

УДК 339.13  
ББК 65.290-2  
С30

**Семенчук, Вячеслав Владимирович.**

С30      Бизнес-хакинг. Ищи уязвимости конкурентов – взрывай рынок / Семенчук Вячеслав Владимирович. – Москва : Эксмо, 2019. – 208 с. – (Бизнес. Как это работает в России).

ISBN 978-5-04-096327-0

Вячеслав Семенчук протестировал на опыте запуска и развития собственных бизнесов принципы хакинга. Усовершенствовал их и предложил новый подход к поиску и созданию новых высокодоходных проектов.

Для создания преимущества компании необходимо трансформировать метод работы с конкурентами, используя их ошибки и провалы как ресурс для собственного роста и развития. Книга раскрывает стратегии, которые помогут усилить позиции бизнеса на рынке и победить противников в битве за рынок.

УДК 339.13  
ББК 65.290-2

ISBN 978-5-04-096327-0

© Семенчук В.В., текст, 2019  
© Оформление. ООО «Издательство «Эксмо», 2019

# ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ.....	11
<b>ГЛАВА 1. УЯЗВИМЫЙ МИР</b> .....	<b>13</b>
Риски и возможности.....	13
Что такое уязвимость?.....	15
Негативное отношение.....	17
Притягательность уязвимости.....	18
Динамичность и вариативность.....	20
Криптонит для Супермена.....	21
Умные суперхищники.....	23
Используем этично.....	27
Ломать, чтобы строить.....	29
Конкуренция уязвимостей.....	35
Инновационные уязвимости.....	37
<b>ГЛАВА 2. ОСОБЕННОСТИ ХАКЕРОВ</b> .....	<b>40</b>
Разносторонние.....	40
Влиятельные.....	41
Бдительные.....	44
Пугающие.....	47
Разные.....	49

## ОГЛАВЛЕНИЕ

Настоящие .....	52
Эффективные .....	54
Предприимчивые .....	56
<b>ГЛАВА 3. ПРИНЦИПЫ ХАКЕРОВ .....</b>	<b>62</b>
Увлеченность делом .....	62
Больше, дольше, усерднее .....	66
Вхождение в состояние потока .....	70
Использование незнания .....	75
Постоянное обучение .....	79
Хакеры верят, что способны научиться .....	82
Хакеры изучают только то, что используют .....	83
Хакеры объединяют теорию с практикой .....	85
Хакеры обучаются самостоятельно учиться .....	86
Перенос знаний и навыков .....	87
Системный подход .....	93
Жизнь и бизнес как игра .....	101
Стратегия .....	106
Разница между работой и игрой .....	109
Будь как Рико и Роже .....	111
Создание сообществ .....	112
Командная работа .....	119
Сооснователи .....	119
Формирование команды .....	122
Конкуренты .....	124
Большая идея .....	125

ГЛАВА 4. ПАРАДОКСЫ ХАКИНГА .....	131
Неуловимая криптовалюта .....	131
Смотрим, но не видим .....	134
Одна идея, многие смыслы .....	139
Уязвимости мышления .....	143
Страх ошибок .....	144
Непринятие нового .....	145
Ограниченность «здорового смысла» .....	146
Перекладывание ответственности .....	148
Желание ничегонеделания .....	148
Перегруженность информацией .....	149
Бизнес – это система .....	150
Бизнес-идея – это модель системы .....	152
Создание модели системы .....	154
Меняем готовое .....	154
Ищем то, что уже есть .....	157
Объясняем известным .....	158
Все начинается с идеи взлома .....	159
ГЛАВА 5. ВЗЛАМЫВАЕМ СИСТЕМУ .....	162
Изучаем систему .....	162
Идея в ящике .....	162
Находим ящики .....	165
Изучаем ящики .....	169
Экспериментируем для поиска идеи .....	171
Строим гипотезы .....	171
Проверка гипотез .....	173
<i>Черные ящики</i> .....	174

## ОГЛАВЛЕНИЕ

<i>Белые ящики</i> . . . . .	175
<i>Серые ящики</i> . . . . .	175
Контролируемый провал . . . . .	176
Серия экспериментов . . . . .	180
<i>Первый шаг подсказывает второй</i> . . . . .	180
<i>Ориентируйтесь на обратную связь</i> . . . . .	180
<i>Сложить по-новому</i> . . . . .	181
<i>Рандомизированное контролируемое испытание</i> . . . . .	182
Создаем идею из уязвимости . . . . .	183
На основе изучения ящика . . . . .	183
На основе нахождения ошибок . . . . .	185
Создание новой идеи . . . . .	187
Простые, но быстрые идеи . . . . .	190
Маленькие перспективные идеи . . . . .	192
Взращивание большой идеи . . . . .	193
ПОСЛЕСЛОВИЕ . . . . .	196
УКАЗАТЕЛЬ . . . . .	197

*Ищи уязвимости – находи новые идеи  
для бизнеса в реальном мире*



# ПРЕДИСЛОВИЕ

Я запустил почти четыре десятка стартапов. Развиваю их, потом продаю и запускаю новые. Поэтому меня часто спрашивают, как найти идею для старта нового проекта. Однажды я понял, что у меня нет ответа – каждый день идеи сами приходят мне в голову. За год их набирается больше тысячи, и нужно лишь выбирать лучшие, для чего я создал систему валидации. В методике поиска идей я никогда не нуждался.

Все изменилось, когда я основал проект Akselerator.ru и начал обучать предпринимателей. Тогда возникла насущная необходимость научить резидентов акселератора делать то, что у меня получается само собой. Почему у меня полно идей, а у кого-то их вообще нет? Как находить идеи? Откуда они возникают у меня? Я понял это год назад, когда писал свою третью книгу. В ней я рассказал, как создавать мобильные приложения. Предисловие написали специалисты по кибербезопасности, которые защищают компании от хакерских атак и расследуют киберпреступления. Они работают с уязвимостями чужого бизнеса и ищут тех, кто использует уязвимости не лучшим образом, – с хакерами.

Последние пять лет, как бизнес-хирург, я тоже ищу уязвимости в бизнесе других людей, тем самым помогая проектам «излечиваться», расти и развиваться. С пяти лет я неотделим от компьютера. В детстве папа учил меня программировать. В подростковом возрасте я изучал журнал «Хакер», где прочитал, как работают, что делают и как думают хакеры. Это повлияло на мои привычки, способ мышления и выбор проектов. Я всегда интересовался информационными технологиями, пытаюсь понять, как все устроено и почему работает.

Большинство моих бизнес-проектов по-прежнему связаны с ИТ, я постоянно сталкиваюсь с уязвимостями и ошибками в программ-



## ПРЕДИСЛОВИЕ

ном обеспечении, использую новые технологии и инструменты, которые дает Интернет. Но как бизнес-хирург я работаю с уязвимостями в широком смысле этого слова. Мои поиски не ограничиваются ИТ и ИТ-бизнесом. В этой книге я расскажу, как использовать хакерское мышление для поиска новых идей через поиск уязвимостей в любой сфере человеческой деятельности.

С уважением,  
**Вячеслав Семенчук,**  
ваш бизнес-хирург

# ГЛАВА 1

## УЯЗВИМЫЙ МИР

### Риски и возможности

«Нас взломали!»

«Я порезался!»

«Мой стартап привлек более трехсот миллионов рублей инвестиций!»

Что общего у этих событий, произошедших со мной? Первые два – неприятности разной величины, третье – это успех. Первые два могут произойти с кем угодно и где угодно, часто случайно, третье требует тяжелого труда и большого количества времени. Я потратил много лет на свой стартап, прежде чем смог привлечь крупные инвестиции.

Эти три совершенно разных события вызваны одним и тем же фактором, который присутствует во всем, что нас окружает. Он характерен как для крупных корпораций, так и для мелких проектов, для людей, животных и вещей. Он присутствует в вас, вашем коте и компьютере одновременно. Он во всем и везде, и обычно его называют одним словом – «уязвимость».

Мой сайт взломали злоумышленники, когда нашли уязвимость в программном обеспечении. Я порезался, потому что кожа человека чувствительна к острым лезвиям. Мне удалось привлечь более трехсот миллионов рублей инвестиций, потому что сначала я обнаружил уязвимость в чужом бизнесе, а потом нашел способ ее исправить и запустил собственный бизнес.

Знаете, как появляется большинство бизнес-проектов? Почкованием! Кто-то открывает новый бизнес, очень похожий на прежний, но это улучшенная, исправленная версия, в которой основатель устранил уязвимости старого бизнеса. Многие инновации появились только потому, что была найдена и устранена уязвимость старой технологии. Например, космическим полетам мешает дороговизна. Илон Маск нашел способ их удешевить, создав многоразовые ракеты.

Как выразилась Брене Браун, называющая себя исследователем-рассказчиком: «Мы живем в уязвимом мире»<sup>1</sup>. Уязвимо все: вещи, люди, природа в целом. Мы уязвимы к смерти и процессам старения, к чувствам любви и ненависти, к желанию добиться успеха и жить в достатке. Вещи вокруг нас уязвимы в отношении механических повреждений, старения, моды. Даже наша планета оказалась уязвимой к человеческой деятельности, потому что мы вмешались в естественный отбор, уничтожив много видов животных и растений.

Уязвимости позволяют развиваться, находить новые идеи, создавать новые технологии, исправлять ошибки. «Нет предела совершенству», потому что все может быть улучшено, а все может быть улучшено, потому что во всем есть уязвимости. Уязвимость – необходимое условие эволюции.

«Абсолютная неуязвимость недостижима, а значит, нам нужен механизм, посредством которого система станет непрерывно обновляться»

НАССИМ ТАЛЕБ. «Антихрупкость, Как извлечь выгоду из хаоса»

Иметь уязвимости естественно. Каждая уязвимость – это риск и возможность роста и развития одновременно, потому что там,

<sup>1</sup> Брене Браун. TED. Сила уязвимости. URL: [https://www.ted.com/talks/brene\\_brown\\_on\\_vulnerability/transcript?language=ru#t-30892](https://www.ted.com/talks/brene_brown_on_vulnerability/transcript?language=ru#t-30892)

где есть возможность – всегда есть риск, а там, где присутствует риск – всегда есть возможность. Благодаря уязвимостям мы учимся и приспособляемся к постоянно меняющимся условиям жизни, растем и развиваемся.

## Что такое уязвимость?

От людей с разным опытом, знаниями и вкусами мы услышим разные ответы, и каждый будет прав по-своему. Раньше я думал об уязвимости как о возможном взломе программного обеспечения и компьютеров и ассоциировал это понятие с хакерами и ошибками программистов. Кто-то скажет, что уязвимость – это возможность нанесения или получения вреда со стороны другого человека. Кто-то подумает, что речь идет об уязвимости к болезням и стихийным бедствиям, против которых люди чаще всего бессильны. Тот, кто объединит эти и многие другие ответы, будет ближе всего к истине.

В данный момент лучшее определение уязвимости дают специалисты информационных технологий, так как только в этой сфере деятельности действительно идет активная работа с уязвимостями в широком смысле этого слова. Только в ИТ уязвимости не просто ищут, находят и устраняют, но и целенаправленно создают, чтобы использовать с разными целями.

Наилучшее определение уязвимости, я нашел в ГОСТе Р 53114-2008 «Термины и определения общетехнических понятий»:

Уязвимость: внутренние свойства объекта, создающие восприимчивость к воздействию источника риска, которое может привести к какому-либо последствию<sup>2</sup>.

---

<sup>2</sup> ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».