стратегию его развития, которая позволит минимизировать потери и достичь поставленных целей.

Своевременное управление рисками, которые возникают при внедрении корпоративных информационных систем на предприятиях и негативно влияют на реализацию проекта внедрения, позволит устранить недостатки проекта, тем самым повысить его эффективность и результаты.

МЕТОДЫ РАСЧЕТА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Солоненко Олег**, Молдавская Экономическая Академия (Республика Молдова)*

In this work were present methods for calculating cost-effectiveness of information security system.

Введение. Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ – применять системы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты. Для расчета можно выбрать одну из перечисленных в [1] методик.

Расчет затрат на информационнцю безопасность

Для количественной оценки предварительно необходимо рассчитать затраты на:

- приобретение и ввод в эксплуатацию программно-технических средств: серверов, компьютеров конечных пользователей, периферийных устройств и сетевых компонентов.
- приобретение, настройку, плановые и внеплановые проверки и испытания средств защиты информации;
- содержание персонала, стоимость работ и аутсорсинг;
- формирование политики безопасности предприятия и контроль за ее соблюдением;
- проверку навыков эксплуатации средств защиты персоналом предприятия;
- выявление причин нарушения политики безопасности, организационные и прочие расхо-

ды, которые непосредственно связаны с предупредительными мероприятиями;
- осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации;
- проверку сотрудников на лояльность, выявление угроз безопасности;
- ликвидацию последствий нарушения режима информационной безопасности;
- организацию взаимодействия и координации между подразделениями для решения конкретных повседневных задач;
- проведение внутреннего и внешенго аудита безопасности
- идентификацию угроз безопасности,уязвимостей и оценке степени риска
- восстановление системы безопасности до соответствия требованиям политики безопасности;
- установка патчей или приобретение последних версий программных средств защиты инфомрации;
- восстановление баз данных и прочих информационных массивов;
- проведение расследований нарушений политики безопасности
- обновление планов обеспечения непрерывности деятельности службы безопасности.
- внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;
- выполнение обязательства перед государством и партнерами
- юридические споры,выплаты компенсаций и потери в результате разрыва деловых отношений..
- организацию системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой.
- поддержание системы резервного копирования и ведения архива данных;
- контроль изменений состояния информационной среды предприятия;
- повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, вычислительной техники и т.п.

Приведенный список затрат является не полным и может быт дополнен из [2].

TCO можно расчитать по формуле:

$$\mathbf{TCO(E) = cost0(E) + \sum_{t=1}^{t=n} cost\ t(E) / T,}$$

где, cost0(E) единовременне затраты (закупка, установка и тд.), cost t(E) текущие затрат в течении времени эксплуатации (операционные и прочие), T – время эксплуатации. [3]

Метод расчета ROSI можно представить так.

1. Определяется ожидаемая потеря денежных средств за год по причине возникновения инцидента ИБ - Annual Loss Expectancy (ALE). Показатель ALE вычисляется как произведение ущерба от некоего инцидента ИБ в денежном эквиваленте на количество возникновений (или вероятность возникновения) этого инцидента в течение года.
2. Применение меры защиты предполагает снижение вероятности возникновения инцидента ИБ, поэтому определяется также так называемый модифицированный показатель ALE (mALE), как произведение ущерба от инцидента ИБ в денежном эквиваленте на количество возникновений (или вероятность возникновения) этого инцидента после применения средств защиты.
3. Разница между ALE и mALE, за вычетом стоимости всех затрат перечисленных выше и есть ROSI.

Вывод

Единого рецепта на все случаи жизни не существует. Многое зависит от того, как воспринимает проект бизнес-руководство. Каждый из методов обладает своими достоинствами и недостатками и имеют свои предпочтительные области применения.

Иинфраструктурный проект может быть оценен прежде всего с помощью TCO, ALE. Оценка бизнес-проектов — это, прежде всего, оценка отдачи для бизнеса, и ее лучше делать при помощи ROI, EVA. Для финансовой оценки аутсорсинговых проектов подойдут ROI, TCO, ALE. Если принята программа создания нового бизнеса в сфере аутсорсинга то можно применять EVA, усиленную оценкой рисков и возможностей на основе ROI.[4]

Литература

1. Базаров Р. Во всех измерениях журнал “CIO World”№9; http://www.cio-world.ru/offline/2006/52/286650/
2. Козаченко В. - Управление общей стоимостью владения КИС http://www.cfin.ru/itm/kis/kis_tco.shtml

3. Robinson Ph., Stephenson B. - "TCO-aware provisioning of information security infrastructure" HP Labs, http://www.hpl.hp.com/techreports/2008/HPL-2008-195.pdf
4. Полякова М. - "ИТ и деньги"; http://www.osp.ru/titles/cw/article/article_9491929.html

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ И ПЕРСПЕКТИВЫ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Константин Андроник, Василий Власов
Славянский университет (Республика Молдова)

Some modern possibilities of use computer стеганографии for the decision of problems of information safety are considered. Development prospects are defined.

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии (от греческого «тайнопись»), появилось новое направление в области защиты информации - компьютерная стеганография (КС). Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации [2].

Основными положениями современной компьютерной стеганографии являются следующие [1, 3]:

I. Методы скрытия должны обеспечивать аутентичность и целостность файла.

II. Предполагается, что противнику известны все возможные стеганографические методы.

III. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации - ключа.

IV. Даже если факт скрытия сообщения стал известен противнику