Виктор ЖИТАРУ,
Молдавская экономическая академия

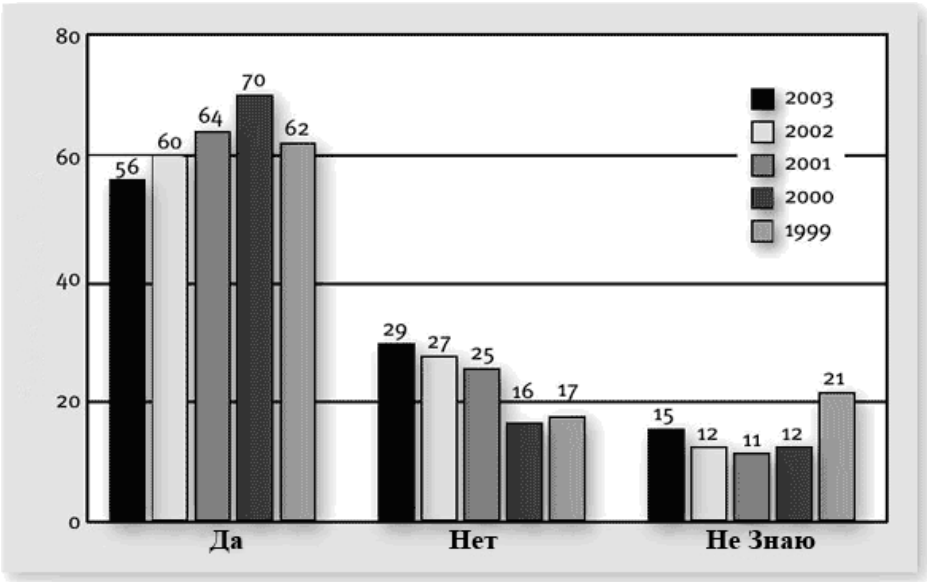
СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА АНАЛИЗА И КОНТРОЛЯ РИСКОВ (НА ПРИМЕРЕ CRAMM AND RISCKWATCH)

This article contains information about two methods of risk management: CRAMM and RisckWatch. Here you will find the description of these two methods and what can they offer.

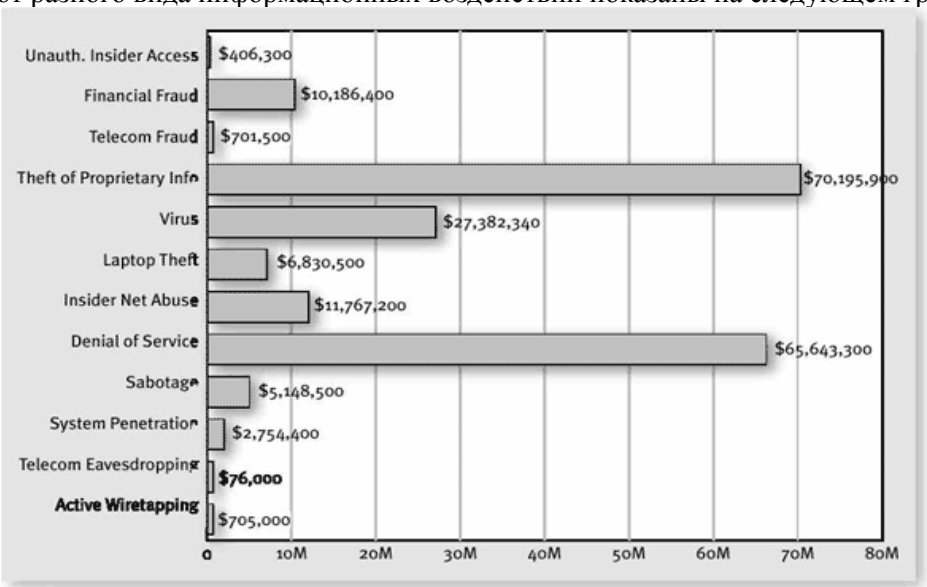
Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса. Основной вопрос современного бизнеса – как оценить достаточный уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ – применение систем анализа рисков, позволяющих оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков к затратам на ИБ).

Для подтверждения факта актуальности задачи обеспечения безопасности бизнеса, воспользуемся отчетом ФБР за 2003 год. Данные были собраны на основе опроса 530 американских компаний (средний и крупный бизнес).

Статистика инцидентов области ИТ-безопасности неумолима. Согласно данным ФБР, в 2003 году 56% опрошенных компаний подвергались атаке:



Потери от разного вида информационных воздействий показаны на следующем графике:



По статистике, самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются две причины:

1) ограничение бюджета;
2) отсутствие поддержки со стороны руководства.

Обе причины возникают из-за непонимания руководством серьезности вопроса и сложности для ИТ-менеджера задачи обосновать, зачем необходимо вкладывать деньги в информационную безопасность. Зачастую многие склонны думать, что основная проблема заключается в том, что ИТ-менеджеры и руководители разговаривают на разных языках — техническом и финансовом, но ведь и самим ИТ-специалистам часто трудно оценить, на что потратить деньги и сколько их требуется для обеспечения большей защищенности системы компании, чтобы эти расходы не оказались напрасными или чрезмерными.

Обоснование необходимости инвестиций в информационную безопасность. Для решения данной задачи были разработаны программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch).

Метод CRAMM

CRAMM (the UK Goverment Risk Analysis and Managment Method) был разработан Службой безопасности Великобритании (UK Security Service) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта.

В настоящее время CRAMM – это довольно мощный и универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач, включая: проведение обследования ИС и выпуск сопроводительной документации на всех этапах его проведения; проведение аудита в соответствии с требованиями Британского правительства, а также стандарта BS 7799:1995 – Code of Practice for Information Security Management BS7799; разработку политики безопасности и плана обеспечения непрерывности бизнеса.

Программное обеспечение RiskWatch

RiskWatch, разрабатываемое американской компанией RiskWatch, является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков: RiskWatch for Physical Security – для физических методов защиты ИС; RiskWatch for Information Systems – для информационных рисков; HIPAA-WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA;

RiskWatch RW17799 for ISO17799 – для оценки требованиям стандарта ISO17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются «предсказание годовых потерь» (Annual Loss Expectancy – ALE) и оценка «возврата от инвестиций» (Return on Investment – ROI). Семейство программных продуктов RiskWatch, имеет массу достоинств.

Литература:

1. Методологии управления ИТ-рисками – http://www.osp.ru/os/2006/08/3584582/_p1.html
2. Современные методы и средства анализа и управление рисками информационных систем компаний – http://citforum.ru/products/dsec/cramm/
3. Современные методы и средства анализа и контроля рисков информационных систем компаний – http://www.ixbt.com/cm/informationsystem-risks012004.shtml