Оценивая риски, ИТ-специалисты не ограничиваются лишь одними информационными системами, программным, аппаратным и коммуникационным обеспечением, а рассматривают также вопросы физической безопасности и учитывают человеческий фактор.

Оценку ИТ-рисков следует проводить не реже двух раз в год, чтобы можно было гарантировать, что не остались невыявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно.

Внутри организации работа по оценке рисков должна быть нормализована путем формирования соответствующей политики, создания стандартов и руководств.

Эффективные процессы управления ИТ-рисками сокращают затраты и могут повысить валовой доход. От процессов управления ИТ-рисками может быть получена значительная прямая экономия затрат, отражающаяся на чистой прибыли, в долгосрочной перспективе гораздо более ценными. В целом будет повышение валового дохода, как следствие своевременного оповещения о рисках, стратегические инвестиции и улучшение производительности.

Список нормативной и научной литературы:

1. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.
2. NIST 800-30:2002 Руководство по управлению рисками для ИТ-систем.
3. COBIT Контрольные объекты для информационных и смежных технологий.

Олег Солоненко,
S&T Mold

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

This article describes how to assess the cost-effectiveness of information security through methodologies ROI, TCO, as well as the possibility of applying a set of methods to assess a number of financial and non-financial indicators such as KPI and BSC.

Информационная безопасность – есть *процесс*, направленный на достижение состояния защищённости информационной среды: устройств, процессов, программ, и данных, обеспечивающий конфиденциальность, целостность и доступность информации, которая обрабатывается, хранится и передается в этой среде.

Классической оценкой эффективности информационной безопасности является аудит на соответствие

стандарту. Несколько лет назад, Азиатско-Тихоокеанское экономическое сотрудничество по телекоммуникациям и информатизации (APEC TEL), составило список существовавших на тот момент стандартов ИБ, исключая Россию и страны СНГ, и дало их краткое описание в документе "APEC-TEL – INFORMATION SYSTEMS SECURITY STANDARDS HANDBOOK". Источником для списка были: ISO/IEC, CCITT, IETF, ANSI, NIST, EESSI и другие. Их оказалось свыше пяти сотен. Количество национальных стандартов в России по информационной безопасности более 30**.** В Молдове в качестве стандарта был принят SM ISO/CEI 17799:2004 Информационные технологии. Свод практических правил для управления информационной безопасностью, который представляет собой перевод на русский и румынский языки стандарта ISO/IEC 17799:2000 Information technology – Code of practice for information security management.

Информационные ресурсы, как и материальные ресурсы, обладают качеством и количеством**,** имеют себестоимость и цену. Себестоимость информации определяется количеством, затраченной на ее производство энергии (умственных усилий), финансовых и материальных затрат на ее документирование, хранение, обеспечение сохранности, обработку и передачу по каналам связи. Цена информации, как и остальных товаров, складывается из себестоимости и величины прибыли от ее реализации. Как видно из вышеизложенного, информация обладает свойствами товара, и, следовательно, как и любой товар, она может участвовать в товарообороте и являться объектом права, иметь производителя, собственника, владельца и потребителя.

С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект. С точки зрения обладателя – сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства, и сбыта товаров и услуг.

При попытке использовать *классические методы оценки инвестиционных проектов* при оценке экономической эффективности информационной безопасности, предполагающей определение такого показателя, как коэффициент рентабельности инвестиций (ROI), существуют сложности с оценкой цены информации, вероятности осуществления угрозы и как следствие – стоимости нанесенного ущерба в результате данной угрозы, так как отсутствуют статистические данные по стране и по отраслям. Результаты тяжело аргументировать для представления финансовому руководству, так как экономическая эффективность возникает при возникновении прогнозируемого события. То есть экономическая эффективность возникает при успешной реализации угрозы.

При использовании расчета по *затратным методам оценки* – определение совокупной стоимости владения (Total Cost of Ownership, TCO) необходимо сравнение определенного показателя TCO с аналогичными показателями TCO по отрасли

(с аналогичными компаниями) и с «лучшими в группе», что неприменимо по причине отсутствия таких данных в нашей стране.

Комплексные методы оценки набора финансовых и нефинансовых показателей эффективности (KeyPerformance Indicators, KPI) и сбалансированная система показателей Нортона и Каплана (Balanced Scorecard, BSC) могут быть применены для оценки экономической эффективности информационной безопасности, как это описано в *Control Objectives for Information and related Technology* (COBIT®) и в ряде статей на сайте Information System Audit and Control Association (ISACA). Сложность внедрения заключается в том, что уровень зрелости организации по модели Технологической Зрелости (Capability Maturity Model Integrated, CMMI) должен быть "Quantitatively Managed". Это значит, что в организации определены и описаны процессы и установлены стандарты в пределах организации. Присутствует детальное описание всех процессов, в котором лучше раскрываются связи и зависимости, знание которых позволяет улучшить управление. Выбраны способы, которые при использовании статистических методов и других количественных техник позволяют контролировать качество выполнения процессов.

Экономическая эффективность процесса управления информационной безопасностью во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются. Управление рисками позволяет структурировать деятельность управления информационной безопасностью, найти общий язык с высшим менеджментом организации, оценить эффективность работы и обосновать решения по выбору конкретных технических и организационных мер защиты перед высшим менеджментом. Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности организации как среднего, так и высшего звена. Какие бы подходы ни использовались для измерения и улучшения степени информационной защищенности в организации, оценка их объективности, по-видимому, является принципиальным фактором, способствующим рассмотрению степени их эффективности и основы для внесения необходимых усовершенствований в области информационной безопасности организации.

Литература:

1. О. Дворчук. *Показатели экономической эффективности ИТ-Проектов.* http://www.security.ase.md/publ/ru/pubru107/Dvorciuk_O.pdf
2. Н. Куканова. *Современные методы и средства анализа и управления рисками информационных систем компаний*. http://www.dsec.ru/about/articles/ar_compare/
3. Е. Акимов. IT-security. *Экономическая эффективность и управление рисками*. http://www.docflow.ru/analytic_full.asp?param=32185
4. И. Ляпунов. *Информационная безопасность перерастает в безопасность бизнес-процессов*.

http://www.jet.msk.su/publication_detail/?nid=bdb77c9afe3d0ff1e1b4eed-32c7fd71a&sid=sr
5. Артем Жуков. *Что такое система информационной безопасности, ее необходимость, состояние информационной безопасности в России на сегодняшний день*. http://infosecurity.report.ru/material.asp?MID=152
6. А. Лукацкий. *О заблуждениях в безопасности, ставших классикой*. http://bankir.ru/analytics/infosec/1367694
7. V. Grembergen. *COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade* http://www.isaca.org/Content/ContentGroups/Journal1/20058/jpdf0-506-CobiT-Management.pdf
8. А. Лукацкий. *BSC и информационная безопасность*. http://www.osp.ru/cio/2009/01/5766348/

Valentin Pocotilenco, Veaceslav Sidorenco,
Technical University of Moldova, Stefan-cel-Mare av., 168,
Alexei Altuhov, Petru Bogatencov ,
RENAM Association Str. Academiei, 5, of 331

MD-GRID CERTIFICATION AUTHORITY

Certificate Authority is a trusted network entity, responsible for managing X509 digital certificates and is a trusted entity that validates the identity of the holder of a digital certificate. Paper describes the particularities of MD-Grid CA established for grid users and scientific communities of Moldova.

I. Introduction

A Certification Authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption and decryption. The CA computer, where the signing of the certificates will take place, needs to be a dedicated machine, running no other services than those needed for the CA operations. The CA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

Software-based private keys of the CA must be protected with a pass phrase of at least 15 elements and that is known only by designated personnel of the CA. On-line CA's using Host Security Module (HSM) must adopt a similar or better level of security. Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled.

II. RENAM services

RENAM Association implements and run a range of services that require authorization or authentication [1,2]:

- CERT – since May 2007 RENAM association start own CERT center.