УДК 338.24

О. В. Одаренко, ст. преп. (КУБГ, г. Киев, Украина)

РЕПУТАЦИОННЫЕ РИСКИ СТАРТАПОВ

Репутационные риски являются ныне одними из наиболее весомых и значимых в риск-спектре компаний. Современный бизнес все более и более становится зависимым от так называемых «новых рисков», продуцируемых экономикой 4.0. Отличительной особенностью «новых рисков» является их нетрадиционный характер. Возникают риски, связанные с поколением миллениалов, составляющих в настоящее время значительную часть потребительской аудитории, например, продукции IT-сектора. Бизнес, даже высокотехнологический, зачастую оказывается не готов к принятию / минимизации «новых рисков» и превращения их в новые возможности. Пренебрежение репутационными рисками в эпоху публичности вполне способно привести компанию к кризису, что в условиях экономической неопределенности может существенно ослабить конкурентные позиции на рынке.

Наиболее ярко влияние репутационных рисков проявляется в стартапах. Под стартапом будем понимать определение Стива Бленка: «Стартап – это организация, созданная для поиска повторяемой и масштабируемой бизнес-модели» [1]. Высокие риски обеспечивают стартап-проектам высокую доходность. Но, в то же время, по утверждению одного из практиков бизнес-акселерации Д. Довгополого, 99, 7% компаний-стартапов становятся банкротами в первый же год существования [1]. Как правило, банкротство стартапов наступает из-за низкой доходности, недостаточности / нерегулярности инвестиций, отсутствия «портфельной» стратегии, расфокусировки проекта [1]. Все перечисленные Д. Довгополым причины банкротства являются актуальными и для компаний, давно присутствующих на рынке. Однако в условиях экономической неопределенности и турбулентности внешней среды, компании становятся зависимыми от событий вне прогнозов – «черных лебедей» по Н. Талебу. Репутационные риски, продуцируемые «человеческим фактором» очень часто играют роль «черных лебедей».

Репутационные риски сопровождают стартапы с момента появления самой идеи проекта. Очевидно, что всегда найдется кто-то – человек или группа лиц, кому идея покажется неприемлемой с этической, религиозной, политической или иной точки зрения. О влиянии стартап-неудач на репутацию бизнесмена исследователи и практики спорят. С одной стороны, неудачный проект всегда связывают с конкретным именем инициатора / исполнителя (в компании с «историей» репутация топ-менеджера становится серьезным нематериальным ак-

тивом), а с другой – стартап-неудача заставляет бизнес-игроков тщательнее проверять гипотезы проекта, тщательнее определять потенциальную аудиторию и партнеров / инвесторов / акционеров.

На основании анализа научной литературы и практики риск-менеджмента, а автор тезисов достаточно длительное время занимается проблематикой риск-менеджмента в компаниях рынка телекоммуникаций, выделим наиболее существенные репутационные риски стартапов. Это:

- Провокационность идеи с точки зрения устоявшихся нор морали, религии, политики, десйтвующих в данном регионе.
- Пренебрежение нормами действующего законодательства, прежде всего, в сфере налогообложения.
- Пренебрежение политикой обработки персональных данных (Privacy Policy) в частности, «правом на забвение» в отношении инвесторов / клиентов.
- Пренебрежение информационной безопасностью / защитой корпоративных сетей.
- Пренебрежение кадровой политикой, в частности, партнерскими взаимоотношениями.
- Невнимание к техникам социальной инженерии, которые могут быть использованы против сотрудников компании.
- Низкий уровень коммуникативных связей в команде стартапа.
- Нарушение принципа «знай своего клиента» / неточности в «портрете клиента».
- Отсутствие публичной коммуникации.
- Отсутствие / низкий уровень GR.
- Утаивание информации о кризисах / отсутствие антикризисного плана.
- Отказ от использования современных методов построения доверия в бизнесе.

Отдельно следует отметить, что пренебрежение / низкий уровень кибербезопасности является системным фактором, продуцирующим разнообразные репутационные риски. «Эксперты чаще всего среди главных ошибок предпринимателей, связанных с кибербезопасностью, называют следующие.

Первая – слишком несерьезное отношение к этой проблеме.

Вторая – неправильная оценка рисков. Вы спросите, что может случиться с небольшой компанией? Хищение денег в системе интернет-банкинга, остановка работы инфраструктуры путем саботажа (используя вирус-шифровальщик), кража коммерческой тайны, подмена информации, майнинг на серверах, угрозы сотрудникам, рассылка спама с принадлежащих компании компьютеров или, еще хуже, ис-

пользование компьютеров для участия в каких-то промежуточных атаках – это сильно подставляет компанию и несет угрозу ее репутации. Но если защищаться от всех угроз сразу, придется работать только на оборону, забывая о клиентах. Поэтому необходимо сортировать проблемы по степени их критичности.

Здесь возникает **третья**: из-за неправильной оценки рисков многие фирмы покупают ненужное оборудование или делают то, чего делать не нужно, и это приводит к бессмысленной трате финансовых и временных ресурсов.

Четвертая – забывать о том, что главное звено в кибербезопасности – человек. Сотрудник может нажать на опасную ссылку в письме, вставить не ту флешку, забыть что-то проверить. Поэтому необходимо обучать кибербезопасности всех сотрудников, а не полагаться на IT-специалистов.

Пятая – нельзя думать, что компьютерная безопасность заканчивается на событии "я нашел вирус, я его удалил". Вы удалили вирус на своем компьютере, но не стоит забывать, что он попал в ваше устройство с какого-то сервера. И этим сервером управляет человек, который продолжает рассылать этот и другие вирусы на множество других компьютеров. Не факт, что следующий вирус вы тоже обнаружите. Помните, что для успешной кибератаки на всю ИТ-инфраструктуру компании достаточно одного уязвимого телефона, подключенного к корпоративной сети. У каждого сотрудника на рабочем месте есть как минимум одно личное устройство» [2].

В этой связи актуальным становится умение видеть не одну возможность, а целые потоки возможностей. Уместным является применение стратегии превращения рисков в преимущества, что позволяет своевременно осуществлять upgrade (обновление) целей и задач компании, а также ее управленческих стратегий, бизнес-процессов и технологических циклов. Инвестиции в анализ рисков должны стать приоритетными для компании.

ЛИТЕРАТУРА

1 Довгополый Д. 99,7% неудач стартапов: мифы и реальность // Д. Довгополый [Текст] // [Электронный ресурс]. – Режим доступа: http://www.e-c-m.ru/jour/article/view/292/292, свободный. – Назв. с экрана (дата обращения: 13.01.2020).

2 Кравченко В. Бизнес 5.0: как построить успешный стартап или компанию, игнорируя риски кибербезопасности / В. Кравченко [Текст] // [Электронный ресурс]. – Режим доступа: https://delo.ua/business/biznes-50-kak-postroit-uspeshnyj-startap-ili-k-355171/, свободный. – Назв. с экрана (дата обращения: 13.01.2020).