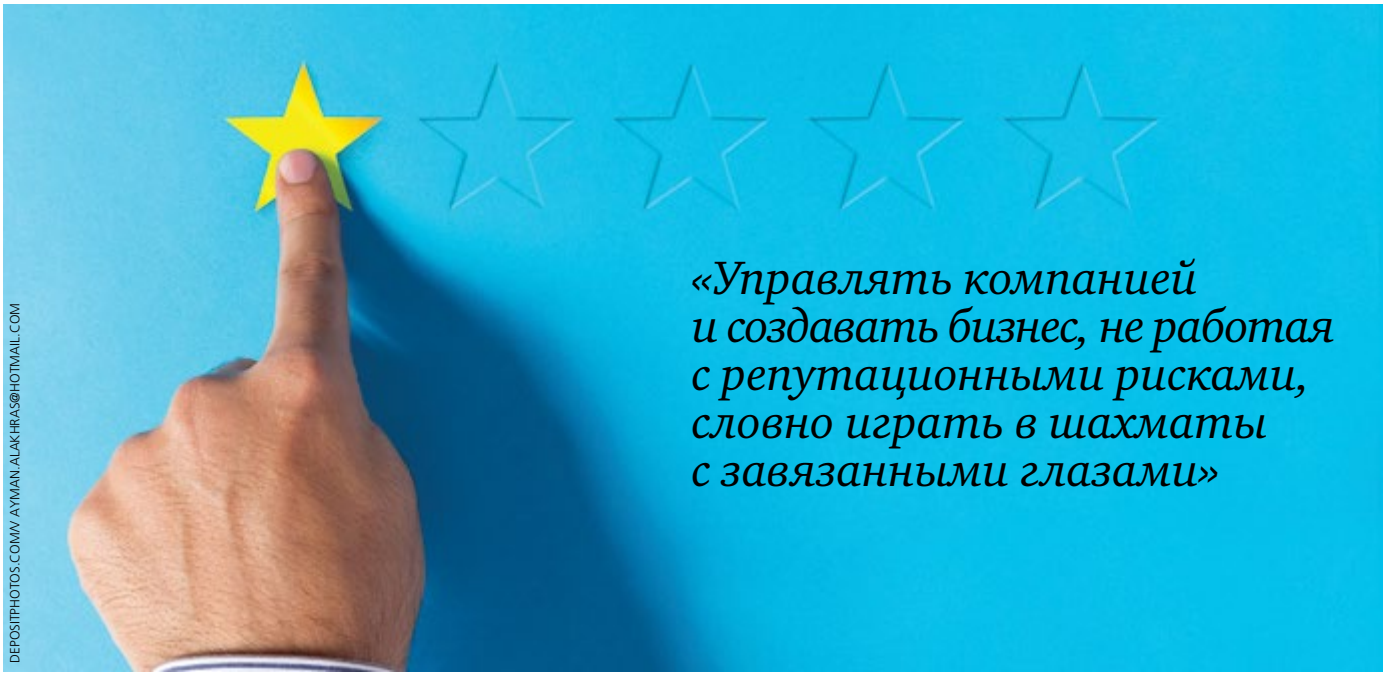
АННА КУЛИК,
Президент АНО НИЦКБ

Информационные войны и репутационные риски



«Управлять компанией и создавать бизнес, не работая с репутационными рисками, словно играть в шахматы с завязанными глазами»

DEPOSITPHOTOS.COM/V AYMAN.ALAKHRAS@HOTMAIL.COM

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ с самого начала деятельности одним из направлений изучения ставил перед собой вопрос прогнозирования, выявления и профилактики репутационных рисков (далее РР), ведь, зачастую становясь основой вектора информационной атаки на компанию, они являются причиной значительных убытков. Сам по себе тот или иной РР вреда не несёт, поскольку является лишь инструментом, элементом информационной атаки. Репутационный риск, как угрозообразующий фактор, может сопровождать деятельность компании на протяжении многих лет, это совершенно не значит, что о его существовании не нужно помнить и работать с ним.

Полагаю, это допустимо сравнить со «спящими разведчиками-нелегалами». Они могут находиться в чужой стране всю жизнь и так и не получить ни одного задания, но любое государство предпринимает колоссальные меры для их обнаружения и обезвреживания или контроля. Иллюстрацией данного тезиса служит волна «общественных проверок» торговых центров, прокатившаяся по городам России после трагедии в Кемерово. Проблемы с соблюдением правил пожарной безопасности существуют у всех, но до того периода они волновали разве что проверяющего. Как только они были преданы гласности, возникли соответствующие угрозы репутации

В таких ситуациях одну из ведущих ролей в профилактике и ликвидации последствий, по мнению опрошенных в ходе исследования, могут сыграть PR-службы компании, системно занимающиеся восприятием бренда. Таким образом, предупреждение репутационных рисков без участия данной категории специалистов не представляется возможным. При этом противодействие разворачивающейся информационной атаке не может быть эффективным без использования компетенций, которыми обладают сотрудники службы безопасности, способные отследить и установить организаторов и исполнителей, юридических отделов, обеспечивающих законность контрмер и выявляющих нарушения действующего законодательства со стороны оппонентов, и других заинтересованных подразделений компании.

Вместе с тем выявление и предупреждение репутационных рисков затруднено отсутствием их полноценного теоретико-научного осмысления, классификации, выделения признаков и детерминант. В ходе исследования было предложено выделить две категории рисков:

Внутренние: недовольные сотрудники, коммерческий подкуп, неэтичное поведение руководства и топ-менеджмента, ребрендинг/слияние, некачественный товар или услуга.

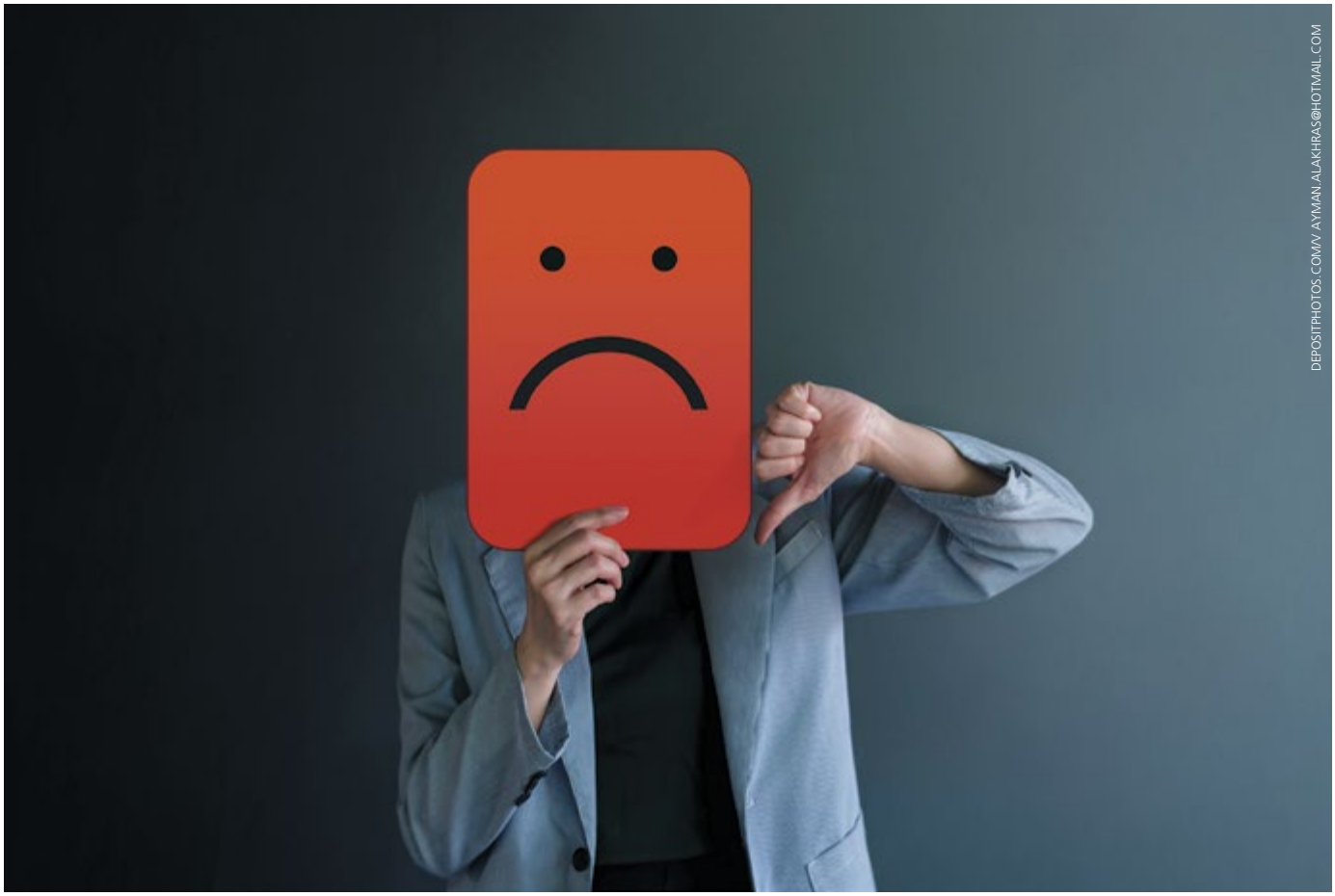
Социальные сети используются не только для поиска информации, но и для ее распространения. Так считают 87% опрошенных в ходе исследования

Внешние: атака конкурентов, недовольные клиенты, непроверенные провайдеры/подрядчики, давление со стороны контролирующих органов, давление на сферу в целом.

Модели использования данных категорий «уязвимостей» для организации информационной атаки отличаются, а значит, определив, к какой группе относится PP, можно прогнозировать развитие ситуации, используемые средства, в некоторых случаях возможно определить источник угрозы и конечную цель.

Так одной из наиболее распространенных сегодня угроз по-прежнему является утечка конфиденциальной информации. Чаще всего первое, в чем столкнувшиеся с такого рода проблемой видят проблему, – это вмешательство в работу технических средств связи и обработки информации. Однако стоит отметить, что первичную роль в утечке данных в подавляющем большинстве играют сотрудники, делая это осознанно или по халатности. В практике корпоративных расследований встречаются случаи, когда сотрудник сделал фотографию на рабочем месте, на которой в кадр попали документы, содержащие сведения ограниченного доступа, и выложил ее на своей странице в социальной сети. После этого данная публикация была обнаружена конкурентом, а информация использована для организации атаки. Важно отметить, что социальные сети используются не только для поиска информации, но и, как считают 87 % опрошенных в ходе исследования, для ее распространения при подготовке и проведении информационной атаки. Очевидный на первый взгляд вывод в действительности таковым не является. Инструментарий информационных войн необычайно широк и все время пополняется новыми видами «вооружений». Так еще совсем недавно первое место заняли бы сервисы микроблогов.

Стоит оговориться, что сегодня уже непросто понять, как осуществлялся трансферт технологий информационных войн – из политики в бизнес, или наоборот, но модели, характерные для взаимоотношений отдельных политических деятелей и целых стран, используются и в корпоративном секторе, хотя и менее открыто. Одновременно с этим в ходе исследования выявлены отличия между «войнами» в малом и крупном бизнесе. Неправильно организованная атака на конкурента сама по себе может стать для крупного игрока репутационным риском, что заставляет корпоративных гигантов прибегать к таким методам нечасто и довольно аккуратно. А вот «деликатные» материалы в отношении ТОП-менеджера компании могут стать реальной угрозой. В малом бизнесе ситуация выглядит иначе. Конкуренты зачастую используют неэтичные и не всегда законные методы.



Таким образом, допустимо озвучить одну из гипотез, сформулированных в результате работы над исследованием: малый бизнес чаще подвергается воздействию внешних репутационных угроз, в то время как крупный чаще всего становится жертвой внутренних рисков. Однако это лишь тенденция, которая не исключает и других сценариев развития событий, поскольку виды репутационных рисков в разных компаниях схожи, а вот информационные атаки, базирующиеся на них, всегда разные.

Более того в практике встречаются случаи, когда репутационным риском становится подрядчик. Так в результате аудита состояния репутации крупной FMCG компании было установлено, что служба безопасности пользуется услугами «консалтингового агентства», которое в свою очередь публично заявляет о своем взаимодействии. Однако данное «агентство» в открытых источниках распространяет перечень предоставляемых услуг, среди которых взлом корпоративных сетей, перегрузка колл-центров конкурентов, различного рода проверки сотрудников. Вместе с тем в качестве примеров используются отчеты, которых приводятся неизмененные установочные данные проверенных лиц. Избегая лишних подробностей, отметим, что проиллюстрировать наличие связи приведенной выше крупной компании с этим «консалтинговым агентством» не составляет труда, что это дает возможность обвинить их клиента в использовании не вполне законных методов работы с персоналом.

Репутация – один из главных активов, а угроза репутации – риск серьезных финансовых потерь

Таким образом, предпринята попытка классификации репутационных рисков, выявления их особенностей, признаков и методов профилактики и противодействия. Одновременно с этим изучены некоторые инструменты и тактики организации информационных атак, рассмотрены приемы их нивелирования. Важной составляющей исследования стали обобщение полученных сведений, подготовка методических рекомендаций и проведение обсуждений результатов с участием специалистов и экспертов в различных областях научной и профессиональной деятельности. Практика проведения подобных прикладных исследований представляется эффективным способом выработки и совершенствования технологий обеспечения бизнеса. ●