

12+

Роман Бондарь

Цифровой рэкет

КАК ПРОДАЕТСЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



Роман Бондарь

Цифровой рэкет.

Как продаётся

безопасность в интернете

<https://litres.ru/74148193>

ISBN 9785006996991

Аннотация

Это не книга про безопасность. И не про маркетинг. Это книга про то, как страх стал продуктом, а уязвимость — валютой. Про рынок, где бизнес платит не за результат, а за ощущение контроля.

«Цифровой рэкет» — это разбор модели, в которой угрозы перестали быть явными, но стали тотальными. Они больше не ломают двери — они отключают процессы. Не требуют денег напрямую — они формируют зависимость. Вы не видите давления, но принимаете решения так, как будто оно есть.

Содержание

Об авторе	5
Дисклеймер	8
Введение	10
Ключевые признаки цифрового рэкета	18
Часть I. Когда страх был прямым	21
Глава 1. Рэкет как примитивная, но честная модель рынка страха	21
Глава 2. Почему бизнес соглашался платить	25
Глава 3. Механика «крыши»: контроль, зависимость, невозможность выхода	29
Часть II. Переезд бизнеса в цифру	33
Глава 4. От палаточного ларька к цифровому активу	33
Глава 5. Новая уязвимость: бизнес не понимает, как устроена его собственная цифровая среда	37
Конец ознакомительного фрагмента.	39

Цифровой рэкет. Как продаётся безопасность в интернете

Роман Бондарь

© Роман Бондарь, 2026

ISBN 978-5-0069-9699-1

Создано в интеллектуальной издательской системе Ridero

Цифровой рэкет. Как продаётся безопасность в интернете.

Автор: Роман Бондарь.

г. Иваново, 2026 год.

О книге

Жанр: аналитический нон-фикшн.

Формат: концептуально-аналитический разбор с описанием практического опыта.

Об авторе

Роман Бондарь — исследователь цифровой среды, автор книг о скрытой логике интернет-индустрий и человек, который слишком долго находился внутри системы, чтобы воспринимать её объяснения без критики.

Более 15 лет он работает на пересечении интернет-маркетинга, поисковых технологий и анализа цифровых систем. Его профессиональный путь — это не просто практика внедрения инструментов, а последовательное изучение того, как формируются алгоритмы, как создаётся влияние и каким образом в цифровой среде возникает зависимость.

В разные годы он занимался поисковой оптимизацией, стратегическим развитием интернет-проектов и аналитикой поисковых систем, возглавлял SEO-направление в IMarketing и наблюдал индустрию изнутри — в тот момент, когда она ещё сохраняла видимость измеримого результата.

Параллельно в своей работе он регулярно сталкивается с вопросами информационной безопасности и архитектуры приложений (AppSec). Это позволило ему рассматривать цифровую среду не только как маркетинговую экосистему, но и как инфраструктуру контроля, уязвимостей, интерпретаций и зависимости.

В своих исследованиях автор принципиально не разделяет маркетинг, технологии и безопасность. Потому что в ре-

альности они давно работают как единая система.

Новая книга «Цифровой рэкет» продолжает эту линию и расширяет её: от анализа иллюзий — к разбору самой экономики страха, зависимости и интерпретации, которая формирует современные цифровые рынки.

Роман Бондарь — автор книг:

— «Пиратские войны» — о реальной структуре теневых цифровых рынков и механике их возникновения

— «Трудно быть хакером» — о трансформации цифровой свободы и появлении ответной системы контроля

— «Поиск без результата» — о моменте, когда SEO перестала иметь проверяемый результат и превратилась в бесконечный процесс

— «Цифровой актив. Когда бизнес отказался от суверенитета» — о подмене собственности доступом и добровольной передаче контроля в экосистемы

— «Никто не помнит экспертов» — о кризисе экспертизы и иллюзии влияния в эпоху личных брендов

— «Цифровой рэкет. Как продаётся безопасность в интернете» — о том, как страх, сложность и интерпретация превращаются в устойчивую модель рынка

Все его книги объединяет одна линия: разбор иллюзий, на которых держится современный интернет.

— иллюзия результата

— иллюзия влияния

— иллюзия безопасности

- иллюзия собственности
- иллюзия экспертизы
- иллюзия контроля

Автор не пишет «про технологии» в привычном смысле. Он пишет про поведение системы и человека внутри неё. Его тексты — это не инструкции и не попытка чему-то научить. Это попытка зафиксировать момент, в котором привычные объяснения перестают работать, но продолжают использоваться по инерции. Он не стремится быть удобным для индустрии. Потому что удобство — это то, на чём она зарабатывает. Его задача — описывать реальность так, как она проявляется на практике. Даже если это делает её менее комфортной для восприятия.

Дисклеймер

Эта книга посвящена анализу рыночной логики, а не обвинению конкретных людей, компаний или отраслей. Все приведённые в ней примеры, кейсы и сценарии являются собирательными и отражают типовые ситуации, которые могут встречаться в цифровой экономике. Любые совпадения с реальными компаниями или событиями случайны.

Автор не ставит под сомнение необходимость информационной безопасности, технической поддержки, маркетинга, консалтинга и других профессиональных услуг. Напротив, книга исходит из того, что эти функции объективно важны для устойчивости бизнеса. Критическому рассмотрению подвергаются не сами услуги, а отдельные модели их представления, продажи и интерпретации в условиях информационной асимметрии и высокой сложности цифровой среды.

Материалы книги не являются юридической, финансовой или технической рекомендацией. Все решения, связанные с выбором подрядчиков, построением инфраструктуры и обеспечением безопасности, должны приниматься с учётом конкретных условий бизнеса и, при необходимости, с привлечением профильных специалистов.

Цель книги — не сформировать недоверие к рынку, а развить способность к осознанной оценке. Показать, как в слож-

ной среде переплетаются реальные риски и способы их интерпретации, и на что стоит обращать внимание, чтобы сохранять управляемость и принимать решения не только под влиянием тревоги, но и на основе понимания.

Автор признаёт, что рынок неоднороден. В нём присутствуют как добросовестные специалисты и компании, так и практики, которые могут усиливать зависимость клиента. Описанные механизмы не являются универсальными и не применимы ко всем участникам рынка без исключения.

Книга не призывает отказываться от услуг специалистов или игнорировать угрозы. Она призывает к другому — к сохранению позиции управления, к пониманию собственной инфраструктуры и к способности различать, где заканчивается объективная необходимость и начинается работа с восприятием риска.

Любое использование идей и подходов, изложенных в книге, осуществляется читателем самостоятельно и под его личную ответственность.

Введение

Почему эта книга вообще появилась

Эта книга не про 90-е. И уж точно не про ностальгию по ним. Тем не менее начать придётся именно оттуда — не потому, что прошлое требует внимания само по себе, а потому что в нём гораздо проще увидеть те механики, которые сегодня стали менее заметными, но не исчезли.

В девяностые всё было предельно прямолинейно. Если у тебя был бизнес, у тебя почти неизбежно появлялась проблема. И если у тебя была проблема, рано или поздно находились люди, которые предлагали её решить. Формула была простой и понятной: платишь — работаешь спокойно, не платишь — спокойствие заканчивается. Это называлось «крыша». Грубая, примитивная, иногда откровенно жестокая, но в каком-то смысле честная. Источник угрозы был очевиден, правила игры — тоже. Ты платил не за безопасность как таковую, а за предсказуемость. За возможность проснуться утром и знать, что сегодня ничего не произойдёт.

Сегодня всё выглядит иначе. У тебя больше нет ларька, который можно обойти вокруг и понять, где он начинается и где заканчивается. У тебя есть сайт, CRM, база клиентов, домен, облачные сервисы, рекламные кабинеты, платёжные системы, десятки интеграций и зависимостей. Твой бизнес больше не находится в одном месте — он распределён,

размазан по инфраструктуре, которую невозможно увидеть целиком. Вместе с этим изменилась и сама природа уязвимости. Теперь, чтобы остановить бизнес, не нужно выбивать дверь или разбивать витрину. Достаточно лишить доступа, нарушить процессы, повредить данные или просто создать условия, при которых всё это может произойти в любой момент.

Именно здесь возникает новая реальность, в которой страх становится не эпизодом, а постоянным фоном. Страх потерять доступ, страх утечки, страх сбоя, страх репутационных и финансовых последствий. И вместе с этим страхом формируется целый рынок — рынок безопасности. Рынок, в котором больше никто не говорит напрямую: «у тебя будут проблемы». Здесь используют другой язык. Более сложный, более убедительный, более рациональный на вид. Говорят об уязвимостях, о рисках, о поверхности атаки, о вероятности инцидента. И почти всегда за этим следует пауза — та самая пауза, в которой возникает предложение решения.

Долгое время меня не покидало ощущение, что за всем этим скрывается нечто знакомое. Не сами технологии и не необходимость защищаться от угроз — с этим как раз всё понятно. Речь о другом. О логике, которая неожиданно оказалась слишком похожей на ту, что уже существовала раньше, просто в иной форме. Логике, где сначала появляется неопределённость, затем её объясняют, затем усиливают тревогу, после чего предлагают контроль, и в итоге возникает

регулярный платёж за то, чтобы всё оставалось под этим контролем.

В какой-то момент стало очевидно: изменилась оболочка, но не всегда изменилась сама механика. И именно это наблюдение стало отправной точкой для этой книги.

Важно сразу обозначить границы. Эта книга не про то, что «все в IT плохие», и не про то, что безопасность — это иллюзия. Угрозы реальны. Уязвимости существуют независимо от того, говорим мы о них или нет. Атаки происходят, данные теряются, доступы перехватываются, и бизнес действительно может оказаться в ситуации, когда он лишается всего — от информации до репутации. Игнорировать это — значит сознательно идти к проблеме.

Но одновременно с этим существует и другая сторона. Любой рынок, который возникает вокруг угроз, рано или поздно начинает жить по собственным законам. И один из этих законов довольно прост: чем выше уровень тревоги, тем легче продаётся защита. Это не обязательно означает злой умысел. Чаще это означает, что сама структура рынка постепенно подталкивает участников к определённом поведению — к усилению значимости риска, к усложнению картины, к формированию зависимости клиента от тех, кто способен эту картину объяснить.

Современный бизнес в этом смысле оказался в положении, которое во многом напоминает ситуацию тридцатилетней давности. Он понимает, что у него есть риск, но не до

конца понимает его природу. Он осознаёт возможность потерь, но не знает, откуда именно может прийти удар. Он слышит экспертов, но не всегда способен проверить, где заканчивается объективная оценка и начинается интерпретация. И в этой точке возникает зависимость — не обязательно навязанная, не обязательно осознанная, но вполне системная.

Эта книга — не попытка обвинить и не попытка разоблачить конкретных людей или компании. Это попытка посмотреть на происходящее глубже — не через призму технологий, а через призму логики рынка. Логике, в которой страх, сложность и неопределённость становятся не только проблемой, но и ресурсом. Ресурсом, вокруг которого выстраиваются услуги, отношения и модели монетизации.

Я решил писать об этом не потому, что хочу спорить с отраслью, а потому что слишком часто видел одну и ту же ситуацию. Бизнес, который не понимает собственную инфраструктуру. Бизнес, который не владеет своими доступами. Бизнес, который не может до конца оценить, за что именно он платит. И в итоге — бизнес, который остаётся в единственной понятной для себя стратегии: продолжать платить, потому что альтернатива выглядит слишком неопределённой и, следовательно, слишком опасной.

Неудобство этой темы в том, что она проходит по границе. Между реальной безопасностью и продажей тревоги. Между необходимой защитой и формированием зависимости. Между экспертизой и той интерпретацией реальности, от которой

напрямую зависит решение клиента. Здесь нет чёрно-белых ответов и простых выводов. Есть только попытка разобраться в том, как именно устроена система, в которой мы все сегодня находимся.

И если в результате чтения этой книги изменится не список используемых инструментов, а сам способ мышления о безопасности — значит, она появилась не зря.

Но прежде чем начать говорить более предметно, давайте сначала определимся с терминологией, которая будет проходить через всю книгу, чтобы у читателя было четкое понимание о чем идет речь.

Рэкет — это форма организованного противоправного экономического принуждения, при которой субъект (лицо или группа лиц) систематически извлекает финансовую или иную выгоду из бизнеса или частного лица путём угроз, давления или создания риска ущерба, одновременно предлагая «защиту» от этих же или аналогичных угроз.

Ключевые признаки рэкета:

- наличие угрозы или давления (явного или подразумеваемого);
- регулярный характер платежей (а не разовая сделка);
- формирование зависимости жертвы от субъекта давления;
- предложение защиты от риска, который не обязательно полностью устраняется;
- асимметрия силы между сторонами;

— отсутствие добровольности в классическом рыночном смысле.

Важное уточнение:

Рэкет отличается от обычного вымогательства тем, что:

- носит системный и длительный характер;
- оформляется как псевдосервис (защита, покровительство);
- интегрируется в экономическую деятельность жертвы.

Рэкет в 1990-е годы — это специфическая форма неформального регулирования и контроля предпринимательской деятельности в условиях слабых государственных институтов, при которой организованные группы осуществляли систематическое экономическое принуждение бизнеса, взимая регулярные платежи в обмен на управляемость рисков, физическую безопасность и защиту от конкурирующих угроз.

Характерные особенности рэкета в 90-х:

1. Институциональная замещающая функция

Рэкет выполнял роль частичной замены неэффективных или отсутствующих государственных механизмов защиты собственности и контрактов.

2. Территориальность

Контроль осуществлялся по географическому принципу — «район», «рынок», «объект».

3. Системность и структурированность

Рэкет не был хаотичным — существовали:

- иерархии
- зоны влияния
- неформальные договорённости между группами

4. Регулярная экономическая модель

Платежи носили абонентский характер:

- фиксированные суммы
- процент от оборота
- периодичность (ежемесячно, еженедельно)

5. Связка «угроза — защита»

Субъекты, предлагающие защиту, часто:

- сами являлись источником угрозы
- либо контролировали её распространение

6. Ограниченная легитимность через практику

Несмотря на противоправный характер, рэкёт:

- воспринимался бизнесом как «рабочая реальность»
- становился частью хозяйственной деятельности

Цифровой рэкёт — это рыночная или квазирыночная модель извлечения экономической выгоды из уязвимости бизнеса в цифровой среде, при которой субъект (организация или специалист) формирует, усиливает или интерпретирует риски информационной, технической или инфраструктурной природы и предлагает услуги по их контролю или снижению, закрепляя зависимость клиента через регулярные платежи и информационную асимметрию.

Цифровой рэкёт не обязательно является противоправной деятельностью и может функционировать в рамках ле-

гального рынка услуг. Его отличительная особенность заключается не в наличии угроз как таковых, а в способе их экономической упаковки и использования в качестве механизма формирования спроса и долгосрочной зависимости.

Ключевые признаки цифрового рэкета

1. Наличие уязвимости как базового ресурса

Уязвимость может быть:

- реальной (технические дыры, слабая защита)
- потенциальной (возможные риски)
- интерпретируемой (усиленной через экспертную оцен-

ку)

2. Формирование или усиление восприятия угрозы

Риск:

- описывается
- структурируется
- масштабируется в сознании клиента

При этом:

- уровень угрозы может быть объективным
- но её восприятие часто усиливается через язык и по-

дачу

3. Предложение контроля вместо устранения неопределённости

Клиенту продаётся не абсолютная безопасность, а:

- мониторинг
- сопровождение
- реагирование

— соответствие стандартам

То есть управление риском, а не его исчезновение.

4. Регулярная экономическая модель

Платёж:

— носит абонентский характер

— связан с поддержанием состояния «под контролем»

— не всегда привязан к измеримому результату

5. Информационная асимметрия

Клиент:

— не способен полностью проверить качество услуги

— зависит от интерпретации специалиста

— принимает решения в условиях ограниченного пони-

мания

6. Формирование зависимости

Зависимость возникает через:

— контроль доступов

— сложность инфраструктуры

— отсутствие прозрачности

— отсутствие возможности быстрой замены исполнителя

Цифровой рэкет ≠ информационная безопасность.

Информационная безопасность — это объективно необходимая функция защиты данных и инфраструктуры.

Цифровой рэкет — это способ организации рынка вокруг этой функции, при котором страх и сложность могут использоваться как инструмент монетизации.

Получается, что «Цифровой рэкет» — это модель, в кото-

рой уязвимость превращается в продукт через страх, а страх — в источник регулярного дохода.

В рамках этой книги под «цифровым рэкетом» понимается не противоправная деятельность как таковая, а определённая рыночная логика, в которой уязвимость бизнеса используется как основа для формирования страха, а страх — как механизм продажи и удержания услуг. Если в классическом рэкете платили за то, чтобы проблемы не возникли, то в цифровом рэкете платят за то, чтобы вероятность проблем оставалась под контролем — даже если сама эта вероятность до конца не измерима.

Часть I. Когда страх был прямым

Глава 1. Рэкет как примитивная, но честная модель рынка страха

Чтобы понять, как устроен современный рынок безопасности, иногда полезно вернуться туда, где всё было проще и грубее. Не из-за того, что прошлое лучше объясняет настоящее, а потому, что в нём меньше масок. Там, где сегодня действуют сложные формулировки и аккуратные отчёты, тогда работали прямые договорённости, в которых не оставалось места иллюзиям.

Рэкет в девяностые часто воспринимается как хаос — набор случайных столкновений, агрессии и криминальных историй. Но при более внимательном взгляде становится ясно, что это была вполне устойчивая система. Примитивная по форме, но весьма логичная по сути. В ней были свои правила, свои роли, свои механизмы удержания клиента. И главное — в ней была чёткая экономическая модель.

В основе этой модели лежала уязвимость бизнеса. Любой коммерсант того времени находился в ситуации, где он не мог быть полностью защищён. Государственные институты были слабы, формальные механизмы защиты либо не рабо-

тали, либо не вызывали доверия. Это создавало пространство неопределённости, в котором риск становился постоянным фоном. И именно на этом фоне появлялся тот, кто предлагал решение.

«Крыша» в классическом понимании не продавала безопасность в её абсолютном смысле. Она продавала управляемость риска. Это важное различие, которое часто упускают. Речь шла не о том, чтобы полностью устранить угрозу, а о том, чтобы сделать её предсказуемой. Угроза могла оставаться, но она переставала быть хаотичной. Она становилась частью договорённости.

Платёж в этой системе был регулярным не случайно. Страх — это не разовое событие. Это состояние, которое требует постоянного обслуживания. Нельзя один раз заплатить и считать, что вопрос закрыт навсегда. Неопределённость возвращается, если её не поддерживать в контролируемых рамках. Поэтому плата превращалась в процесс, а не в сделку. Это был не разовый акт, а форма отношений.

Главный товар, который продавался в этой системе, не был связан напрямую с физической защитой. Да, могли быть люди, которые обеспечивали порядок, могли быть договорённости с другими группами, могли существовать механизмы давления на потенциальные угрозы. Но всё это было лишь внешним проявлением. Внутри продавалось другое — снижение неопределённости. Возможность планировать хотя бы на короткую дистанцию. Уверенность в том, что пра-

вила не изменятся внезапно.

Коммерсант платил не за справедливость. Справедливость в этой системе не была категорией. Он платил за предсказуемость. За то, чтобы понимать, где заканчиваются его риски и где начинаются гарантии. За то, чтобы его бизнес не зависел от случайного стечения обстоятельств. В условиях, где случайность могла стоить всего, предсказуемость становилась ценностью.

Если убрать моральную оценку, рэкет можно рассматривать как один из самых простых способов монетизации уязвимости. Там не было сложных конструкций, не было длинных объяснений, не было необходимости убеждать клиента в абстрактных рисках. Уязвимость была очевидна, угроза — ощутима, решение — конкретно. Именно эта прямолинейность делала систему устойчивой.

В этом смысле рэкет был грубым, но в каком-то парадоксальном смысле честным. Источник угрозы часто находился рядом с теми, кто предлагал защиту. Иногда он совпадал с ними полностью, иногда — частично, но связь была очевидной. Клиент понимал, за что он платит, даже если не мог это сформулировать словами. Он понимал, что платит не за идеальный порядок, а за то, чтобы хаос не вышел за пределы допустимого.

Это была модель, в которой не было иллюзий прозрачности. Не было попытки представить происходящее как нечто иное. Всё было названо своими именами, пусть и не всегда

вслух. И именно поэтому она так хорошо подходит в качестве отправной точки. Не потому, что её нужно оправдывать или повторять, а потому, что в ней отчётливо видна базовая логика: уязвимость создаёт страх, страх формирует спрос, а спрос рождает того, кто готов этот страх упорядочить — за определённую цену.

Дальше меняются инструменты. Меняется язык. Меняется уровень сложности. Но сама конструкция остаётся узнаваемой.

Глава 2. Почему бизнес соглашался платить

На первый взгляд может показаться, что согласие бизнеса на подобные условия было проявлением слабости, страха или даже недальновидности. Но такая интерпретация слишком поверхностна. Она упрощает реальность до уровня морали, игнорируя экономическую логику, в которой принимались решения. На практике всё было гораздо рациональнее и, в определённом смысле, неизбежнее.

Любой бизнес существует в системе правил. Когда эти правила понятны, стабильны и защищены институтами — законом, судом, правоохранительными органами — предприниматель может опираться на них как на основу своей деятельности. Он понимает, какие риски допустимы, какие последствия наступят в случае конфликта, и какие механизмы позволят ему защитить свои интересы. В такой системе безопасность перестаёт быть личной проблемой и становится частью общей инфраструктуры.

Но когда государство не выполняет эту функцию, возникает вакуум. И рынок, как любая адаптивная система, не терпит пустоты. Там, где отсутствует формальная защита, появляются её неформальные аналоги. Не потому, что кто-то сознательно проектирует их с нуля, а потому что сама среда вынуждает участников искать способы снизить неопреде-

лённость.

В этом контексте «крыша» перестаёт выглядеть как исключительно криминальное явление и начинает восприниматься как своеобразный суррогат безопасности. Неидеальный, зачастую агрессивный, но выполняющий конкретную функцию — стабилизацию рисков. Это не отменяет его противоправной природы, но позволяет понять, почему он стал частью экономической реальности.

Предприниматель в такой среде не выбирал между «хорошим» и «плохим». Он выбирал между управляемым и неуправляемым риском. Между предсказуемыми потерями и потенциально катастрофическими. И в этом выборе регулярный платёж начинал выглядеть не как уступка, а как инструмент выживания.

Страх в этой системе играл ключевую роль. Но важно понимать: это был не иррациональный страх, а страх, основанный на наблюдаемой реальности. Потери были конкретными, угрозы — ощутимыми, последствия — быстрыми и тяжёлыми. В таких условиях страх становился экономическим фактором, который можно учитывать, сравнивать и, в определённой степени, «покупать».

Именно поэтому регулярная плата воспринималась как меньшее зло. Она превращала неопределённость в фиксированное обязательство. Да, это были издержки. Но это были понятные издержки. Они позволяли строить хоть какую-то модель планирования, закладывать расходы, рассчитывать

маржу. В условиях, где внезапный удар мог уничтожить бизнес за один день, такая предсказуемость приобретала особую ценность.

Здесь проявляется важный психологический сдвиг: страх убытка оказывается сильнее желания свободы. Свобода в среде с высокой неопределённостью теряет свою привлекательность, потому что не даёт гарантий. Напротив, она увеличивает зону риска. В то время как зависимость, если она сопровождается стабильностью, начинает восприниматься как более рациональный выбор.

Ещё один важный момент — невозможность точно измерить риск. Когда предприниматель не может определить вероятность угрозы, оценить её масштаб и последствия, он оказывается в ситуации, где классические методы управления перестают работать. В такой среде на первый план выходят не цифры, а отношения. Связи, договорённости, личные гарантии начинают заменять формальные механизмы оценки и защиты.

«Крыша» в этом смысле становилась не только защитой, но и формой социального контракта. Контракта, в котором не было юридической силы, но была практическая применимость. Предприниматель покупал не уважение и не статус — он покупал право продолжать работу в условиях, где это право не было обеспечено ничем иным.

Важно подчеркнуть: эта модель не возникла из-за наивности или слабости бизнеса. Она возникла как адаптация к сре-

де, в которой альтернативы либо отсутствовали, либо были значительно менее эффективны. Рациональность здесь проявлялась не в следовании идеалам, а в способности выживать в конкретных условиях.

Именно поэтому эта глава важна для дальнейшего понимания. Если рассматривать подобные явления исключительно как результат давления, легко упустить вторую сторону — согласие, основанное на расчёте. А без этого невозможно увидеть полную картину. Потому что в любой системе, где существует регулярный платёж за снижение риска, всегда есть не только тот, кто предлагает, но и тот, кто соглашается. И причины этого согласия почти всегда глубже, чем кажется на первый взгляд.

Глава 3. Механика «крыши»: контроль, зависимость, невозможность выхода

Рэкет редко был разовым событием. Он не ограничивался моментом первого контакта, не сводился к одному платежу и не заканчивался после «решения вопроса». Его настоящая сила заключалась в другом — в способности превращаться в устойчивую модель отношений, в которой клиент постепенно терял возможность выйти из системы без серьёзных последствий.

Первый платёж почти никогда не воспринимался как точка невозврата. Скорее — как временная мера, компромисс, вынужденное решение в конкретной ситуации. Предприниматель мог думать, что это лишь способ «переждать», выиграть время, стабилизировать положение. Но сама конструкция таких отношений была устроена иначе. Она не предусматривала краткосрочности. С момента первого соглашения начинался процесс встраивания.

Платёж закреплял не только факт взаимодействия, но и новую реальность. Бизнес начинал существовать внутри системы, где его устойчивость частично зависела от внешнего субъекта. И чем дольше продолжались эти отношения, тем глубже становилась эта зависимость. Постепенно исчезала

возможность вернуться в исходную точку, потому что сама исходная точка переставала существовать.

«Защита» в этой модели переставала быть услугой в привычном смысле. Услуга предполагает возможность выбора, сравнения, отказа. Здесь же возникала иная логика — логика привязки. Ты не просто платил за определённое действие, ты становился частью структуры, в которой отказ от участия означал рост риска. Причём этот риск был не абстрактным, а вполне конкретным и ожидаемым.

Со временем формировался эффект невозвратных отношений. Чем дольше предприниматель находился внутри системы, тем больше факторов начинали удерживать его в ней. Возникала инерция, основанная не только на страхе, но и на привычке. Система начинала восприниматься как часть нормального порядка вещей. Отказ от неё требовал не только смелости, но и готовности принять неопределённость, к которой бизнес уже отвык.

Особую роль в этом процессе играла невозможность объективной оценки результата. Клиент не мог точно определить, от чего именно его защитили. Не было прозрачных метрик, не было сопоставимых сценариев, не было контрольной группы, с которой можно было бы сравнить своё положение. Отсутствие проблем становилось единственным наблюдаемым результатом.

И здесь происходил важный сдвиг в восприятии. Если ничего не происходит — значит, система работает. Если бизнес

функционирует без сбоев — значит, защита эффективна. Постепенно отсутствие негативных событий начинало восприниматься не как нормальное состояние, а как доказательство ценности оплачиваемой услуги.

Это создавало замкнутый контур. Любое сомнение в необходимости платежа сталкивалось с простым аргументом: «пока платишь — всё спокойно». И проверить обратное можно было только одним способом — перестать платить. Но этот способ был связан с риском, который предприниматель уже однажды решил минимизировать. Таким образом, сама возможность проверки становилась слишком дорогой.

В результате зависимость укреплялась не только внешним давлением, но и внутренней логикой принятия решений. Рациональность, которая когда-то привела к первому платежу, начинала работать на поддержание системы. Отказ от неё требовал не просто пересмотра условий, а изменения всей модели восприятия риска.

Именно здесь проявляется одна из ключевых особенностей подобных механизмов: они не нуждаются в постоянном напоминании о своей силе. Достаточно один раз встроиться в структуру, чтобы она начала воспроизводить себя через поведение клиента. Контроль становится не только внешним, но и внутренним — он закрепляется в ожиданиях, в оценке рисков, в самой логике планирования бизнеса.

В этом смысле рэкет был не столько актом принуждения, сколько системой управления неопределённостью через за-

висимость. Он не устранял риск полностью, но делал его предсказуемым и, что важнее, управляемым через регулярные отношения.

Эта логика имеет важное продолжение. Самой устойчивой оказывается та услуга, результат которой невозможно до конца верифицировать. Там, где нет точного измерения, всегда остаётся пространство для интерпретации. И именно в этом пространстве формируется долгосрочная привязка клиента — не через силу, а через невозможность окончательно понять, что произойдёт, если он выйдет из системы.

Часть II. Переезд бизнеса в цифру

Глава 4. От палаточного ларька к цифровому активу

Любой бизнес привязан к своим активам. В девяностые эти активы были осязаемыми: помещение, товар, оборудование, точка продаж. Их можно было увидеть, пересчитать, физически защитить. Уязвимость бизнеса в значительной степени совпадала с уязвимостью его материальной оболочки. Если разбивали витрину, ломали замок или выносили товар — это было прямым и понятным ударом.

Со временем эта логика начала меняться. Бизнес постепенно переехал в другую среду — менее заметную, но гораздо более сложную. Сегодня его основа всё чаще находится не в физическом пространстве, а в цифровой инфраструктуре. Сайт, база клиентов, доменное имя, корпоративная почта, CRM-система, облачные документы, платёжные сервисы, рекламные кабинеты — всё это стало не вспомогательными элементами, а ядром деятельности.

Именно здесь происходит принципиальный сдвиг. Объект, который нужно защищать, меняет свою природу. Он становится нематериальным, распределённым и в значитель-

ной степени невидимым для самого владельца. Бизнес может продолжать работать в привычном физическом формате — офис, склад, сотрудники — но его ключевые процессы уже зависят от систем, которые невозможно «обойти глазами».

Цифровой актив при этом часто оказывается дороже своей физической оболочки. Потеря помещения — это серьёзно, но она, как правило, имеет понятные последствия и относительно ясный сценарий восстановления. Потеря доступа к данным, к базе клиентов, к системе управления заказами или к рекламным каналам может оказаться куда более разрушительной. В отличие от разбитой витрины, которую можно заменить, цифровая потеря часто означает утрату того, что невозможно быстро воспроизвести.

Особенно это касается данных. Они не только фиксируют прошлое бизнеса, но и формируют его будущее. История взаимодействия с клиентами, финансовые операции, логика процессов — всё это превращается в основу устойчивости. И именно поэтому доступ к данным становится критической точкой. Потерять данные — значит потерять не только текущие операции, но и способность продолжать их в прежнем виде.

К этому добавляется ещё один слой — репутация. В цифровой среде она становится не абстрактной характеристикой, а экономическим фактором. Утечка информации, компрометация сервиса, сбой в работе сайта или платёжной системы — всё это напрямую влияет на доверие клиентов. И

это доверие можно потерять гораздо быстрее, чем в офлайн-мире, потому что информация распространяется мгновенно и без границ.

В результате экономика угроз меняется. Если раньше ущерб был локальным и часто ограничивался конкретным объектом, то теперь он может быть системным. Один инцидент способен затронуть сразу несколько уровней — операционный, финансовый, репутационный. И самое важное — для этого не требуется физического вторжения.

Сегодня бизнес можно парализовать, не приближаясь к нему в буквальном смысле. Достаточно нарушить доступ к ключевым системам. Достаточно изменить настройки домена, заблокировать аккаунт, нарушить работу сервера или зашифровать данные. В отличие от прошлого, где воздействие было видимым и осязаемым, современное воздействие может быть почти незаметным до момента, когда последствия становятся критическими.

Это создаёт новую форму уязвимости. Она менее очевидна, но более глубока. Её сложнее обнаружить, сложнее оценить и, что особенно важно, сложнее контролировать без специализированных знаний. Владелец бизнеса может прекрасно понимать, как устроены его процессы на уровне операций, но при этом не иметь полного представления о том, как именно они реализованы в цифровой среде.

Именно в этой точке возникает важный переход. Раньше угрозы были связаны с физическим воздействием: мог-

ли выбить стекла, сломать дверь, повредить имущество. Сегодня угроза принимает другую форму. Сайт могут «положить», домен — переоформить, базу клиентов — скопировать и распространить, сервер — зашифровать, рекламные кабинеты — перехватить.

Внешне бизнес может оставаться на месте. Люди приходят в офис, сотрудники выполняют свои задачи, помещение не повреждено. Но при этом ключевые процессы уже остановлены. Заказы не принимаются, платежи не проходят, клиенты не могут получить доступ к сервису. Физическая оболочка остаётся, но функция исчезает.

Это и есть главный результат цифрового перехода. Уязвимость смещается из видимого пространства в невидимое. И вместе с этим меняется сама природа риска. Он становится менее очевидным, но более тотальным. И именно это создаёт новую среду, в которой будут формироваться следующие модели защиты, зависимости и, как следствие, экономических отношений вокруг безопасности.

Глава 5. Новая уязвимость: бизнес не понимает, как устроена его собственная цифровая среда

Переезд бизнеса в цифру изменил не только форму активов, но и характер ответственности за них. В физическом мире владелец, как правило, понимает, чем он владеет. Он знает, где находится его помещение, кто имеет к нему доступ, какие ресурсы используются и как устроены ключевые процессы. Даже если он делегирует управление, у него остаётся базовое представление о структуре.

В цифровой среде эта связь размывается. Бизнес продолжает существовать, процессы продолжают работать, но понимание того, как именно всё устроено, постепенно уходит за пределы компетенции владельца. И это не исключение, а скорее норма. Большинство предпринимателей не знает, как устроены их сайты, на каких серверах они размещены, как организованы резервные копии, кто управляет доступами и где проходит граница между их системой и внешними сервисами.

На первый взгляд это выглядит как естественное следствие развития технологий. Невозможно быть экспертом во всём. Сложность неизбежно приводит к специализации. Но именно здесь возникает новая форма уязвимости — не тех-

ническая, а управленческая. Бизнес начинает зависеть не столько от самой инфраструктуры, сколько от тех, кто её понимает.

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.