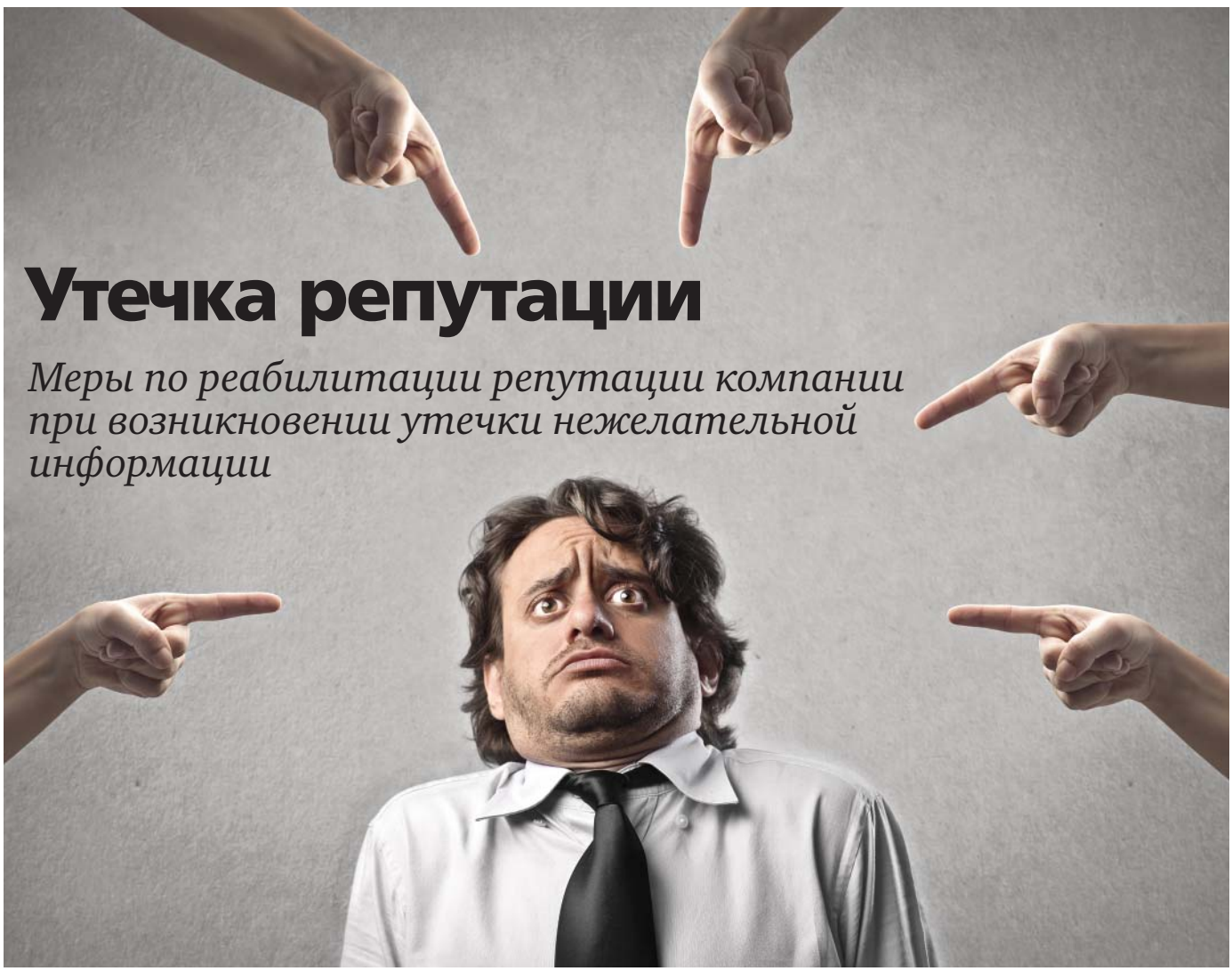
ОЛЬГА ДЫБОВА,
учебный центр «Информзащита»



Утечка репутации

Меры по реабилитации репутации компании при возникновении утечки нежелательной информации

Данные разной степени конфиденциальности утекают из компаний достаточно часто, но об этом знают только ИБ-специалисты (да и то не все и не в 100 % случаев). Информация же об утечке доходит до высшего менеджмента компании и пиарщиков чаще тогда, когда эта самая утечка становится более-менее очевидной. Лучший вариант – когда о факте говорит сотрудник ИБ-подразделения, самый наихудший – когда топ-менеджер узнает подобные новости из внешних источников, например после прочтения утренних газет.

Об очевидных утечках мы и поговорим, отталкиваясь от того, что они могут быть:

- преднамеренными и непреднамеренными;
- бьющие по «кошельку», репутации и нервам или только по «кошельку»;
- которые стали известны благодаря специалистам компании и которые стали известны из внешних источников.

Сначала о преднамеренных и непреднамеренных: статистика некоторых вендоров говорит о том, что большинство утечек – около 80 % – носят все-таки непреднамеренный характер. Например, неопытная секретарша разместила в своем инстаграмме фото из серии «Я вся такая красивая в ресторане на переговорах с шефом и кем-то еще». С одной стороны, ничего особо страшного в этом нет. За исключением случаев, если супруга шефа неадекватна и ревнива, а также если этот «кто-то еще» является тем человеком, общение с которым может быть интересно конкурентам вашей компании, например.

Совершенно очевидно, что любая утечка информации бьет не только по репутации компании, но еще и по «кошельку», причем прежде всего. Если о

факте утечки узнали все, кому об этом лучше бы не знать, то восстановление репутации может быть самым дорогим инструментом из всего комплекса восстановительных мер.

Вообще неплохо, чтобы в компании был предусмотрен примерный план, как реагировать на ту или иную утечку информации в зависимости от ее категории. Может быть, это и звучит немного непривычно, но наличие подобного плана поможет быстрее понять, что произошло и что делать.

В плане должны быть отражены нижеизложенные моменты.

- Аналитика инцидентов, понятная не только специалистам по ИБ.
- Критичность утечки, т. е. какой степени конфиденциальности произошла утечка. Для этого нужно заранее категорировать информацию по важности и критичности для бизнеса.
- Преднамеренность или непреднамеренность утечки. Как говорилось выше, большинство утечек носит непреднамеренный характер. И если еще несколько лет назад было достаточно выстроить систему контроля периметра, то сейчас это становится все сложнее и сложнее. Связан сей факт с проникновением в нашу жизнь социальных сетей, а также мобильных устройств – в корпоративные сети. Самый простой пример – почта на телефоне. Или фотоаппарат на смартфоне: делаем фото документов, тут же на смартфоне распознаем их – и вот готовая утечка. Самый частый случай – пересылка себе на некорпоративную почту для «поработать дома». Или сотрудник взял и сохранил документы на публичном «облаке» и не выставил правильных настроек приватности.
- Следующий шаг чрезвычайно важен. Необходимо оценить юридические последствия утечки и опубликования информации об этой утечке. Есть ряд утечек, о которых вы должны информировать по закону. Например, это утечка персональных данных или данных о банковских карточках. Кроме того, нужно понять, будет ли нести компания прямой юридический ущерб, например иски, в случае, если информация об утечке будет публично доступна. Также нужно знать, несет ли кто-нибудь юридическую ответственность за утечку. Например, если вы – представитель банка или другая структура, имеющая сертификат PCI DSS, то часть ответственности можно смело переложить на аудитора. Но все же самый первый шаг – это обращение в правоохранительные органы. Ведь при развитии ситуации по самому плохому варианту всегда можно апеллировать к тому, что утечка уже расследуется.
- Хорошо, если можно посчитать прямой экономический ущерб. Правда, это не всегда возможно сделать.
- И вот мы подходим к вопросу репутации. Если вы обязаны публиковать данные об утечке, то лучше это сделать в максимально короткие сроки. Лучше, если клиенты и партнеры узнают это от вас, чем от СМИ или от кого-либо еще. Сообщение должно быть лаконичным и без эмоций – это важно: произошло то и то, об этом заявлено куда надо, виновные найдены, меры усилены, выводы сделаны.
- Если вы не должны публиковать информацию, то нужно понять, будет ли известие об инциденте публично доступно. Если вы на 120 % уверены, что информация об утечке не уйдет дальше стен вашего кабинета, то, по сути, ничего делать не нужно. Разве что принять меры по отношению к «безопасникам» и сделать соответствующие выводы, чтобы подобное не повторилось. Если же вы уверены на 100 % в неразглашении утечки, но при этом вас терзают смутные сомнения, или не уверены вовсе, то лучше перестраховаться и привлечь к работе пиарщика и юриста.

Несколько слов о работе специалиста по связям с общественностью: если вы понимаете, что ваш пиарщик в состоянии выполнять только технические функции, например писать релизы, делать мониторинг прессы и оформлять документы после проведенных выставок, то к разрешению ситуации лучше привлечь рекомендованное пиар-агентство. Это будет стоить дорого, но того стоит.

- Если вы узнаете информацию об утечке каких-либо данных родной компании из СМИ, к коим в данном случае можно причислить не только утренние газеты, но и социальные сети, то здесь дело обстоит сложнее. Но главное – не нервничать и не совершать резких движений. Имеет смысл начинать действовать с третьего пункта нашего плана: понять, по каким причинам произошла утечка. Далее – обращение в правоохранительные органы. Некоторые умудряются параллельно «наехать» на СМИ с целью отозвать публикацию. Так вот, этого никто из журналистов не сделает, более того, расскажут о вашей компании еще раз и не в самом выгодном свете.

Хорошо, если можно посчитать прямой экономический ущерб. Правда, это не всегда возможно сделать

Некоторые отрицают факт утечки. Если утечка действительно произошла, то отрицать ее не имеет смысла.

Самый первый комментарий для СМИ, клиентов и партнеров должен быть о том, что по факту утечки идет расследование и о его результатах будет сообщено дополнительно. Если эта утечка критична и несет юридические последствия, то лучше публично информировать о ходе расследования, может, даже завести специальный сайт или отдельную страничку на уже существующем сайте компании. Подобная открытость поможет добиться расположения клиентов, партнеров и представителей СМИ и, как следствие, сохранить репутацию. ●