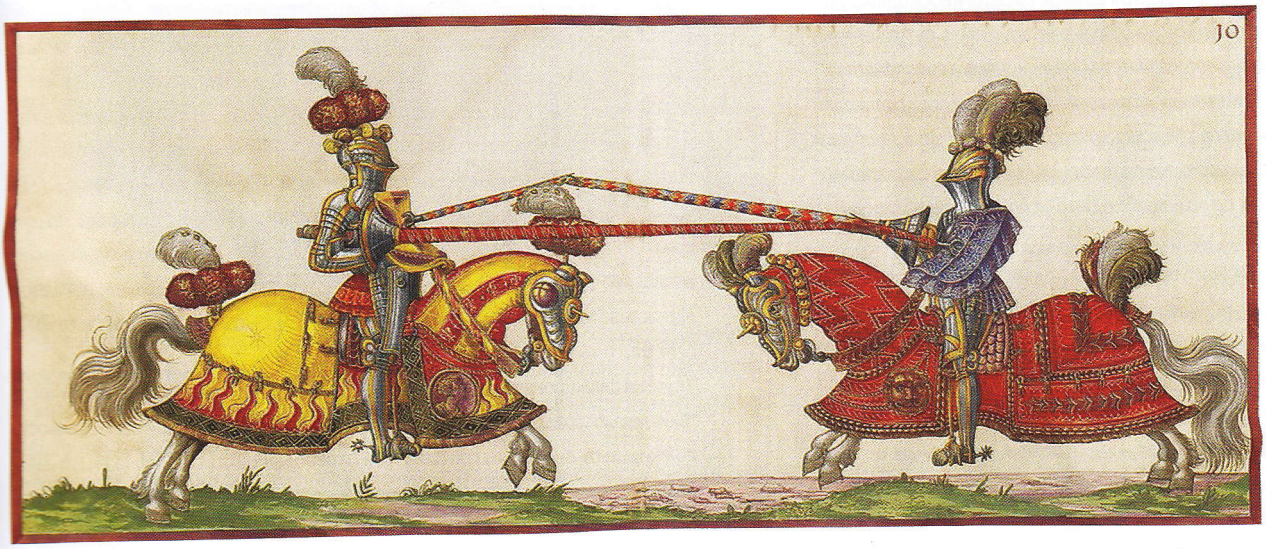
Аудит безопасности — инструмент оценки рисков

Леонид МЕДВЕДЕВ, автор и разработчик курсов по транспортной и объектовой безопасности учебного центра «Информзащита»



Современный мир характеризуется чрезвычайно высоким темпом жизни, а современный бизнес — чрезвычайно высокими темпами изменения ситуации. А вместе с изменением ситуации, как правило, меняются угрозы и риски, связанные с ведением бизнеса. Для борьбы с угрозами и рисками бизнес создает и развивает службы безопасности, которые, как это ни парадоксально, являются в компаниях самым костным и инертным механизмом.

Я, наверное, не открою секрета, если скажу, что большинство существующих служб безопасности чаще всего реагируют на появившуюся угрозу после ее реализации. Это как извечное соревнование меча и щита. Появился новый меч, начинаем дорабатывать существующий щит, но уже после того, как новый меч проделал в старом щите дыру. И хорошо, если только в щите, а не в хозяине этого самого щита. Некоторые сотрудники служб безопасности чаще всего готовятся к уже минувшим сражениям, так как используют для подготовки знания и опыт, полученные в результате анализа уже прошедших событий. Зачастую они абсолютно не готовы к отражению новых угроз и предотвращению новых рисков. Преступники же, изучая прошлые попытки, анализируют существующие средства защиты и стараются каждый раз придумать что-то новое. Что-то, не учтенное существующими системами безопасности.

Помимо внешних угроз сотрудникам служб безопасности приходится бороться и с внутренними. Практика показывает, что иногда в числе подобных угроз оказывается тот самый бизнес, который служба безопасности вроде как должна защищать и оберегать. Как такое может быть? Очень просто. Например, на предприятии сменили технологию производства, забыв предупредить об этом службу безопасности. А в новой технологии, к примеру, применяется питьевой спирт, которого в старой технологии не было. Службу безопасности в известность не поставили — вроде бы какое им дело до производства закупок. В результате не был организован должный контроль за спиртом, кто-то из сотрудников предприятия добрался до заветной емкости, злоупотребил, результатом чего стал несчастный случай на производстве. Это вполне реальная история, произошедшая не так давно в довольно известной компании. Еще один пример. В компании произошла модернизация компьютерной сети. Модернизацию не согласовали со службой безопасности компании. В результате сеть получилась современной, быстрой, продвинутой и... дырявой. В компании началась утечка конфиденциальной информации, убытки составили впечатляющую сумму с большим количеством нолей. Расследование, конечно, выявило и дыры в системе сетевой безопасности, и сотрудников компании, по вине которых произошла утечка. Но все это выявилось постфактум, а к сумме непосредственного ущерба от утечек информации добавилась сумма на экспертизу сети и ее доработку.

Подобных случаев можно привести множество. Объединяет все эти случаи всегда одно и то же: сначала реализация риска, потом поиск методов борьбы с выявленным риском и только потом затыкание обнаруженных дырок в системе безопасности.

Неправильность подобного подхода, на мой взгляд, очевидна. Инструмент, позволяющий службе безопасности стараться работать на опережение, существует уже давно и называется аудит систем безопасности. Вот только, как показывает практика, если в бизнесе проведение аудиторских проверок — явление вполне естественное, более того, часто регулируемое законодательно, то в подразделениях безопасности от слова «аудит» чаще всего шарахаются как черт от ладана. Это не значит, что безопасники стараются жить бесконтрольно. Проверки как плановые, так и внеплановые в службах безопасности — явление весьма распространенное, учения проводятся, ведется строгий учет, в том числе и выявленных недостатков. Вроде бы все и без аудита хорошо. Мне не раз и не два приходилось сталкиваться с резко отрицательной реакцией аудитируемой службы. Если коротко, их реакцию можно охарактеризовать фразой: у нас все нормально, не нужно лезть в наш огород.

Но ведь аудит — это не только проверка того, что есть. Если мы с вами откроем Гост Р ISO 19011-2012 (Руководящие указания по аудиту систем менеджмента) главу 4 «Принципы проведения аудита», то увидим, что аудит — это не только механизм контроля. В первую очередь это механизм, позволяющий последовательно улучшать деятельность организации, в нашем случае службы охраны. А что является первоочередными задачами, когда мы говорим про улучшения в работе подразделения службы охраны? Никакое улучшение в системе безопасности невозможно без проведения оценки угроз и рисков.

Во всех западных, да и во многих российских компаниях внутренние аудиты уже давно стали естественным, а зачастую и обязательным явлением. Более того, в большинстве западных компаний аудит второй стороны является обязательной процедурой при заключении практически любого контракта. Навыками проведения аудитов в таких компаниях владеют не только менеджеры, но и специалисты. А при чем тут безопасность, спросите вы? Простой пример: компания «А» хочет заключить договор о предоставлении логистических услуг с компанией «Б». В перечень логистических услуг входит хранение и перевозка сырья, принадлежащего компании «Б». Вполне естественно, что перед заключением контракта компания «Б» инициирует аудит второй стороны. В числе прочих перед аудиторами стоит задача оценить безопасность хранения и перевозки своего сырья. То есть провести аудит объектовой безопасности и транспортной безопасности.

Или, к примеру, компания «С» хочет взять в аренду у компании «Д» строительную технику. А строительная техника, как известно, у злоумышленников пользуется повышенным спросом. То есть риск хищения этой самой техники достаточно высок. Конечно, частично риски покрываются страховкой. Но, во-первых, между страховым случаем и моментом выплаты страхового возмещения, как правило, проходит довольно много времени, а во-вторых, довольно часто оказывается, что суммы, выплаченной по страховке, на покупку новой аналогичной техники просто не хватает. В подобных ситуациях аудит второй стороны как инструмент минимизации рисков очень эффективен. Оценив уровень безопасности на объектах компании «С», менеджеры компании «Д» имеют возможность при заключении договора аренды не только закладывать материальную ответственность арендатора, но и юридически оговаривать организацию необходимого уровня безопасности арендованной техники.

Вроде все логично. Аудит — процедура не только обязательная, но и полезная. Внутренний аудит позволяет своевременно выявлять новые угрозы и риски, постоянно улучшать и совершенствовать работу служб и подразделений безопасности. Аудит второй стороны позволяет повысить безопасность сделок и минимизировать риск возможных убытков. Так почему же на практике руководство многих охранных подразделений встречает идею аудита в штыки?

Ни для кого не секрет, что в большинстве компаний руководство служб безопасности — это либо бывшие военные, либо бывшие сотрудники правоохранительных органов, специальных подразделений и т. п., вышедшие на пенсию по выслуге, как правило, в больших чинах. Теперь представьте, что проводить аудит второй стороны на фирму, где руководитель службы безопасности — генерал на пенсии, приезжает менеджер или специалист компании-партнера. Молодой парень или девушка, зачастую не служившие в армии, не нюхавшие пороха. При этом они опытные аудиторы и, даже не будучи специалистами в области безопасности, но в совершенстве владея процедурой проведения аудита, находят в существующей системе безопасности предприятия какие-либо уязвимости и, фигурально выражаясь, тыкают в них носом целого генерала. И ладно, если выявленная уязвимость небольшая и обусловлена изменившимися внешними условиями. Бывает и так, что результатом аудита оказывается полное несоответствие системы безопасности предприятия существующим в настоящий момент угрозам и рискам. И если с выявленными небольшими недостатками руководство службы безопасности еще как-то готово мириться, то приговор всей существующей системе чаще всего воспринимается крайне негативно. Мне известны случаи, когда из-за подобной неконструктивной позиции руководства служб безопасности срывались очень крупные и выгодные контракты. Более того, в моей практике было несколько случаев, когда выявленные в процессе аудита второй стороны уязвимости из-за позиции неприятия критики руководством служб безопасности впоследствии наносили крупный ущерб для этой компании. Причем ущерб в подобных ситуациях очень часто оказывается не только материальным, но и репутационным.

Говоря про проведение аудита, нельзя не коснуться морально-этической стороны вопроса. Морально-этический аспект, как ни странно, при рыночных отношениях значительно важнее для репутации любой организации, чем это было при планово-административной системе. Репутация организации на рынке, как известно, оценивается той же суммой, которая складывается из цен всех договоров в портфеле заказов этой организации. Строго говоря, именно объем портфеля заказов равен цене репутации организации. Это в полной мере относится к репутации заказчиков и к тем организациям, которые от имени заказчика проводят аудиты второй стороны.

Рассмотрим два процесса, которые с процедурной стороны очень похожи, чего нельзя сказать о морально-психологической стороне вопроса. Первый процесс — внутренний аудит по системе менеджмента качества на основе стандарта ISO 9001:2000 (ГОСТ Р ИСО 9001-2001); второй — проведение аудита второй стороны.

В первом случае организация самостоятельно и добровольно принимает решение о проведении у нее аудита, самостоятельно и добровольно выбирает и приглашает аудитирующую компанию либо назначает аудиторов из числа сотрудников компании, из своих средств оплачивает проведение аудита, т. е. организация является заказчиком работы, а аудиторы — подрядчиком со всеми вытекающими последствиями, главное из которых — подрядчик несет ответственность перед заказчиком.

Во втором случае решение о проведении аудита второй стороны принимает заказчик (генподрядчик), поэтому ресурсы для проведения этой работы должен выделять также заказчик.

Если же эти две ситуации смешиваются, а еще хуже меняются местами, то получается достаточно неприличная схема, реализация которой в развитии может выглядеть так: проведение аудита второй стороны финансируется проверяемой организацией. Особенно это тревожно, когда заказчик является на рынке фактическим монополистом.

Проведение аудита второй стороны всегда должно быть открытым и прозрачным: должно быть получено согласие проверяемой организации, она должна быть заблаговременно предупреждена о дате аудита; должна быть получена и согласована программа проведения аудита второй стороны, известен состав команды аудиторов. Критерием аудита являются требования заказчика к организации, в нашем случае безопасности у подрядчика. А главное — подрядчик должен сам быть максимально заинтересован в результатах аудита. Не в положительном результате, а именно в результатах. В этом случае мы не только получаем результаты проверки, но и можем рассчитывать на то, что все выявленные риски, угрозы и недостатки будут оперативно устранены на деле, а не только на бумаге.

Ну и, конечно же, позиция собственника — фундамент общей безопасности предприятия. Если собственник бизнеса заинтересован в создании действительно работающей системы безопасности, если эта заинтересованность воплощена в четко сформулированную политику компании, если собственник осознает необходимость осуществления ощутимых затрат на обеспечение должного уровня безопасности, в этом случае даже при наличии каких-либо уязвимостей существующей системы можно быть уверенным: к безопасности тут относятся серьезно, а недостатки системы — явление временное. Если же этого базового фундамента нет, то дальнейшие разговоры на тему безопасности бессмысленны, компании можно только посочувствовать, а о налаживании партнерских отношений с такой компанией десять раз подумать.

Подводя итог, можно сделать вывод: изменения при ведении современного бизнеса зачастую бывают стремительными и глобальными. Не менее стремительно меняются угрозы и риски. И для их успешной минимизации нужно применять все доступные инструменты, в том числе и аудиты по безопасности.