взламывать, значит, он может и защищать. Робототехника и машинное обучение уже изменили промышленность и здравоохранение, а дальше — больше. ИИ можно использовать для тестирования законов и налоговых систем, выявляя лазейки и пробелы до их принятия. В области безопасности ИИ способен анализировать сложные алгоритмы и находить уязвимости раньше хакеров.

Станет ИИ инструментом добра или зла, зависит от контроля со стороны человека. Этика и безопасность использования таких технологий выходят на первый план, ставя нас перед необходимостью создавать гибкие системы управления развитием ИИ.

ХАКЕРСКОЕ МЫШЛЕНИЕ: ВО БЛАГО ИЛИ ВО ЗЛО?

Современный хакинг — это не просто атаки на компьютерные сети, а феномен, который одновременно разрушает устоявшиеся системы и открывает новые возможности. В цифровую эпоху граница между взломом как угрозой и взломом как инновацией становится все более размытой.

С одной стороны, технологические прорывы — от облачных вычислений и искусственного интеллекта до вирусного распространения информации — сделали хакинг мощнее и доступнее, что привело к росту социальных и экономических манипуляций.

С другой стороны, хакинг может выступать инструментом демократизации, позволяя разрушать монополии, вскрывать коррупционные схемы и защищать цифровые права.

Сегодня, как и в давние времена, хакерством часто занимаются привилегированные группы, которые используют его для извлечения финансовых и политических выгод. И с развитием технологий все острее стоит вопрос: как создать механизмы, которые позволят различать «полезные» и «разрушительные» взломы и при этом не будут препятствовать прогрессу?

Необходимы гибкие регулирующие структуры, способные быстро адаптироваться к новым вызовам и находить баланс между безопасностью и свободой. Если подходы к управлению хакингом не будут достаточно совершенными, мы рискуем столкнуться с волной цифрового хаоса, где технологии будут работать не на благо общества, а против него.

---

10 ЛУЧШИХ МЫСЛЕЙ

1.

Мыслить как хакер — значит понимать, как работают системы, как они выходят из строя и как сделать их более надежными.

2.

Если взлом произошел, это означает, что система позволила ему произойти.

3.
Тем, кто понимает правила работы системы, становится не обязательно их соблюдать.

4.
Хакеры всегда оказываются на шаг впереди: сначала происходит взлом, и только после обнаружения ущерба жертва разрабатывает защиту.

5.
Хакеры могут действовать не только из финансовых, но и из политических и этических побуждений.

6.
В технических системах ошибки обычно устраняют сразу после обнаружения. Ошибки в экономике и социальной сфере часто сохраняются очень долго, потому что их защищают лоббисты.

7.
Усилия по обеспечению кибербезопасности охватывают полный жизненный цикл технической системы: проектирование, эксплуатацию и возможности расширения системы.

8.
Системы становятся особенно уязвимыми при изменении вида угроз.

9.
Крупные организации создают максимальные риски для экономики, потому что государство защищает их от банкротства.

10.
Искусственный интеллект (ИИ) можно использовать не только для взломов, но и для защиты технических и социальных систем.