Росс Халелюк

КАК ПОСТРОИТЬ СТАРТАП В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

ПОЛНОЕ ПРАКТИЧЕСКОЕ РУКОВОДСТВО

2

ЧАСТЬ

НОВЫЙ БИЗНЕС — КОМПЛЕКС ЗАДАЧ

Бывают книги, в которых под одной обложкой собрано все, что может понадобиться для решения сложной задачи. И перед вами — именно такая.

Если вы уже создали стартап в сфере кибербезопасности или только задумываетесь над тем, как его создать, и даже если вы работаете в совершенно другой сфере — эта книга научит вас смотреть на любой бизнес как на комплекс креативных, управленческих, технических и маркетинговых задач.

Вы узнаете, зачем компании нужны соучредители из разных сфер, на что обращают внимание инвесторы, от чего зависит успех продукта и как продвигать бизнес, если бюджет на продвижение стремится к нулю. Вы также поймете, на что стоит обращать внимание, а чем можно пренебречь. Почему универсальные продукты могут оказаться хуже специализированных, и чем отличаются продукты-«витамины» от продуктов-«обезболивающих», и какой вариант выбрать. Вы даже поймете, в какой отрасли искать клиентов, которые будут долго приносить вам деньги.

Эта книга — практическое руководство по созданию ИБ-стартапа, справочник по современному бизнес-мышлению, вдохновитель и источник идей.

КАК УСТРОЕН РЫНОК КИБЕРБЕЗОПАСНОСТИ

Кибербезопасность пронизывает все сферы современного бизнеса и динамично развивается вместе с компаниями, влияя на бизнес-процессы и технологии, стратегические и тактические решения.

Для развития кибербезопасности имеют значение три ключевых фактора:

1. технологические инновации — появление облачных технологий, ИИ и других передовых решений;
2. конкуренция и постоянная необходимость адаптироваться ради сохранения конкурентоспособности;
3. эволюция киберугроз — способы взлома совершенствуются, а значит, и способы защиты не должны отставать.

Сегодняшние кибератаки — это завтрашние оборонительные стратегии.

ЛАНДШАФТ ОТРАСЛИ

Стартапы в сфере кибербезопасности играют основную роль во внедрении инноваций. В свою очередь, крупные компании много инвестируют в масштабирование и создание единых платформ, занимаются поглощениями стартапов и интеграцией их технологий. Этого требуют и клиенты, которым удобнее пользоваться объединенными инструментами.

Консолидация и разделение инструментов кибербезопасности — циклический процесс. Сначала появляются узкоспециализированные решения, которые сливаются в платформы, а затем рынок снова нуждается в новых стартапах и инновациях. Это создает динамичную экосистему, где крупные компании и стартапы взаимно выигрывают, и до сих пор неясно, кто окажется победителем в долгосрочной перспективе.

БИЗНЕС НА ДОВЕРИИ: ПЛЮСЫ И МИНУСЫ

Бюджеты клиентов на ИБ неуклонно растут: даже в кризис компании не хотят рисковать и отказываться от защиты. При этом, когда компания покупает систему безопасности, она фактически платит за обещание, что продукт защитит ее от угроз. Проверить это до реальной атаки практически невозможно.

И даже если инструмент работает во время тестирования, он может не справиться с реальной атакой.

Поэтому при выборе продукта клиенты вынуждены полагаться на репутацию разработчиков, на их стабильность и готовность работать быстро.

Все в кибербезопасности строится на доверии, а у этого подхода есть как плюсы, так и заметные минусы. Среди позитивных аспектов автор называет прежде всего устойчивость:

- стартапы в кибербезопасности реже проваливаются. Даже закрытие компании не считается неудачей, поскольку основатели приобретают ценный опыт;
- ориентация на доверие и длинные циклы продаж позволяют ИБ-компаниям работать с постоянными клиентами многие годы;
- возможность зарабатывать достаточно, даже если стартап не стал лидером рынка.

Но есть и негативные аспекты:

- долгий процесс завоевания доверия;
- медленные циклы продаж и внедрения;
- сложность быстрого масштабирования;
- высокий риск копирования идей конкурентами;
- ориентация клиентов на покупку решений у местных поставщиков, что затрудняет глобальную экспансию стартапов.

В сфере кибербезопасности даже крупнейшие компании контролируют менее 10% общего рынка, хотя при этом могут лидировать в отдельных сегментах.

ОСНОВАТЕЛИ ИБ-СТАРТАПОВ

Создание стартапа в области кибербезопасности требует глубоких знаний и практического опыта в технически сложной и быстро меняющейся области. Поэтому, в отличие от других отраслей, здесь редко встречаются молодые предприниматели без опыта. Чаще всего компании ИБ создают люди с репутацией, опытом и связями.

Но даже они часто мыслят фрагментарно:

- иллюзия уникальности: специалисты считают многие проблемы кибербезопасности исключительными, хотя похожие проблемы (например, избыток поставщиков) встречаются и в других технологических областях;
- неиспользование знаний из других сфер: в кибербезопасности не принято заимствовать проверенные подходы из более зрелых IT-отраслей. Вместо этого специалисты часто пытаются изобрести уникальные решения, тратя время и ресурсы на разработку технологий, которые уже существуют.

ИНВЕСТОРЫ

Для развития стартапам необходим капитал. Обычно стартапы финансируют ангелы-инвесторы, венчурные фирмы, стартап-инкубаторы и акселераторы.

На поздних стадиях развития доступны более сложные финансовые инструменты, такие как частные инвесторы и венчурный долг.

АНГЕЛЫ-ИНВЕСТОРЫ

Ангелы-инвесторы — это частные лица, которые инвестируют свой капитал в стартапы на самых ранних стадиях, когда продукт находится на стадии идеи или бета-версии.

Ангелами-инвесторами в сфере ИБ часто становятся руководители и специалисты служб безопасности, а также предприниматели, связанные с вопросами безопасности.

Активные ангелы-инвесторы поддерживают стартапы своим опытом и знаниями, помогая основателям реализовать их идеи. Финансовые («пассивные») ангелы предоставляют только капитал и позволяют основателям работать самостоятельно, что подходит опытным предпринимателям.

Задача ангелов-инвесторов — помочь стартапу перейти на следующий уровень, чтобы привлечь венчурный капитал.

Они помогают с определением проблемы, разработкой и тестированием решений, созданием стратегии сбора средств и выхода на рынок. При оценке стартапов ангелы обращают внимание на:

- команду: опыт и успешные проекты;
- тайминг: синхронизацию продукта с потребностями рынка;
- рыночные предпосылки: наличие платежеспособных клиентов, партнеров, доказательства востребованности.

Предприниматели понимают, что ценность ангела заключается не только в капитале, но и в опыте, ресурсах и помощи. Поэтому они держат ангела в курсе прогресса и даже при наличии венчурного финансирования оставляют долю для ангелов.

Для опытных специалистов в области безопасности привлечь ангелов-инвесторов проще всего через личные связи в своей профессиональной нише.

СИНДИКАТЫ И СООБЩЕСТВА АНГЕЛОВ-ИНВЕСТОРОВ

Синдикаты — это группы инвесторов, которые объединяют средства для коллективных вложений в стартапы, упрощая процесс для предпринимателей и снижая административные расходы.

Помимо средств инвесторов, синдикаты предлагают стартапам доступ к экспертам, расширение сети, стратегическую поддержку и гибкость в вопросах временных рамок и выхода на рынок.

Однако автор замечает, что сообщества ангелов-инвесторов могут иметь и недостатки: ограничения по суммам инвестиций на ранних стадиях, риск утечки конфиденциальной информации и возможные трудности из-за большого числа участников.

Синдикаты инвесторов — это сообщества, внутри которых заключаются сделки, проходит обмен опытом и обучение. Они предоставляют не только капитал, но и консультации и долгосрочную поддержку.

Групповые инвестиции укрепляют репутацию стартапа и повышают шансы на успешное привлечение следующих уровней финансирования.

СТАРТАП-ИНКУБАТОРЫ И АКСЕЛЕРАТОРЫ

Соучредитель и генеральный директор Tidal Cyber Рик Гордон подчеркивает, что акселераторы и инкубаторы помогают разработчикам научиться пользоваться проверенными фреймворками для оценки рыночных сигналов, стратегического и финансового планирования.

Стартап-инкубаторы и акселераторы помогают молодым компаниям, предоставляя не только финансирование, но и ресурсы, наставничество и связи, а взамен получают небольшую долю в бизнесе.

Участие в специализированных программах помогает стартапам наладить связи с потенциальными клиентами и партнерами, что может быть решающим для успеха.

Программы инкубаторов и акселераторов могут принести нестандартные идеи и решения. Однако стоит избегать частых переходов между акселераторами, так как это может замедлить рост компании.

ВЕНЧУРНЫЙ КАПИТАЛ

В отличие от инкубаторов, венчурные инвесторы — это не поддерживающие структуры, а полноценные бизнес-партнеры для стартапов.

Модель венчурного капитала направлена на высокорисковые инвестиции в стартапы с большим потенциалом роста. Инвесторы, вкладывающие в венчурные фонды собственные средства, называются ограниченными партнерами (LP), управляющие партнеры (GP) реализуют инвестиции.

Венчурные фирмы могут инвестировать в компании на любой стадии роста и используют различные подходы к формированию портфеля. Каждая венчурная компания имеет специализацию, определяющую выбор стартапов для инвестирования.

На первой встрече венчурный капиталист оценивает стартап по пяти ключевым параметрам:

1. рынок;
2. команда;
3. продукт;
4. текущие показатели;
5. динамика развития.

На ранних стадиях важнее рынок и команда, на поздних — продукт и конкурентные отличия.

Если венчурный фонд инвестировал в стартап $100 млн, прибыль будет распределяться по схеме 80/20 (ограниченные партнеры получат 80%, а генеральные — 20%). Кроме того, венчурные капиталисты ежегодно получают 2% на покрытие операционных расходов.

ТИПЫ ВЕНЧУРНЫХ КОМПАНИЙ

Специализированные венчурные компании, ориентированные на кибербезопасность, обладают глубокой экспертизой в этой области, что позволяет им эффективно оценивать стартапы. Их сильные связи в отрасли помогают находить партнеров, ресейлеров и клиентов, а специалисты задают более глубокие вопросы, что способствует лучшему пониманию потенциала стартапа. Однако их подход ограничен фокусом исключительно на кибербезопасности, что может затруднить адаптацию к изменениям на рынке и привести к вылету из перспективных трендов.

Универсальные венчурные компании, наоборот, обладают знанием различных рынков и могут рассматривать широкий спектр возможностей, не ограничиваясь одной отраслью. Это дает им большую гибкость и способность адаптироваться к изменениям. Но отсутствие глубоких знаний в области кибербезопасности может затруднить поддержку стартапов на ранних стадиях, а сложности с пониманием специфических особенностей рынка безопасности, таких как важность доверия и длительные циклы покупки, могут стать значительным препятствием.

КОРПОРАТИВНЫЙ ВЕНЧУРНЫЙ КАПИТАЛ

Корпоративный венчурный капитал (CVC) — это инвестиции крупных компаний в стартапы. Корпоративные инвесторы могут быть стратегическими или финансовыми:

- стратегические инвесторы вкладывают средства, чтобы создать совместный проект или укрепить партнерство между материнской компанией и стартапом;
- финансовые инвесторы нацелены на получение прибыли от инвестиций, при этом CVC может работать независимо от материнской компании.

Для успешного сотрудничества с корпоративными венчурными инвесторами важно проявлять инициативу, задавая вопросы о реальных примерах помощи другим компаниям и достигнутых результатах партнерства.

Предприниматели должны убедиться, что венчурная компания имеет эффективные механизмы для привлечения внутренних ресурсов, предоставляет реальную поддержку через технических экспертов и отраслевые знания.

Венчурные студии отличаются от акселераторов и инкубаторов тем, что фокусируются на поддержке малого числа стартапов — обычно от одного до пяти в год. Это делает их идеальными партнерами для начинающих предпринимателей, но для опытных бизнесменов сотрудничество со студией может быть слишком сложным.

ОТНОШЕНИЯ С ИНВЕСТОРАМИ

Стартапам стоит сосредоточиться на создании устойчивого бизнеса, а не только на привлечении финансирования. Развитие продукта и команды важнее презентации для инвесторов, а некоторые компании вообще могут успешно развиваться без внешних инвестиций, сохраняя больший контроль.

Автор советует начинать с привлечения некрупных инвестиций от ангелов-инвесторов и как можно раньше проверять продукт на практике. Это дает возможность быстро получить обратную связь от клиентов и лучше понять рынок. Ранняя концентрация не на росте, а на решении конкретной проблемы формирует устойчивую модель, основанную на реальной ценности.

Выстраивая отношения с венчурными капиталистами, нужно заранее изучать их и выбирать тех, кто разделяет ценности стартапа.

Стартапам стоит регулярно информировать инвесторов через новостные рассылки, демонстрируя успехи и достижения компании.

Харпиндер Сингх из Innovation Endeavors подчеркивает, что правильный инвестор должен быть вовлечен в развитие бизнеса и готов бросать вызов основателю. Привлечение корпоративных венчурных капиталистов требует тщательной оценки их мотивации — стратегии или финансовой прибыли.

ИНФЛЮЕНСЕРЫ

В сфере кибербезопасности существуют три ключевых типа инфлюенсеров, которые оказывают значительное влияние на формирование спроса и поведение покупателей.

Отраслевые аналитики — играют важную роль в установлении новых рыночных категорий, поскольку они исследуют проблемы на рынке и предлагают решения.

Аналитические компании предоставляют исследования, рекомендации и консультации как поставщикам, так и покупателям решений, непосредственно влияя на формирование рыночных тенденций и стратегий бизнеса. На их мнения опираются в процессе принятия решений, сравнения поставщиков, к ним обращаются по вопросам снижения рисков и обмена опытом.

Взаимодействие с аналитиками может быть полезным для повышения видимости стартапа и получения рекомендаций по его развитию. Инструменты взаимодействия с аналитиками — брифинги, запросы и контент-контракты.

Стартапам следует постоянно работать с проверенными аналитиками, четко представлять им свой продукт, демонстрировать его возможности и предоставлять реальные отзывы клиентов.

Саймон Моффатт подчеркивает, что аналитики должны не только помогать поставщикам представить свои решения в контексте бизнес-проблем, но и заботиться о том, чтобы покупатели могли разобраться в технических деталях и выбрать то, что соответствует их требованиям и целям.

Государственные регулирующие органы. Роль правительства состоит в обеспечении безопасности общественных интересов и включает защиту от угроз в сфере кибербезопасности.

Правительство содействует развитию ИБ-отрасли через партнерство с частным сектором, финансирует исследования, создает образовательные программы и способствует обмену информацией о киберугрозах.

Правительство — заказчик, крупнейший покупатель, который открывает компаниям доступ к масштабным контрактам. Кроме того, правительство — регулятор, оно устанавливает стандарты безопасности, что повышает спрос на новые продукты в этой сфере.

Предприниматели должны лоббировать важность киберзащиты, формируя устойчивые связи с государственными органами и отраслевыми ассоциациями, а также участвовать в некоммерческих советах и консультативных комитетах для влияния на принятие решений.

Страховые компании. В отличие от государственных органов, страховые компании — рыночная сила, которая стимулирует спрос на решения по кибербезопасности через свои требования.

Страховые компании заботятся о снижении рисков, устанавливая требования к клиентам, такие как многофакторная аутентификация и обучение сотрудников. Киберстрахование способствует развитию индустрии безопасности и внедрению стандартов и технологий. Разработчики в сфере безопасности могут использовать киберстрахование для продвижения своих продуктов, обеспечивая клиентам соответствие требованиям страховых компаний. Это способствует повышению спроса и снижению страховых премий для клиентов.

ПАРТНЕРСКИЕ КАНАЛЫ

Партнерские каналы — это ключевые точки сотрудничества для роста и масштабирования. Большинство затрат на безопасность проходит через партнеров, таких как ресейлеры, интеграторы и консалтинговые компании, особенно для крупных предприятий. Для достижения повышения доходов компании часто полагаются на партнерские экосистемы.

Shopify получила основную часть дохода через партнерскую сеть, а Microsoft получает 95% своего коммерческого дохода через партнерскую экосистему.

Существует несколько типов партнеров:

1. **Стратегические консультанты** — помогают разрабатывать стратегии безопасности и управлять ими. Сторонние консультанты с опытом в кибербезопасности помогают оценить текущий уровень безопасности, определить риски и разработать стратегические дорожные карты для внедрения защиты в бизнес-план.
2. **Ресейлеры с добавленной стоимостью (VAR)** — помогают клиентам выявлять проблемы безопасности, выбирать поставщиков

и внедрять решения. Они работают с консалтинговыми компаниями и конечными клиентами, поддерживая их в выборе продуктов и решении технических задач. В случае прямого обращения со стороны клиента VAR также могут влиять на выбор оптимальных решений и технологий для их реализации.

3. **Интеграторы** — управляют технической реализацией и адаптацией решений. Они занимаются проектированием, настройкой и интеграцией технологий для реализации стратегии информационной безопасности. Кроме того, интеграторы могут участвовать в выборе технологий, обучать клиентов и помогать им поддерживать безопасность и соответствие требованиям в условиях постоянно меняющейся ИТ-инфраструктуры.
4. **Поставщики услуг безопасности (MSSP)** и услуг **обнаружения и реагирования (MDR)** — обеспечивают мониторинг и поддержку.
5. **Поставщики услуг (MSP)** фокусируются на ИТ-потребностях клиентов. MSP, традиционно занимающиеся обслуживанием ИТ-инфраструктуры, все чаще включают кибербезопасность в свои предложения. Отдельно выделяются поставщики управляемых услуг безопасности (MSSP), которые предоставляют постоянный мониторинг и защиту информационных систем.

ПУТИ ВЫХОДА НА РЫНОК

Для основателей стартапов в сфере кибербезопасности есть несколько путей выхода на рынок: первичное публичное размещение акций (IPO), слияние с другой компанией или поглощение более крупным игроком. Однако самым вероятным вариантом выхода на рынок для стартапов будет поглощение.

Основные покупатели бизнесов в сфере кибербезопасности:

- **компании, выпускающие продукты безопасности,** — приобретают другие решения для расширения возможностей собственной платформы;
- **поставщики услуг в области кибербезопасности** — покупают компании для усиления команды и выхода на новые рынки;
- **технологические компании** — стремятся интегрировать функции безопасности в свои продукты;
- **профессиональные инвесторы** — приобретают недооцененные фирмы с целью повышения их операционной эффективности.

ТРЕНДЫ ИБ-ИНДУСТРИИ

АКТИВНОЕ УЧАСТИЕ КЛИЕНТОВ ВО ВНЕДРЕНИИ РЕШЕНИЙ

Автор отмечает, что процесс внедрения программ безопасности в организациях меняется: традиционная модель с разделением ролей между консалтинговыми фирмами, интеграторами и ресейлерами с добавленной стоимостью больше не работает.

Компании начинают более осознанно подходить к безопасности, разрабатывая индивидуальные решения и контролируя свои системы, вместо того чтобы полагаться на поставщиков.

Все больше организаций ищут партнеров, которые могут предложить комплексные кастомизированные и технически продвинутые решения, охватывающие весь спектр задач по кибербезопасности. Это приводит к устойчивости рынка и увеличению роли поставщиков услуг безопасности полного цикла.

Эксперт по безопасности Брайсон Борт говорит, что безопасность — это наука о данных и для эффективной защиты важен не только выбор инструментов, но и способность управлять данными, используя общепринятые фреймворки для создания гибкой и адаптивной системы безопасности.

РОСТ ЭФФЕКТА ГРАВИТАЦИИ ДАННЫХ

Концепция гравитации данных, предложенная Дэйвом Маккрори в 2010 году, предполагает, что по мере накопления данных в облачных платформах усиливается их «гравитационное притяжение»: сервисы и приложения стремятся переместиться туда, где уже находятся данные.

Компании вроде Snowflake, Google и Amazon активно используют этот эффект, предлагая дополнительные услуги, чтобы захватить рынок и удержать клиентов внутри своей экосистемы.

Стратег Snowflake Омер Сингер подчеркивает, что стартапы в сфере безопасности, сотрудничающие с облачными платформами, получают доступ к широкой клиентской базе и снижают операционные риски, что позволяет экономить и получать конкурентные преимущества.

УСИЛЕНИЕ АРХИТЕКТУРЫ БЕЗОПАСНОСТИ

В последнее время все больше организаций, особенно ориентированных на облачные технологии, переходят к архитектурному подходу в области кибербезопасности.

Исследователь и специалист в области ИБ Фрэнк Вэнг выделяет два ключевых преимущества архитектурных команд безопасности:

- **кастомизацию решений ИБ** — инженеры глубоко понимают задачи, с которыми работают, и способны быстро находить решения;
- **масштабируемость** — они создают решения, которые можно эффективно масштабировать, что особенно важно в условиях стремительно развивающейся ИТ-инфраструктуры.

ДЕМОКРАТИЗАЦИЯ ВЫБОРА ПРОДУКТОВ БЕЗОПАСНОСТИ

По мере роста числа поставщиков решений в области кибербезопасности руководители информационной безопасности (CISO) все чаще делегируют оценку продуктов членам своих команд. Это обусловлено как перегрузкой самих руководителей, так и необходимостью формировать высокоэффективные команды, способные справляться с растущими требованиями к безопасности.

Роль технических специалистов в процессе выбора ИБ-продуктов возрастает: обладая практическим опытом, они лучше понимают реальные потребности организации и способны точнее оценить функциональность предлагаемых инструментов.

Выбор продуктов становится все более демократичным:

- при подходе **сверху вниз** руководители формируют первичный список продуктов для оценки командой;
- при подходе **снизу вверх** инициатива исходит от специалистов, которые предлагают конкретные продукты, исходя из собственных задач и опыта.

Такой комбинированный подход позволяет точнее настраивать системы безопасности под нужды организации.

СБЛИЖЕНИЕ ПРОДУКТОВ И УСЛУГ В КИБЕРБЕЗОПАСНОСТИ

Граница между продуктами и услугами в сфере кибербезопасности постепенно размывается — и в будущем, вероятно, исчезнет совсем. Все больше клиентов ожидают комплексных решений, способных закрывать их потребности в защите.

Компании, традиционно специализирующиеся на услугах, начинают разрабатывать собственные продукты — это позволяет им увеличить маржинальность и улучшить масштабируемость. В то же время продуктовые компании все чаще дополняют свои решения сервисной составляющей, чтобы предоставить клиентам более полное и гибкое покрытие.

Генеральный директор и соучредитель компании Huntress Кайл Ханслован подчеркивает важность гибридного подхода, который сочетает автоматизированные технологии с экспертными знаниями специалистов. Такая комбинация позволяет достигать высокой эффективности и качества — как в глазах клиентов, так и с точки зрения инвесторов.

ОТКРЫТЫЙ КОД КАК МЕТОД ПРОДВИЖЕНИЯ ПРОДУКТА

Отношение к открытому исходному коду значительно изменилось. Если раньше он воспринимался как способ обмена идеями между энтузиастами, то сегодня это подтвержденная коммерческая модель, позволяющая компаниям создавать спрос и зарабатывать.

Проекты с открытым исходным кодом, ранее нерентабельные, теперь успешно применяют различные модели монетизации — от подписок до спонсорства со стороны крупных корпораций. Это позволяет им развивать устойчивый бизнес, масштабироваться и привлекать венчурное финансирование, что ранее считалось невозможным.

В будущем границы между открытым и закрытым кодом в сфере кибербезопасности, вероятно, будут стираться: все больше стартапов используют гибридный подход, совмещая открытость и монетизацию.

По мнению основателя и разработчика nzyme Ленарта Купмана, публикация кода в открытом доступе лишь первый шаг. Чтобы продукт стал успешным на рынке, необходимо инвестировать в качественную документацию, активное продвижение, улучшать пользовательский опыт и предлагать платные услуги, такие как контракты на поддержку. Последние приносят не только доход, но и ценную обратную связь от пользователей.

ПРОДАЖИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В сфере кибербезопасности недопустимы манипулятивные, агрессивные и неэтичные методы продаж, которые подрывают доверие клиентов.

Для долгосрочного успеха необходимо сосредоточиться на понимании реальных проблем клиентов, обеспечить честность и прозрачность маркетинга. Продукты должны быть представлены с четким описанием того, что они могут и не могут делать.

Вместо стандартных методов продаж — холодных звонков или массовых рассылок — все большую роль играют альтернативные каналы коммуникации: формирование профессиональных сообществ, организация мероприятий, ведение подкастов. Эти форматы позволяют устанавливать контакт с аудиторией более органично и устойчиво.

ИЗМЕНЕНИЕ ПОКУПАТЕЛЬСКОГО ПОВЕДЕНИЯ

Большинство руководящих должностей сегодня занимают старшие миллениалы, которые доверяют сообществам и экспертам, а также ценят возможность самостоятельно исследовать и тестировать продукты.

Более молодое поколение часто ориентируется на ценности и этические принципы компаний.

Процесс покупки в ИБ сдвигается к модели, в которой покупатели самостоятельно приходят к поставщикам за решением конкретной проблемы.

Для стартапов и поставщиков это означает необходимость взаимодействовать с сообществами, где обсуждают ИБ-решения, и устанавливать связи с влиятельными фигурами. Кроме того, нужно доносить до потенциальных клиентов информацию об этических стандартах своего бизнеса.

Эксперт в области кибербезопасности, бывший глава исследовательского отдела Tenable Оливер Рочфорд советует уделять больше внимания активному участию в профессиональных сетях.

УПРАВЛЕНИЕ КАДРАМИ В ИБ-СТАРТАПЕ

Для достижения успеха в области кибербезопасности стартапу необходимы:

- **соучредители,** которые разделят ответственность за различные аспекты компании, снизят перегрузку основателей и помогут выработать стратегию;
- **сотрудники,** которые обладают техническими навыками, хорошо разбираются в рыночных трендах, умеют выстраивать доверительные отношения с клиентами и инвесторами.

Все чаще успешные стартапы имеют не двух, а трех или четырех соучредителей. Аккумулирование опыта из разных областей (инжиниринг, разработка, маркетинг, управление) повышает шансы на успех.

Искать соучредителей и сотрудников можно и нужно на отраслевых мероприятиях, а также через рекомендации коллег. В зрелых технологических экосистемах, таких как Кремниевая долина, с подбором ценных кадров для стартапа — от сотрудников до инвесторов — помогают венчурные капиталисты.

Соучредитель и стратег нескольких ИБ-компаний Тед Джулиан отмечает, что при выборе соучредителей и команды важно оценивать людей по их опыту и способности решать реальные проблемы, а не по уровню амбиций и теоретического потенциала.

Молодым стартапам особенно важно отбирать ответственных и готовых к напряженной работе сотрудников.

Автор советует нанимателям четко определять ожидания от сотрудников и давать им возможность профессионального роста. Если стартап развивается в регионе, где нет сформированной экосистемы ИБ, хорошим решением может стать наем удаленных сотрудников. Но при этом обязательно нужно позаботиться об инфраструктуре для эффективного общения и обмена идеями, чтобы команда была на одной волне и имела общую культуру.

Серийный предприниматель в сфере ИБ Энтони Беттини советует искать людей через личные рекомендации, а также нанимать меньше сотрудников, но платить им больше, чтобы снизить управленческие расходы и обеспечить долгосрочное сотрудничество.

ПОИСК РЫНОЧНОГО ФОКУСА

Ключевая задача для стартапа в сфере кибербезопасности — четко определить, для кого он создает продукт. Потребности компаний сильно различаются: крупная международная корпорация с распределенной инфраструктурой сталкивается с иными угрозами, чем небольшая фирма, работающая

на одном локальном рынке. Важно активно взаимодействовать с представителями разных сегментов, чтобы выявить их реальные запросы.

Распространенная ошибка стартапов — ориентация исключительно на технологически продвинутых клиентов, например на облачные компании. Они действительно сталкиваются со сложными задачами, но часто эти задачи нишевые и слабо масштабируемые. Между тем в более традиционных отраслях, таких как банковское дело или розничная торговля, проблемы безопасности не менее актуальны, а уровень подготовки и ресурсов у клиента может быть ниже. Именно здесь открываются возможности для создания востребованных решений.

Стоит различать задачи двух типов:

- «витамины» — решения, которые улучшают ситуацию, но они не критически необходимы;
- «обезболивающее» — решения, без которых клиент не может обойтись.

Успешные стартапы сосредоточиваются на «обезболивающих» — острых проблемах, которые требуют немедленного внимания и при этом имеют очевидную бизнес-ценность для клиента.

Чтобы оценить конкретную задачу с точки зрения ее бизнес-потенциала, можно использовать несколько инструментов:

1) **исследование рынка** — изучать тренды и общаться с профессионалами;
2) **общение с пользователями и покупателями** — создавать и развивать релевантную сеть контактов;
3) **проверка гипотезы** — проводить интервью с 10–25 специалистами, чтобы подтвердить гипотезы;
4) **глубокое изучение** — основательно исследовать проблему, общаясь с 40–50 специалистами.

Важно задавать вопросы, которые помогут понять, как клиенты привыкли решать свои проблемы. Например, вместо «Вы бы использовали наш продукт?» спросите: «Расскажите, как вы решали эту проблему раньше?»

Одна из стратегических ошибок стартапов — ограниченность мышления в выборе проблем. Многие сосредоточены исключительно на вопросах информационной безопасности, в то время как смежные области — конфиденциальность, физическая безопасность, предотвращение мошенничества — остаются в тени. Расширение поля деятельности позволяет не только выйти за рамки конкурентного давления, но и найти новые точки роста. Перспективные направления — от автоматизации бизнес-процессов до применения компьютерного зрения — способны радикально изменить способы решения привычных задач.

ОСОБЕННОСТИ ОБЩЕНИЯ С КЛИЕНТАМИ В ИБ

Общение с клиентами в области кибербезопасности требует подходов, отличных от классического B2C. Здесь не работают механики быстрого роста, эффект вирусности или поверхностное тестирование идей. Успех придет к тем, кто глубоко понимает контекст клиента и готов к длительным циклам продаж.

Стартапам в этой области помогают несколько ключевых принципов:

- **преодоление барьеров доверия.** Установить контакт с клиентами в сфере кибербезопасности непросто: многие перегружены работой и уже сотрудничают со множеством поставщиков. Помогают опросы,

личные встречи и участие в профильных мероприятиях — в таких условиях пользователи более открыты к диалогу;

- **сложный путь клиента.** Продажа решений безопасности — это сложный процесс с несколькими стадиями принятия решений. Важно не упрощать чрезмерно этот путь для клиента и вести его по всем стадиям, начиная с информирования о продукте, через оценку рисков, обсуждение внедрения и поддержки — к покупке;
- **гибкость решений как обязательное условие.** У каждой организации — свой контекст и своя архитектура. Универсальные решения редко работают. Продукт должен легко адаптироваться под разные сценарии применения;
- **фокус на правильную аудиторию.** Не все сегменты рынка одинаково перспективны. Важно определить, где ваши решения будут максимально уместны, и сосредоточиться на этих клиентах;
- **осторожность с опытными пользователями.** Продвинутые клиенты могут требовать специфических функций, которые не нужны массовому рынку. Такие запросы стоит фильтровать, чтобы не перегрузить продукт;
- **систематический сбор обратной связи.** Обратная связь от клиентов — ключ к развитию. Ее должна собирать не только служба поддержки, но и все команды: продуктовая, продажи, маркетинг.

МЕЖДУНАРОДНЫЕ ОТРАСЛЕВЫЕ МЕРОПРИЯТИЯ

Такие события, как **BSides и DEF CON**, предоставляют возможность выступить с докладом и продемонстрировать экспертность компании, что способствует установлению доверительных отношений с клиентами. Это особенно важно для стартапов с ограниченным бюджетом: участие в крупных конференциях может быть дорогостоящим, тогда как локальные и нишевые мероприятия открывают возможности для обучения, расширения команды и обмена идеями.

Для стартапов, ориентирующихся на **руководителей служб информационной безопасности (CISO),** полезными могут быть конференции вроде **Gartner Summit или Forrester Security & Risk.** Они позволяют лучше понять потребности и болевые точки целевой аудитории. Несмотря на высокую стоимость участия, эти мероприятия могут оказаться оправданными, если удастся выступить с докладом: это не только снижает затраты (бесплатный проход), но и укрепляет позиции компании на рынке. А для тех, кто не готов тратиться на билет, неформальные встречи и обсуждения в кафе и кулуарах тоже могут стать эффективным инструментом нетворкинга.

RSA Conference (RSAC) — одно из крупнейших событий в сфере кибербезопасности, ежегодно собирающее более 45 тысяч участников. Участие может быть дорого, но у стартапов есть способы снизить затраты. Среди них — участие в **RSAC Early Stage Expo** или конкурс **RSAC Innovation Sandbox**, где можно представить свой продукт широкой аудитории и получить признание отрасли.

ПРИЧИНЫ НЕУДАЧ ИБ-СТАРТАПОВ

Есть несколько типичных ошибок, которые приводят к краху стартапов в сфере кибербезопасности:

1. **Слабый менеджмент.** Предприниматели, которые начинают свою карьеру с работы с продуктами и инструментами безопасности, могут слишком фокусироваться на продукте, забывая о таких важных аспектах строительства бизнеса, как управление кадрами, маркетинг и отношения с инвесторами.
2. **Незнание контекста отрасли.** Рынок кибербезопасности сложен, и предприниматели должны понимать, как взаимодействуют регулирование, венчурный капитал, правовой ландшафт и партнерские каналы. Важно отлично понимать и сферу применения продукта: стартап, ориентирующийся на банковскую отрасль, может столкнуться с совершенно иными проблемами, чем те, кто работает с облачными компаниями.

General Magic предложила прототипы смартфонов в 1990-е, когда сети передачи данных были слабыми, а технологии — дорогими. Поэтому отличная разработка провалилась из-за недостатка покупателей.

3. **Непонимание рынка.** Предложение продукта должно быть своевременным, не слишком ранним и не слишком поздним.
4. **Слабая бизнес-модель.** Раннее моделирование и тестирование гипотез монетизации критично для долгосрочной устойчивости.
5. **Игнорирование реальных потребностей клиентов.** Многие стартапы привлекают инвестиции, нанимают большие команды и начинают масштабироваться, не убедившись в том, что их продукт полностью соответствует требованиям и целям клиентов. Стартапы, которые стремятся создать «единую систему управления», часто делают слишком сложные продукты и терпят неудачу.

Решения о покупке ИБ могут принимать не только специалисты по безопасности, но и другие ключевые фигуры, такие как IT-руководители или менеджеры по рискам.

6. **Отсутствие маркетинговой стратегии.** Часто основатели ошибаются, полагая, что продукт будет продаваться сам по себе, и не имеют ни маркетинговой стратегии, ни портрета потребителя.
7. **Знак равенства между продажей инвесторам и продажей клиентам.** Если стартап успешно привлекает инвестиции, это не значит, что он будет так же успешен у корпоративных потребителей, которые ищут решение для текущих задач. Как отмечает эксперт по кибербезопасности Фрэнсис Одум, успешные компании не только предлагают качественные продукты, но и разрабатывают эффективные механизмы выхода на рынок.

ВРЕМЯ ДЕЙСТВОВАТЬ

Сегодня индустрия кибербезопасности находится на пороге изменений. Стартапы, способные не просто предугадывать будущее, но и активно его формировать, имеют все шансы занять значимые позиции на рынке. Ориентация на реальные потребности, фокус на ценности, готовность к нестандартным шагам и экономическая устойчивость — вот что делает такие компании востребованными. Это открывает возможности не только для крупных игроков, но и для малых и средних команд, способных делать эффективные продукты без громоздкой структуры и избыточных ресурсов.

10 ЛУЧШИХ МЫСЛЕЙ

1.
Рынок кибербезопасности имеет сложный ландшафт, в котором стартапы отвечают за инновации, а крупные компании — за интеграцию и масштабирование.

2.
С инвесторами необходимо работать на всем цикле развития бизнеса стартапа, рассказывая им об успехах и наиболее значимых результатах.

3.
Привлекая финансирование, важно сохранять фокус на создании продукта и жизнеспособного бизнеса, а не на пожеланиях инвесторов.

4.
Инвесторы могут помочь стартапу не только деньгами, но и ценными связями, кадрами и практическим опытом.

5.
Продукт, который разрабатывает стартап, должен решать реальные и острые проблемы клиентов. Обезболивающее легче продать, чем витамины.

6.
Для успешного продвижения стартапу нужно поддерживать связи с инфлюенсерами: отраслевыми аналитиками, госрегуляторами и страховыми компаниями.

7.
Партнеры, через которых стартап может получить доступ к клиентским бюджетам, — это стратегические консультанты, ресейлеры, интеграторы, поставщики услуг в области ИБ.

8.
Для успеха стартапу необходимы соучредители с опытом в разных сферах и ответственные, динамичные кадры, которых можно найти по рекомендациям или на отраслевых мероприятиях.

9.

Продажи в сфере кибербезопасности — сложный и длительный процесс, в основе которого лежит создание доверия клиента к поставщику.

10.

Для успеха стартапу нужен не только классный продукт, но и сильная бизнес-модель и внятная стратегия роста.