Менеджмент проектов в области корпоративной информационной безопасности

как общий язык с топ-менеджментом

Владимир Булдыжов, CISM

Перспективы информационной безопасности в текущих условиях

Текущая экономическая ситуация в мире и в Украине диктует предприятиям требования повышения эффективности своей деятельности, снижения накладных расходов и сохранения репутации компании.

По результатам исследования Ernst&Young, проведенного на рынках России и стран СНГ, проблемы информационной безопасности считаются актуальными в период экономического спада. На безопасности не экономят.

Эффективность службы информационной безопасности – это, прежде всего, экономическая эффективность инвестиций в проекты информационной безопасности.

Структура ущерба от нарушений информационной безопасности

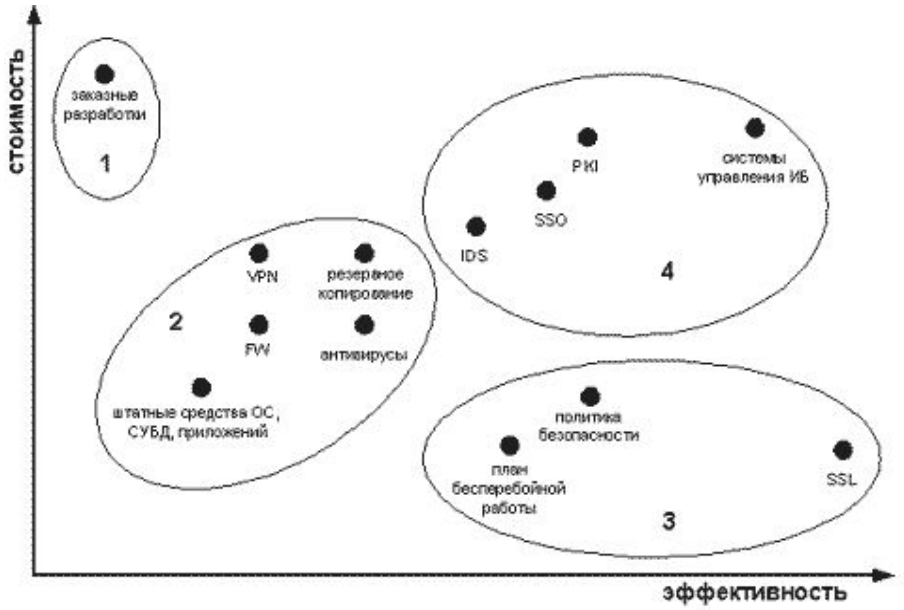
Существует два основных подхода к обоснованию инвестиций в информационную безопасность, основанные на оценке угроз:

1. Оценка количества нарушений.

2. Оценка ущерба от нарушений (до 80% - внутренние инциденты).

Эффективность службы информационной безопасности

Графический анализ, предложенный Стивеном Россом, Deloitte&Touche.



1. Заказные разработки – наименее эффективны.
2. Штатные средства ОС, СУБД и традиционные средства защиты – имеют хорошее отношение цена/качество.
3. Организационные меры (аудит, анализ риска, политика, план BCP, процедуры, регламенты) – имеют **наилучшее отношение цена/качество**.
4. Наиболее дорогие и наиболее эффективные средства защиты – IDS, SSO, PKI, DLP/ILP, КСУИБ. При их внедрении рекомендуется выполнять анализ рисков.

Проектный подход в информационной безопасности

Ключевые шаги подхода, рекомендуемого ISACA.

1. Полное подчинение *стратегии ИТ и стратегии ИБ – стратегии бизнеса*, **целей ИТ и ИБ – целям бизнеса**.

2. Анализ рисков. Выбор средств управления рисками.

3. Разработка программы (портфеля проектов) ИБ на основании анализа рисков.

4. Управление программой (проектами ИБ).

5. Управление инцидентами и реагирование на них.

Проектный подход в информационной безопасности

Анализ рисков (любая методика, например ISO 27000).

Средства управления риском:

- deterrent, сдерживающие (снижают вероятность угроз или восприимчивость к ним, по другой формулировке – мотивирование пользователя путем предупреждений),
- preventive, предотвращающие (снижают уязвимости, делают невозможными атаки, снижают воздействие: управление доступом, шифрование, аутентификация),
- corrective (recovery), корректирующие (снижающие воздействие: резервирование и восстановление),
- compensatory, компенсирующие (компенс. возрастающий риск: добавление доп. средств в дополнение к существующим слабым),
- detective, обнаруживающие (обнар. атаки или сканирования и включающие превентивные или корректирующие средства: журналы аудита, IDS, контрольные суммы).

Ключевые факторы успеха проектов информационной безопасности

Прозрачная и эффективная методика анализа рисков, обеспечивающая объективность и повторяемость результатов при одинаковых исходных данных, вне зависимости от эксперта, который применяет методику.

Поддержка высшего руководства организации, учреждение руководящего комитета по информационной безопасности (CEO, CIO, COO, CFO, CxO), высокая осведомленность пользователей о требованиях ИБ, чёткое распределение ответственности.

Своевременное реагирование на новые риски и внесение изменений в проекты снижения рисков. Применение лучших практик и стандартов при организации ИБ.

Квалификация персонала службы ИБ не только в архитектурных вопросах, но и в управленческих, экономических, психологических, юридических.

Сертификация специалистов = повышение прозрачности инвестиций

Одним из наиболее эффективных способов получения конкурентного преимущества на рынке труда и создания добавленной ценности специалиста по информационной безопасности является **официальное подтверждение его опыта и знаний** путем сертификации.

Это особенно актуально *в текущих экономических условиях*, когда рынок заставляет предприятия работать более эффективно, следовательно, тратить средства на наиболее эффективных специалистов, а значит, видеть, насколько оправданы инвестиции в информационную безопасность.

Сертификация CISM

Сертификация специалистов по информационной безопасности CISM является одной из наиболее престижных и востребованных во всем мире.

Сертификат	Среднегодовая зарплата в США, $
ISACA (CISM, CISA)	**98 571**
(ISC)^2 (CISSP, SSCP)	95 155
GIAC (GSEC, GSWIN, и др.)	80 093
Вендор (Microsoft, Cisco)	79 430
CompTIA (Security+, и др.)	68 036

Особенность курса в том, что он предназначен не только для ИТ-специалистов, но и для экономистов, финансистов, риск-менеджеров и топ-менеджеров.

Курс устанавливает взаимосвязь между ИБ и менеджментом: для специалистов по ИБ позволяет перейти на качественно новый уровень управления ИБ, правильно обосновать бюджет, оптимально распределить ресурсы в соответствии с рисками организации, управлять проектами, а для менеджеров — повысить прозрачность инвестиций и управляемость ИБ без глубокого проникновения в архитектурные особенности ИТ.

Ассоциация ISACA

Неприбыльная организация ISACA ведет свою историю с 1967 г.

Ассоциация известна в мире ИТ как авторитетный источник знаний и лучших практик, один из основных авторов стандартов COBIT и ValIT, концепции IT Governance, методик аудита и управления ИТ, массы обучающих, исследовательских и аналитических материалов.

Активность ISACA непрерывна и разнообразна. Ассоциация издает журнал, проводит конференции, в том числе в режиме онлайн.

В 70 странах находится 175 официальных филиалов. В 160 странах 75 тыс. членов организации. В Украине в настоящее время формируется филиал. Членство свободное.

Сертификация CISM в Киеве

Ассоциация ISACA проводит сертификацию специалистов в области аудита (CISA), информационной безопасности (CISM) и управления ИТ (CGEIT). Данные программы имеют аккредитацию ANSI.

На базе филиала (chapter-in-formation) и компании Ernst&Young функционирует сертификационный центр CISA/CISM. Для сертификации необходима сдача экзамена CISM, проводимого в форме теста на бумаге, подписание ряда обязательств, а также документально подтвержденный опыт в информационной безопасности не менее 5 лет.

Подготовка к сертификации CISM: **http://cism.com.ua**.

Спасибо за внимание!

Вопросы?

Владимир Булдыжов, CISM
vladimir @ buldyzhov.com