Бюджетирование закупок для службы ИБ

Бюджетирование для самых маленьких:
«– Мы хотели построить два маленьких домика, – схитрил крокодил.
– Ну что ж, – сказал Иван Иванович, – я вам дам кирпичи
на один маленький домик».

Эдуард Успенский. Крокодил Гена и его друзья

Игорь Собецкий, *разработчик и автор курсов по экономической безопасности*
Учебный центр «Информзащита»

В этой статье мы рассмотрим некоторые сложности, возникающие в ходе приобретения службой безопасности компании необходимого для ее деятельности оборудования и материалов.

Основной проблемой является необходимость засекречивания некоторых аспектов деятельности службы безопасности компании. В частности, не предназначены для всеобщего распространения сведения:

- об использовании систем DLP[1];
- о применяемой службой безопасности аппаратуре для выявления РЭС/СТС[2];
- о системах записи телефонных переговоров;
- об иных технических средствах контроля за деятельностью персонала;
- о технических средствах видеонаблюдения и сигнализации;
- о методах конкурентной разведки.

Очевидно, что служба безопасности компании просто не сможет работать, если вся эта информация станет общеизвестной. Народная мудрость гласит: «Кто предупрежден, тот вооружен». И у корпоративных злоумышленников появляется прекрасный шанс сделать свое черное дело, не опасаясь справедливого возмездия: конфиденциальную информацию можно просто сфотографировать прямо с экрана монитора, не предназначенную для чужих ушей беседу – провести вечером из дома, получше спрятать выносимые по пути домой вещи удобнее в «мертвой» зоне видеокамеры…

В реальной же ситуации, как правило, в большинстве компаний обеспечивается самая широкая гласность проводимых закупок. Для начала инициатор закупки – в нашем случае это начальник службы безопасности – должен разъяснить руководству компании необходимость того или иного оборудования (или программного обеспечения). Уже на этой стадии информация о предстоящем приобретении может распространиться в коллективе[3]. Затем инициатору предстоит провести конкурс по выбору поставщика[4] или обосновать объемистой докладной запиской его безальтернативность. Затем материалы конкурса вместе с досье на поставщика представляются финансовому контролеру компании, в чьи обязанности входит перепроверить целесообразность закупок именно данного оборудования. Финансовый контролер тоже захочет подстраховаться и проконсультируется по этому поводу со «сведущими людьми», как минимум, с ИТ-директором или специалистом. И только после всех этих процедур счет от поставщика наконец поступает в бухгалтерию на оплату.

В сухом остатке – оборудования еще нет, а все подробности уже известны, как минимум, 5–8 работникам, не состоящим в штате службы безопасности. Даже если все эти люди кристальной честности, у каждого из них есть друзья, знакомые, да и просто болтовню в курилке никто не отменял. В свою очередь, наиболее продвинутые корпоративные жулики сами заботятся о своей безопасности и могут навести соответ-

[1] *От английских слов Data Leak Prevention – система предотвращения утечки данных.*
[2] *Радиоэлектронные и специальные технические средства для негласного получения информации.*
[3] *Особенно, если руководитель решает подстраховаться и консультируется с несколькими «независимыми специалистами» из числа своих подчиненных.*
[4] *До обеда не следует читать не только советские газеты, но и закон № 44-ФЗ.*

ствующие справки у знакомых в бухгалтерии или ИТ-отделе. Иными словами, к моменту внедрения с таким трудом закупленное оборудование будет уже малополезно для обеспечения безопасности компании.

Таким образом, перед каждым начальником службы безопасности встает вопрос: как обеспечить конфиденциальность своих закупок в масштабах компании? Некоторые специалисты идут по пути сокращения круга «посвященных» работников: «свой» бухгалтер, «свой» финансовый контролер и т. п. Однако такой вариант не представляется удачным. Как известно, когда тайну знают трое – это уже практически общедоступная информация. Разница с изначальным вариантом будет только в скорости распространения «секретных» сведений. Практически во всех современных российских компаниях информация об официально проведенных закупках доступна, как минимум, всем работникам бухгалтерии. И даже если в платежных документах стоит что-нибудь обтекаемое, вроде «изделия М-506» или «платы «Спрут-7», заинтересованный работник всегда сможет найти необходимую информацию в сети Интернет. Современные корпоративные казнокрады весьма заинтересованы в своей безопасности, и теперь наиболее продвинутые из них смогут обеспечить себе надежную защиту практически от любых контрольных мероприятий.

Второй вариант обеспечения конфиденциальности – тайное финансирование закупок службы безопасности в обход принятых в компании процедур. При таком подходе необходимое для обеспечения безопасности компании оборудование оплачивается из «черной кассы». Ну а сама касса пополняется традиционными для подпольного бизнеса способами: «премиями» надежным и лояльным работникам, банальной обналичкой и оплатой фиктивных работ подставным компаниям.

Этот способ обеспечивает практически абсолютную секретность: «черная касса» в единоличном распоряжении начальника службы безопасности, все закупки, установка и эксплуатация приобретенного оборудования осуществляются его подчиненными. Вероятность утечки информации минимальна. Единственный и фатальный недостаток данного метода – законность тут и не ночевала. После тайных закупок в компании оказывается, по сути, бесхозное имущество – оборудование, принадлежность которого не подтверждена документально. Соответственно, счастье начальника службы безопасности длится до первой проверки со стороны контролирующих органов. В тяжелых случаях при таких проверках может быть обнаружена и «черная касса», после чего компания приобретает в глазах проверяющих негативную репутацию, а государственный бюджет[5] неплохо пополняется за счет наложенных на нее штрафов.

Чтобы не подставить компанию под карающую длань государства, можно использовать третий вариант – разработку и внедрение специальной процедуры закупок оборудования для нужд корпоративной службы безопасности. Такая процедура должна предусматривать наличие у этого подразделения собственного бюджета, размер которого утверждается в начале года генеральным директором компании. Как правило, обоснование этого бюджета производится с помощью докладной записки, недоступной широкому кругу читателей[6]. После этого в течение года начальник службы безопасности единолично или через своих подчиненных осуществляет закупки в рамках установленного бюджета без дополнительного согласования своих шагов с кем бы то ни было. При этом все приобретенное оборудование и программное обеспечение во всех бухгалтерских документах и инвентаризационных ведомостях фигурирует исключительно под условными наименованиями. Даже если работники бухгалтерии окажутся чрезмерно любознательными, утечка информации маловероятна. Пару раз рассекретив таинственные обозначения типа «ErichKrause 26/6» (офисный степлер) или «2028-NPEE» (липкие бумажки для записей), пытливый работник успокоится и уже не заинтересуется не менее таинственными изделиями типа «Edic» или «Safe'n'Soft».

Разумеется, этот вариант официально прописывается как минимум в положении о службе безопасности компании. В ряде случаев изменения потребуется внести также и в положение об организации корпоративных закупок.

Для того чтобы убедить первое лицо компании санкционировать эти изменения, можно провести несложную демонстрацию. «Организуйте» штатным способом закупку какого-либо «шпионского» оборудования. Обязательно предупредите всех участников бизнес-процесса о строжайшей конфиденциальности, а примерно через неделю уже можно знакомить руководителя с циркулирующими в компании слухами. Как правило, после такого эксперимента руководитель соглашается полностью засекретить все дальнейшие закупки.

В отличие от предыдущего варианта, этот способ вполне соответствует действующему законодательству и обеспечивает вожделенный баланс между защитой интересов компании и правопослушным поведением. Завершающим штрихом при такой системе закупок для службы безопасности будет составление в конце года небольшой справки для руководства с анализом экономической эффективности сделанных вложений. Например: «приобретены 4 скрытые видеокамеры на общую сумму 36 тысяч рублей, с их помощью пресечено хищений продукции на 360 тысяч рублей». При рациональном использовании купленного оборудования экономическая отдача будет вполне реальной, и такая справка станет залогом сбалансированного бюджета службы безопасности на следующий год. ■

[5] *Всем известно, что работники государственных контролирующих органов РФ принципиально не берут взяток.*

[4] *Типовая аудитория для такого рода докладов – генеральный директор, финансовый директор или коммерческий директор, в отдельных случаях – главный бухгалтер и члены совета директоров компании.*