Йоаким Каламарис

МЕТОДИ ЗА ОЦЕНКА НА ИКОНОМИЧЕСКАТА ЕФЕКТИВНОСТ НА СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Разгледани са методите за оценка на икономическата ефективност на системите за информационна сигурност, които намират пряко практическо приложение: на оценка на съвкупната стойност на собствеността; на коефициента на възвръщаемост на инвестициите, на ефективността на инвестициите, прилагани в технологии за сигурност; методите на добавената икономическа стойност и на изходната икономическа стойност; на управление на портфейла на активите за информационна сигурност;на оценка на действителните възможности; на жизнения цикъл на изкуствените системи; на система на балансираните показатели; на очакваните загуби; за анализ на дървото на грешките; на дисконтираните парични потоци.

JEL: C12; C88

Според някои автори всеки метод за оценка на икономическата ефективност на системите за информационна сигурност (ИС) трябва да отговаря на няколко изисквания:[1]

- *да дава количествена оценка на разходите за сигурност*, използвайки качествени показатели за предвиждане на вероятните събития и техните последствия;
- *да бъде прозрачен* от гледна точка на потребителя и да предоставя възможност за въвеждане на собствени емпирични данни;
- *да е универсален*, т.е. еднакво приложим за оценка на разходите за придобиване на технически средства, специализирано и универсално програмно осигуряване, разходи за услуги, за персонал, обучение на крайните потребители и т. н.;
- *да позволява моделиране на ситуацията*, при която съществуват няколко ответни мерки, насочени към предотвратяване на определена заплаха, влияещи в различна степен върху намаляването на вероятността от произшествия.

Оценка на съвкупната стойност на собствеността

Методиката за оценка на съвкупната стойност на собствеността (*Total Cost of Ownership* - TCO)[2] първоначално е разработвана от компанията

[1] *Петренко, С. А., Е. М.Терехова*. Оценка затрат на защиту информации. - Защита информации. Инсайс, январь-февраль, 2005, N 1; *Петренко, С. А., Е. М.Терехова*. Обоснование инвестиций в сигурность, http://www.osp.ru/cio/2006/01/036.htm

[2] Да оценим информационните технологии. - CIO, 2002, N 4; *Басараб, С*. Экономическая эффективность систем информационной сигурности, http://www.security.ase.md/publ/ru/pubru80/pubru80.pps.

Gartner Group през 1986 - 1987 г. с цел да се установят разходите от внедряването на информационните технологии. Тя позволява да се пресметне цялата разходна част на информационните активи на компанията, включвайки преките и косвените разходи за апаратно-програмни средства, организационни мероприятия, обучение и повишаване квалификацията на сътрудниците на компанията, реорганизация, преструктуриране на бизнеса и т.н.

В края на февруари 1998 г., след като *Gartner Group* придобива *Interpose*, тя става едноличен притежател на всички ресурси на тази най-популярна методика, превърнала се в основен инструмент за пресмятане на TCO и в други области на компютърните технологии. Например сега съществува методика за пресмятане на TCO на документооборота, на различните апаратни платформи, мрежи, програмно осигуряване.

Поради *измеримостта на оценката на икономическата ефективност* на корпоративната система за защита на информация, се появява възможност за оперативно решаване на задачите за контрола и корекцията на показателите за икономическа ефективност и в частност на *показателя TCO*. Така този показател може да се използва като *инструмент за оптимизация на разходите за осигуряване на необходимото ниво на сигурност на* компютърните системи и обосноваване бюджета на ИС.

Методиката TCO позволява да се:

- получи адекватна информация за нивото на защитеност на разпределена изчислителна среда и съвкупната стойност на владение на корпоративната система за защита на информацията;
- сравнят подразделенията на службата по ИС на компанията както помежду си, така и с аналогични подразделения на други предприятия в дадения отрасъл;
- оптимизират инвестициите за ИС на компанията, отчитайки реалната стойност на *показателя TCO*.

Показателят TCO е равен *на сумата на преките и косвените разходи за организация (реорганизация), експлоатация и съпровождане на корпоративната система за защита на информация в течение на година.*[3]

TCO = Преки разходи + Косвени разходи

Преките разходи включват както капитални компоненти на разходите (асоциирани с фиксирани активи или *"собственост*"), така и разходи за труд, които се отчитат в категориите "операции" и "административно управление". Тук се отнасят разходите за услуги на отдалечени потребители и други, свързани с поддръжката на дейността на организацията.

---

[3] *Арзуманов, С. В.* Оценка эффективности инвестиций в информационную сигурность. – INSIDE, 2005, N 1, http://www.inside-zi.ru/pages/1_2005/23.html] *Исаев, В.* Как обосновать затраты на информационную сигурность? http://www.iitrust.ru/articles/zat_ibezop.htm; *Мурадян, А*. TCO изнутри – версия 2. Изд. "Коминфо Консалтинг", http://telecominfo.ru/index.html?t=2000; *Разумов, М.* Обоснование расходов на системы обнаружения вторжений, 2004 , http://www.securitylab.ru/analytics/216222.php.

Косвените разходи отразяват влиянието на компютърните информационни системи (КИС) и подсистемите за защита на информацията на сътрудниците на компанията посредством такива измерими показатели като *престой* и *спиране на корпоративната система* за защита на информацията, *разходи за операции и поддръжка* (които не се отнасят към преките разходи). Много често косвените разходи играят значителна роля, тъй като те обикновено първоначално не се отразяват в бюджета за ИС, а впоследствие, което в крайна сметка води до ръст на *"скритите"* разходи на компанията за ИС.

Показателят TCO може да се използва практически на всички основни етапи на жизнения цикъл на корпоративната система за защита на информацията и позволява да се въведе ред в съществуващите и планираните разходи за ИС. От тази гледна точка той дава възможност обективно и независимо да се обоснове икономическата целесъобразност от внедряването и използването на конкретни организационни и технически мерки и средства за защита на информацията. За обективност на решението е необходимо допълнително да се отчита състоянието на външната и вътрешната среда на предприятието (показателите за технологическо, кадро-во и финансово развитие), тъй като невинаги *най-малкият показател TCO* за корпоративната система за защита на информацията може да бъде оптимален за компанията.

Сравняването на този показател с аналогични показатели на TCO по отрасли (с аналогични компании) и с *"по-добрите в групата*" позволява обективно и независимо да се обосноват разходите на компанията за ИС, както и да се обоснове, че проектът за създаване или реорганизация на корпоративната система за ИС е оптимален в сравнение с някакъв средностатистически проект в областта на защитата на информацията в отрасъла. Сравнението може да направи с помощта на усреднени показатели за TCO по отрасли, пресметнати от експерти на *Gartner Group* или от собствените експерти на компанията с помощта на методите на математическата статистика и обработката на наблюдения.

Методиката TCO позволява да се отговори на следните въпроси:[4]

- Какви парични средства се изразходват за ИС?
- Оптимални ли са разходите за ИС за бизнеса на компанията?
- Доколко е ефективна работата на службата по ИС на компанията в сравнение с другите отдели?
- Как ефективно да се управлява инвестираното в защитата на информацията?
- Какви направления да се изберат за развитие на корпоративната система за тази защита?

[4] *Петренко, С.* Оценка затрат компании на информационную сигурность, http://www.citforum.ru /security/articles/ocenka_zatrat/

• Как да се обоснове бюджетът на компанията за ИС и да се докаже ефективността на съществуващата корпоративна система за защита на информацията и службите по ИС?

• Каква е оптималната структура на тези служби?

• Как да се оцени ефективността на нов проект в областта на защитата на информацията?

Тази методика може да отчита спецификата на някои компании с помощта на т. нар. *коефициенти за поправка*, например:

• на *стойността на основните компоненти* на корпоративната система за защита на информацията и КИС;

• на *работната заплата на сътрудниците*, отчитайки дохода на компанията, географското й положение, типа на производство и местонахождението на организацията (голям град или не);

• по отношение на *видовете крайни потребители на ИТ*;

• на *използването* на т.нар. *по-добри практики* (*best practice*) в областта на управлението на ИС;

• относно *степента на сложност* на използваната информационна технология и нейното интегриране в производствения процес на организацията (например с влияние до 40%).

Определянето на разходите на компанията за ИС изисква решаването на *три основни задачи*:

1. Оценка на текущото ниво на ТСО на корпоративната система за защита на информацията и КИС.

2. Одит на ИС на компанията на основата на сравнения на нейното ниво на сигурност и предлаганото (по-добра световна практика) ниво на ТСО.

3. Формиране на целеви модел на ТСО.

Оценка на текущото ниво на ТСО

По време на работата по оценката на ТСО се осъществява събиране на информация и пресмятане на показателите на ТСО за организацията в няколко направления:

• съществуващите компоненти на КИС, вкл. системата за защита на информацията, и информационните активи на компанията (сървъри, клиентски компютри, периферни устройства, мрежови устройства);

• разходите за апаратни и програмни средства за защита на информацията (разход за материали, амортизация);

• разходите за организация на ИС в компанията (обслужване на системите за защита на информацията и системите за контрол и защита на информацията, както и собствени средства за защита на периферните устройства, сървъри, мрежови устройства, планиране и управление на процесите по защита на информацията, разработка на концепция и политика по сигурност и др.);

• разходите за организационни мерки за защита на информацията;

• косвените разходи за организация на ИС в компанията и в частност, осигуряване на непрекъснатост или устойчивост на бизнеса на компанията.

Одит на ИС на компанията

По резултатите от събеседвания с топ-мениджърите на компанията и провеждане на инструментални проверки на нивото на сигурност на организацията се прави анализ в няколко основни аспекта:

- политики за сигурност;
- организационни въпроси на управлението на подсистемата за сигурност;
- класификация и управление на информационните ресурси;
- управление на персонала;
- физическа сигурност;
- администриране на компютърните системи и мрежи;
- управление на достъпа до системите;
- разработка на системите;
- планиране на непрекъсваема работа на организацията;
- проверка на системата за съответствие с изискванията за ИС.

Въз основа на проведения анализ се избира модел на ТСО, сравнявайки го със средните и оптималните стойности за репрезентативна група аналогични обекти, които имат сходни с разглежданата организация показатели по обем на бизнеса. Такава група се избира от базата данни за ефективност на разходите за ИС и ефективност на съответните профили на защита на аналогичните компании.

Сравнението на текущия показател на ТСО за проверяваната компания с моделните му стойности позволява да се анализира ефективността на организацията на ИС на компанията. В резултат от това се установяват *"тесните"* места в организацията, причините за тяхното появяване и избирането на по-нататъшните стъпки по реорганизация на корпоративната система за защита на информацията и осигуряване на необходимото ниво на сигурност на КИС.

Формиране на целеви модел на ТСО

В съответствие с резултатите от проведения одит се моделира целевият (желаният) модел, отчитащ перспективите за развитие на бизнеса и корпоративната система за защита на информацията (активи, сложност, методи на *"по-добрите практики"*, типовете системи за защита на информацията и за колективна защита на информацията, квалификацията на сътрудниците на компанията и т.н.).

Освен това се разглеждат капиталните разходи и разходите за труд, необходими за провеждане на преобразувания на текущата среда в целева. В разходите за труд при внедряване се включват тези за планиране, развитие, обучение и разработка. Тук също влизат възможните временни увеличения на разходите за управление и поддръжка.

За обосноваване ефекта от внедряването на новата корпоративна система за защита на информацията могат да бъдат използвани моделни характеристики за намаляване на съвкупните разходи, отразяващи възможните изменения в тази система.

Оценката на ефективността на инвестициите за ИС зависи от *нивото на зрялост на организацията*. Съгласно методиката на *Gartner Group* са определени четири нива на зрялост на от гледна точка на осигуряването на ИС:[5]

0 ниво:

- никой в компанията не се занимава с ИС; ръководството не осъзнава важността на проблемите по сигурността;
- липсва финансиране;
- ИС се реализира със стандартните средства на операционната система, системата за управление на базата данни (СУБД) и приложенията (паролна защита, разграничаване на достъпа до ресурси и сервизи).

1 ниво:

- ИС се разглежда от ръководството като чисто *"технически"* проблем, липсва единна програма (концепция, политика) за развитие на системата за осигуряване на информационна сигурност (СОИС) на компанията;
- финансирането се води в рамките на общия ИТ-бюджет;
- ИС се реализира със средства от нулево ниво, плюс средства за резервно копиране, антивирусни средства, междумрежови екрани, средства за организация на VPN (традиционни средства за защита).

2 ниво:

- ИС се приема от ръководството като комплекс от организационни и технически мероприятия, съществува разбиране на нейната важност за производствения процес, има утвърдена от ръководството програма за развитие на такава система;
- финансирането се води в рамките на отделен бюджет;
- ИС се реализира със средствата на първото ниво, плюс средства за усилване на автентизацията, за анализ на съобщенията по електронната поща и web-съдържанието, IDS (системи за откриване на заплахи), средства за анализ на сигурността, SSO (средства за еднократна автентизация), PKI (инфраструктура на открити ключове) и организационни мерки (вътрешен и външен одит, анализ на риска, политика по ИС, положения, процедури, регламенти и ръководства).

3 ниво:

- ИС е част от корпоративната култура, назначен е CISA (старши ръководител по тези въпроси);

---

[5] *Петренко, С., С. Симонов, Р. Кислов*. Информационная сигурность – экономические аспекты. - Jet Info Online, 2003, N 10, http://www.citforum.ru/security/articles/sec/index.shtml.

• финансирането се води в рамките на отделен бюджет;

• ИС се реализира със средства от второ ниво – системи за управление на информационната сигурност, CSIRT (група за реагиране на инциденти и нарушения на ИС), SLA (съглашение за ниво на сервиз).

Някои автори предлагат друга класификация на организациите според нивото на зрялост, която включва *пет нива* на компаниите и техните характеристики:[6] *анархия; фолклор; стандарти; измеримо; оптимизируемо*.

Според нас подобна методика може да се прилага ефективно в организации от последните две нива на зрялост ("измеримо", "оптимизируемо"), частично да бъде полезна при ниво на зрялост "стандарти" и безполезна за първите две нива.

Ще анализираме методиката, базираща се на TCO *Advisor Client&Server Model*, която може да се представи в *четири основни етапа*:[7]

Етап 1. Определяне профила на предприятието

Съгласно класификацията на *Interpose* има 17 профила на предприятията, като всеки от тях има по три градации - малко, средно и голямо предприятие. Например средното предприятие във финансовия отрасъл има около 50 сървъра и 2000 работни станции.

След избора на профил на предприятието се събират данни за неговия бюджет като: общ брутен доход, брутен доход, пресметнат за едно компютърно работно място, процентен показател на ръста за разглеждания период, бюджет за информационни технологии.

Етап 2. Анкетиране и анализ на работните места

На този етап на администраторите и потребителите се раздават специални анкети, които са предназначени за събиране на информация за количеството работни места, стойността при закупуване на компонентите и т.н. Част от анкетата, попълвана от администратора, е представена на табл. 1.

Таблица 1

Анкета за оценка на работно място

Оборудване	Всичко	Закупено	Взето под аренда
Сървъри	50	50	0
Клиентски места	3,120	3,120	0
Принтери	613	613	0
Мрежови компоненти	212	180	32
Общ брой устройства	3995	3963	32
Потребители	2894		

[6] *Симонов, С. В.* Технологии и инструментарий для управления рисками. - Jet Info, 2003, N 2.

[7] *Мурадян, А.* TCO изнутри. - Компьютерра, март 1998, N 10.

Освен общите данни се събира по-подробна информация за оборудването - с*ървъри, клиентски места, мрежови компоненти* (мостове, комутатори, устройства за съхраняване на информация и т.н.). След това се прави сравнение на стойностите на тези компоненти със средните стойности на същите компоненти за отрасъла (табл. 2).

Таблица 2

Сравняване на фактическите стойности за предприятието със средните стойности за отрасъла

	Средно за отрасъла (С) (ед.)	Фактически за предприятието (Ф) (ед.)	Ф – С (ед.)	Разлика (%)
Клиентски места на всеки потребител	1	1	0	0
Потребители на всеки сървър	25	58	33	132
Потребители на всеки принтер	15	5	-10	-69
Потребители на FTE (Full Time Equivalent) на всеки мрежови администратор	40	48	8	20
Потребители на FTE службата за поддръжка	86	193	107	125

Етап 3. Събиране и анализ на друга информация

По-нататък се събира информация за преките и косвените разходи за апаратура и програмно осигуряване; плащания за арендувано оборудване и други разходи за компютърна техника; за управление на ИТ; разходи за краен потребител и т.н.

Етап 4. Изчисляване стойността на TCO

След като е направено рутинното събиране на изходните данни и са въведени в програмата, тя извършва изчисляването на TCO. Необходимо е след това да се направи сравнение на получените резултати със средните показатели за промишления отрасъл и да се определят *критичните моменти в разходите*.

Фактори, влияещи на величината на TCO

Една от основните грешки на повечето мениджъри при проектирането на ИТ-системата е невярната ориентация към средния потребител, вследствие от което настъпва непрогнозируем ръст на разходите за ИТ. В резултат от това повечето потребители получават *усреднена по корпоративния стандарт производителност на техниката*, даже и когато в техните функции влиза само набор на текст по форма, а компютрите се използват не повече от 10%. В същото време потребителите, от които се изисква максимална производителност, могат да не получат техника, адекватна на техните работни функции. Затова *Gartner Group* препоръчва при проектирането на ИС да се наблегне на

детайлизацията на изпълняваните от работниците функции и подборът на техника да се осъществява според индивидуалните нужди, а не по усреднени показатели. Във връзка с това се предлага опростена *градация на потребителите* по изпълними функции и стойността на времето за престой:

1. Работниците, които изпълняват критични и уникални за предприятието задачи, работещи с жизненоважни данни.

2. Мобилни работници, които често пътуват. Обикновено те работят с много скъпа и чувствителна техника. Изискванията към сервизното обслужване, поддръжката и оборудването също са високи. Стойността на времето за престой е максимална.

3. Работници, занимаващи се с обработката на информация. Това е най-размитата категория. Стойността на времето за престой може силно да варира, макар в повечето случаи да е висока.

4. Работници, осъществяващи механичен вход на информация в системата посредством определени форми. Броят на работните функции е ограничен до една-две.

Фактори, влияещи на увеличаването на ТСО

1. Човешкият фактор, по-точно действията на крайния потребител. Най-съществена част от стойността на владение на РС е свързана с разходите за труд. Повечето от проблемите на потребителя изискват пряка намеса на администратора в неговия компютър, увеличавайки трудовите разходи на административния персонал. Например: невнимателно изтриване на системни потребителски файлове; изменение в конфигурацията на системата; инсталация на допълнителни програми, водеща до конфликти с вече използвано програмно осигуряване; непроизводителни действия на крайния потребител, по-точно времето, изразходвано за тях.

2. Ненормативни конфигурации на РС. Повечето организации използват отделни модели компютри от различни производители, които предварително са конфигурирани от доставчика без отчитане спецификата на потребителя. Освен това те могат да се отличават и по състав. След известно време, когато се изисква добавяне или обновяване на драйвери и приложения, съответно рязко нарастват времевите и финансовите разходи.

3. Информация и приложения, твърдо привързани към определени автоматизирани работни места. Потребителите са ограничени от използването на компютъра и приложенията само на собственото си работно място. Макар че съществува възможност за създаване на отдалечен достъп до приложения, разходите нарастват поради невъзможността за приложения на друга техника.

4. Увеличаване броя на мобилните потребители. Съгласно данни на *Forrester Research* 82% от общия брой РС съставляват стандартни настолни РС, включени към мрежа. Броят на мобилните потребители (също по данни на *Forrester Research*) в края на 2000 г. е 63%.

5. Риск от неправилно инвестиране в информационни технологии. Грешката на повечето фирми е в ориентацията им към стандартни статии от

бюджета без оценка на възможните рискове. Например достатъчна е една успешна вирусна атака, така че възстановяването на информационната структура да "изяде" не само годишния бюджет за ИТ, но и цялата печалба на компанията.

6. Рискове, произтичащи от производителя на оборудване и програмно осигуряване. Те се свързват най-вече с някои от посочените фактори. Съществено тегло има показателят "динамика на развитие на пазара". Незрелостта на пазара, вследствие на която могат да настъпят маркетингови войни, по подобие на дъмпинга води обикновено до ориентация на производителите към краткосрочни инвестиционни програми. Това от своя страна предизвиква съкращаване на *"второстепенните"* разходи (например за сервиз) и намаляване на разходите за предпродажбено окомплектоване на детайли, водещо до появата на пазара на *"сурови"* изделия. Накрая се стига до ориентация към модел, при който извежданото на пазара изделие след стадия на огромно търсене не преминава към етап на устойчиво търсене, а към друг модел на търсене на по-привлекателни характеристики. Всички тези фактори водят в крайна сметка до нарастване на финансовите рискове за потребителя.

7. Неточни изисквания към проектираната ИС, неадекватно макетиране и тестване на работния модел. Тези проблеми са много популярни - потребителят не знае какво иска, а изпълнителят не знае какво не може.

8. Високи норми на заработка, установени за един сътрудник. Макар че стойностите за отделните отрасли на промишлеността се различават съществено, препоръчва се те да бъдат разглеждани в съответствие с работната заплата на сътрудника и редица други финансови показатели.

9. Слаба защита на ИС от дефекти при проектирането на системата. Примери в това отношение са: грешна схема на организация на електрозахранването, отсъствие на съответни мерки по осигуряване на секретност, невярна система за контрол на целостта на данните, плюс защита от несанкциониран достъп, а също кражби както на информация, така и на техника.

10. Неефективна система за възстановяване на частичната работоспособност на системата при форсмажорни ситуации.

Фактори, влияещи на намаляването на стойността на ТСО

1. Наличие на автоматично управление на работните места и програмите за инвентаризация на системата.

2. Вградена антивирусна програма на клиентските места и сървърите.

3. Поддръжка на системата от средства за мрежово управление.

4. Наличие на централизирана специализирана служба за решаване на възможните проблеми.

5. Използване на специално адаптирани за конкретната система компоненти на програмното осигуряване, ненарушаващи целостта на архитектурата на системата.

6. Вградена система за откриване на грешки, предназначена за следене и предупреждение при непланирани престои.

7. Потребителите имат достъп само до онези програми и функции, които са необходими за изпълнение на работните задължения.

8. Стандартизирани апаратни и програмни компоненти на работните места (минимално 80% от общия брой потребители).

9. Наличие на система за защита на жизненоважните данни и план за максимално бързото им възстановяване.

10. Централизирано закупуване на идентични модели техника от един производител.

11. Система за мониторинг и следене за измененията на конфигурацията на работните места.

12. Последователна унификация и замяна на проблемните компоненти на архитектурата с нови, отговарящи на инициативите за намаляване на стойността и съкращаване срока за възвръщане на инвестициите.

13. Изследване на разходните компоненти на TCO и определяне на критичните пунктове в инвестиционната програма.

14. Обучение на потребителите на ефективни методи на работа със системата и приложенията.

15. Обучение и сертификация на административния персонал по технологиите, използвани в мрежата.

16. Наличие на мотивация у персонала за предоставяне на високо ниво на сервизно обслужване.

Оценка на коефициента на възвръщаемост на инвестициите (*Return On Investment*)

През последните години, когато се смята, че "*разцветът*" на необмислените инвестиции вече е преминал, от информационните технологии се изисква и реална полза – необходимо е да се изясни защо трябва да се инвестира в тяхното развитие и защо в такива размери.

Най-сложна в този план е ИС, в чието внедряване ръководството на фирмата като правило вижда само допълнителни разходи и го разглежда като нещо, в което само се инвестират средства, без да има възвръщаемост от тях. Ето защо е нужна добра обосновка относно инвестирането в ИС както и правилно определяне на критериите, по които се прави избор на един или друг вариант на защита. [8]

За да се оценят и обосноват икономически внасяните в бизнеса изменения, се използва финансовият показател *"възвръщаемост на инвестициите"* (*Return On Investment* - ROI). В общия случай той се определя по следната формула:

$$ROI = \frac{Доходи - Разходи}{Инвестиции}$$, където:

[8] IT-SECURITY. Экономическая эффективность и управление рисками. Infotecs Internet Trust, http://www.iitrust.ru/articles/it-sec_risk.htm.

Доходи са доходите на компанията за отчетния период (година);
Разходи – разходите на компанията за отчетния период (година);
Инвестиции - инвестициите, направени от компанията.

ROI е интегрален критерий, позволяващ да се оцени доколко ефективно работят вложените в компанията средства.

За да се разбере какво е влиянието на инвестициите за ИС върху ROI, може да се изчисли помощното *roi*, обусловено само от измененията в системата за ИС:

$roi = \frac{\Delta Доходи - \Delta Разходи}{\Delta Инвестиции}$, където:

roi е показателят на изменението на ROI, обусловен от инвестиции в ИС;
$\Delta Доходи$ - изменението в доходите, обусловено от инвестиции за ИС;
$\Delta Разходи$ - изменението в разходите, обусловено от инвестиции в ИС;
$\Delta Инвестиции$ - инвестициите, направени в ИС.

Нека ROI до внасянето на измененията в системата за ИС в компанията означим с ROI_{old}, съответно направените инвестиции - $И_{old}$, а планираните инвестиции $\Delta И$. Тогава след внедряване на проекта ROI ще се определя по следната формула:

$$ROI = ROI_{old} * \frac{И_{old}}{И_{old} + \Delta И} + roi * \frac{\Delta И}{И_{old} + \Delta И}$$

В зависимост от ефективности на проекта по ИС и отношението на размера на инвестициите в него към общите инвестиции в компанията общата ефективност може да се промени, така че: *roi* > *ROI*; *roi* < *ROI* или *roi* = *ROI*.

Изменение на приходите

Системата за ИС няма пряко влияние върху изменението на доходите на компанията, затова като правило не би трябвало да се очаква увеличаване на приходите й след инвестиции в ИС. $\Delta Доходи$ обаче не трябва веднага да се приравнява на нула, тъй като съществуват редица стандартни информационни системи, в които грамотно построената система за защита на информацията може да окаже влияние върху ръста на доходите на компанията. Например съгласно изследвания на *PriceWaterhouse Coopers* именно недостатъчната сигурност на електронните разплащания е основна бариера за потребителите, т.е. реализацията на системата за ИС в такива случаи обуславя доверието на клиентите, а значи и притока на пари.

Сега сериозно конкурентно предимство в системите *"банка-клиент"* или електронните търговски системи представлява прилагането на *сертифицирана криптография*. Използването на такива решения при построяването

на системата за ИС може значително да допринесе за увеличаването на доходите на компанията.

Внедряването на системата за ИС като правило води до по-продуктивно използване на работното време на сътрудниците. Това е свързано с ограничаване достъпа до информация, която не е необходима за работа, например развлекателни сайтове, както и с намаляване на неслужебния обмен на информация. Несъмнено съществуват и други фактори за ръста на доходите. Намаляване на доходите не настъпва, т.е. $\Delta Доходи$ не е отрицателна величина.

Изменение на разходите

Не е възможно да се работи въобще без разходи - операционни загуби има винаги. Това са разходи за разработка на проекта, за обучение, а понякога и стойността на средствата за защита на информация (характерно за аутсорсинга например). Но има съставни компоненти, които могат да ги компенсират и даже да доведат до намаляване на разходите след реализацията на проекта.

Главната причина, поради която се строи или модернизира системата за ИС, е *увеличаването на сигурността от рискове*. Очакваната стойност на рисковете може да се изчисли, например за година, по следния начин:

$Risk = \sum V_{risk} * C_{risk}$, където:

V_{risk} е вероятността за реализация на риска;

C_{risk} - загубите от реализацията на риска.

От своя страна V_{risk} се определя по формулата:

$V_{risk} = \sum V_{atack} * S_{risk}$, където:

V_{atack} е вероятността за опит за атака/инцидент;

S_{risk} - сигурността от тази атака/инцидент (от 0 до 1: 0 - висока, 1 - ниска).

Пресмятайки разликата в стойностите на рисковете до и след внедряване/изменение на системата за ИС, се определя понижаването на разходите за неутрализиране на загубите.

Съществува и мнение, че системата за ИС води до намаляване на операционните разходи за администриране. Но това не е съвсем точно. Ако не е отделяно никакво или почти никакво внимание на защитата на информацията, то допълнителни разходи ще изисква дори използването на междумрежови екран (да не говорим за построяването на по-сложни системи). Опростяване на администрирането е възможно само в случай на внасяне на

изменения във вече съществуваща система, например при преход към по-прогресивна технология с мощни и гъвкави средства за управление, смяна на доставчика на услуги и др. По такъв начин в повечето проекти, свързани с появата на нова функционалност на системата за защита, не може да се очаква намаляване на разходите и величината $\Delta Разходи$ може да бъде както отрицателна, така и положителна.

След изчисляването на *roi* е необходимо то да бъде сравнено със следните "*прагови величини*":

1. roi < 0, т.е. ефективността на проекта за ИС е отрицателна. Това е най-лошият вариант, но той не е рядко срещан. Има и още по-лоша възможност - когато *roi* на проекта за ИС е толкова отрицателен, че поради това отрицателен може да стане и ROI коефициентът на компанията;

2. ROI > roi > 0, т.е. внедряването на проекта за ИС ще доведе до намаляване на общия ROI коефициент на компанията;

3. roi > ROI, т.е. внедряването на проекта ще допринесе за увеличаване на общия коефициент ROI на компанията.

В първия случай всеки икономист би се отказал от проекта, тъй като той носи загуби и трябва да се замисли дали си струва да го реализира. Във втория случай проектът намалява общата ефективност, но все пак е доходоносен. В случай 3 проектът веднага може да бъде предложен за внедряване, защото се оказва печеливш и води до повишаване на ефективността. Но и тук може да се допусне грешка, тъй като е необходимо управление на рисковете и колкото и да е странно, дори в първия вариант отказът от проекта за ИС е преждевременен (разбира се, ако ROI е все пак положителна величина).

Управление на рисковете

За нагледност ще приведем пример с компания, която застрахова своя офис в случай на пожар. Доходите по-скоро няма да се изменят, разходите ще се определят от стойността на застрахователната полица и увеличаването на сигурността от риск. Очевидно е обаче, че стойността на полицата е много по-голяма, отколкото вероятните загуби от пожар. Ако се пресметне *roi* от покупката на застрахователна полица, то тази величина ще бъде отрицателна. Тогава защо застрахователният институт е толкова популярен?

В този случай стойността на щетата от такова произшествие като пожар е значителна и ако въпреки ниската вероятност той настъпи, то това ще е удар за компанията, който съществено ще подкопае целия й бизнес, а може и да доведе до банкрут.

Аналогично, при оценка на рисковете за ИС е необходимо да се отчита не само произведението на щетата с вероятността за нейното възникване, но и абсолютната стойност на тази щета. Ако стойността на загубата е съизмерима с тази на цялата кампания, то даже при ниска (но, разбира се, не

около нулата) вероятност трябва да се повлияе на проектирането на системата за ИС.

Да разгледаме неголяма, бурно развиваща се Интернет-компания, предоставяща хостинг, за която ще направим примерна оценка на ефективността на проекта за ИС. В компанията са инвестирани 100 000 USD, а разликата между доходите и разходите е 40 000 USD годишно, т.е. *ROI* = 0.4. В резултат от мощна атака на даваните под аренда сървъри (например унищожаване на цялата им информация) всички клиенти напускат, т.е. компанията ще бъде закрита. Щетата може да се приравни на стойността на целия проект - 100 000 USD. С вероятност 10% в текущата година успешно е проведена мощна "*хакерска*" атака. Така съществуващият риск се оценява на 10 000 USD годишно. Инсталирането на мощен междумрежови екран със система за откриване на атаки струва около 10 000 USD и ще изисква операционни разходи например от около 1000 USD на месец (за техническа поддръжка, обучение, заплати, амортизация и т.н.). Реализацията на този проект за защита ще измени вероятността за успешна атака 10 пъти и ще съкрати стойността на риска до 1000 USD на година.

Тогава *roi* се пресмята по следния начин:

$$roi = \frac{9000 - 12 * 1000}{10000} = -30\%$$

Следователно в този случай икономическата изгода е отрицателна.

Нека предположим, че всяка година от 10 такива неголеми Интернет-компании една се закрива вследствие на хакерска атака, а очакваният "*срок на живот*" на компанията е 5 години. Готова ли е тя да работи в условията на такава неопределеност? Вероятно, не.

Може ли управлението на рисковете да се формализира?

Предварително, в зависимост от техните вероятности *Vrisk* и загубите *Crisk*, ще разделим всички рискове на категории и ще получим следната таблица (стойностите са взети условно).

Таблица 3

Категории рискове

		Вероятности *Vrisk*		
		Несъществена (<1%)	Съществена (от 1% до 10%)	Висока (по-голяма от 10%)
Загуби *Crisk*	Незначителни (< 1% от стойността на предприятието)	1	2	2
	Значителни (от 1% до 10%)	2	2	2
	Критично високи (> 10%)	2	3a	3b

Рисковете от категория 1 са несъществени за компанията даже в случай, че те се осъществяват. Освен това тяхната вероятност не е голяма и ще има незначително влияние при пресмятането на икономическия ефект.

Рисковете от категория 2 могат да бъдат добре оценени при пресмятане на *roi* и не се изисква допълнително внимание.

Рисковете от категория 3, имащи вероятност, която не е близка до нулевата, и можещи да доведат до критични за компанията загуби, изискват допълнително внимание и не мога да бъдат оценени по методиката за пресмятане на *roi* (макар че очевидно рискове с висока вероятност по-скоро ще допринесат съществено за пресмятането на *roi*).

Рисковете от подкатегория *3b* са неприемливи за организацията и трябва да бъдат неутрализирани във всеки случай, дори ако за това трябва да се преустроят всички бизнес-процеси на компанията. Необходимо е да се отбележи, че по-скоро няма да има толкова вероятни и критични рискове.

Фактът за наличие на рискове от подкатегория *3a* трябва да бъде доведен до знанието на ръководството на компанията и вече то да вземе решение доколко е възможно да се продължава дейността при такива условия.

Използвайки инструментариума за пресмятане на *roi* и сравняването му с общия ROI коефициент на компанията, могат да се направят изводи за необходимостта, общата ефективност на проекта за ИС, както и да се съпоставят няколко проекта.

Препоръчва се окончателният избор на един или друг проект да се направи по *критерия за максимално roi*, при условие на неутрализиране в дадения проект на рисковете със съществена вероятност, можещи да доведат до критични загуби за компанията.

Методиката на *Gartner Group* за оценка на съвкупната стойност на собствеността – TCO, е приложима и при оценката на икономическата ефективност на системите за ИС. Заедно с TCO могат да се използват различни методи за пресмятане на възвръщаемостта на инвестициите (ROI). Според някои автори[9] достатъчно резултативно е *използването на методиката TCO, приложена към разходната част и ROI относно направените инвестиции.*

Оценка на ефективността на инвестициите, прилагани в технологии за сигурност (*Applied Information Economics - AIE)*

Методът е разработена от Дъглас Хабард, ръководител на компанията "*Hubbard Ross".*[10] Тази компания, основана през март 1999 г., става първата организация, която използва методиката AIE за анализ на ефективността на

[9] *Петренко, С., С. Симонов, Р. Кислов* . Цит. съч.

[10] *Hubbard, D*. How to Measure Anything: Finding the Value of Intangibles in Business. John Wily & Sons, due for release in July 20, 2007.

инвестициите в технологиите за сигурност от финансова и икономическа гледна точка.

AIE обединява теориите за управление на портфейлите, традиционните счетоводни подходи (вкл. възвръщаемост на инвестициите ROI) и статистически методи, с които може да се изрази неопределеност в количествените оценки. С него може да се построи кривата на вероятностното разпределение, описващо очакваните резултати, да се оцени рискът и възвръщаемостта на инвестициите.[11]

Тази методика позволява да се повиши точността на показателя "*действителна икономическа стойност на инвестициите в технологии за сигурност"* за сметка на определянето на ROI до и след инвестиране. Прилагането на AIE позволява да се съкрати неопределеността на разходите, рисковете и изгодите, в т. ч. и неочевидните.

Отчетът за свършената работа включва в себе си получените сведения, препоръки и коментари на консултантите, както и сводна таблица, отразяваща взаимното влияние на разходите, печалбата и рисковете.

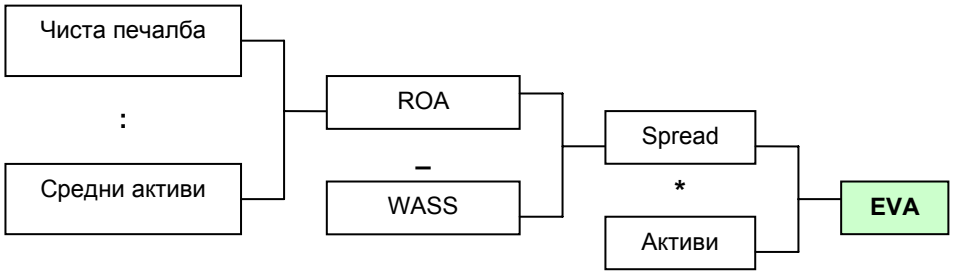
Метод на добавената икономическа стойност (*Economic Value Added - EVA*)

Консултантската компания "*Stern&Stewart Co*.", основана през 1982 г., се специализира в оценката на акционерния капитал с нов инструментариум за финансов анализ. Тя е една от първите, разработила собствена методика за изчисляване на *добавената икономическа стойност - EVA*.

В системите за управление, ориентирани към стойността, се смята, че стойността на компанията се определя от дисконтираната величина на бъдещите парични потоци *Cash Flow* (CF), а добавена стойност *Value Added* (VA) възниква в случая, когато рентабилността на активите ROA на компанията превишава среднопретеглените загуби на капитал *Weighted Average Cost of Capital* (WACC).

Фигура

Модел на добавената икономическа стойност (EVA)



[11] CIO, 2002, N 4.

Разликата между рентабилността на активите и среднопретеглените загуби на капитал се означават с термина "*spread*". С други думи, стойността на компанията се увеличава, ако *ROA* > *WACC*, и намалява, ако *ROA* < *WACC*. Именно на този базов принцип е основана концепцията за икономическата добавена стойност[12] (вж. фигурата).

Ключов момент на концепцията за икономическата добавена стойност е пресмятането на *среднопретеглените загуби на капитала WACC*.

За да изясним по-добре този модел, ще разгледаме елементарен пример. Структура на пасива от баланса (структурата на капитала) на компания *X* е следната: 40% - собствен капитал; 30% - краткосрочни банкови кредити; 30% - кредиторска задлъжнялост пред доставчици. Стойността на кредиторската задлъжнялост е оценена от финансовия директор на 24% годишно (въз основа на разликата между цената на заплащане на ресурсите веднага и цената на заплащане след месец, съставяща около 2%). Стойността на краткосрочните банкови кредити е 15% годишно, а собственият капитал, формиран от учредителите на компанията, се оценява на 17% годишно. В опростена форма среднопретеглените разходи за използване на капитала могат да се пресметнат, като се умножи делът на една или друга част от капитала на компанията (собствен капитал, краткосрочни кредити, кредиторска задлъжнялост) на неговата стойност, измерена в проценти за година, и получените величини се съберат:

0.4*17% + 0.3*15% + 0.3*24% = 18.5%.

Това означава, че компанията може да разчита на увеличение на своята капитал единствено ако рентабилността на нейните активи надвишава 18.5% (среднопретеглените разходи на капитал). В противен случай, компанията работи само за да може за изплати разходите, свързани с привлечения и използвания капитал.

Нека допуснем, че средните активи на компанията през отчетната година са 500 000 EUR, а рентабилността на активите (съотношението на чистата печалба към величината на активите) - 20%. Тогава можем да констатираме създаване на икономическа добавена стойност в размер на 7500 EUR.

[(20% - 185%) * 500 000] = 7500.

Ако рентабилността на активите на компанията е например,16% годишно, то стойността на компанията ще се намали със 7500 EUR.

Метод на изходната икономическа стойност (*Economic Value Sourced - EVS)*

Този метод е разработен от компанията "*Cawly & the Meta Group",*[13] която оказва услуги на средни и големи компании, измервайки количествено

[12] *Толкач, В*. Balanced Scorecard - взгляд в будущее, http://quality.eup.ru/MATERIALY5/bsfuture.html.

[13] *Bailey, J., A. Drommi, J. Ingalsbe, N. Mead, D. Shoemaker*. Models for Assessing the Cost and Value of Software Assurance, 2007.

възвръщаемостта от инвестициите в технологии за сигурност. Той предполага точно пресмятане на всички възможни рискове за бизнеса, свързани с внедряването и функционирането на корпоративната система за защита на информацията. Разширено е използването на такива инструментални средства за оценка на ИТ като *добавената икономическа стойност* (EVA), *вътрешната норма на рентабилност* (IRR) и *възвръщаемостта на инвестициите* (ROI) за сметка на определянето и въвличането в оценъчния процес на параметрите на три стратегически фактора: *редукция на риска*, *увеличаване на продуктивността* и *намаляване на времето.*

Управление на портфейла на активите за информационна сигурност (*Portfolio Management - PM)*

Тази методика предполага, че компаниите управляват технологиите за сигурност така, както биха управлявали акционерен инвестиционен фонд, отчитайки обема, размера, срока, печалбата и риска на всяка инвестиция. Портфейлът на активите на технологиите за сигурност се състои от *статични и динамични активи.*

Към *статичните* се отнасят: апаратно-програмните средства за защита на информацията, операционните системи и пакетите приложни програми, мрежовото оборудване и програмното осигуряване, данните и информацията, оказваните услуги, човешките ресурси и др. В състава на *динамичните активи* влизат различни проекти по разширяване и обновяване на целия портфейл на активите, знания и опит, интелектуален капитал и т.н.

По този начин управлението на портфейла на активите на технологиите за сигурност представлява непрекъснат анализ на взаимодействието на възникващите възможности и наличните ресурси. Непрекъснатостта на процеса на управление е свързана с външните изменения (например на ситуацията на пазара, на позициите на конкурента и др.) и с вътрешни изменения (например в стратегията на компанията, в каналите за дистрибуция, в номенклатурата на стоките и услугите и т.н.). Директорът на службата за сигурност се разглежда като "*фондов мениджър*", който управлява инвестициите в технологии за сигурност, стремейки се към максимизация на печалбата.

Оценка на действителните възможности (*Real Option Valuation - ROV*)

ROV [14] е ключова концепция за построяване на модел на "*гъвкави възможности на компанията*" в бъдеще. Тази методика разглежда технологиите за сигурност в качеството на набор от възможности с голяма степен на тяхната детайлизация. Правилното решение се приема след щателен анализ на широк спектър от показатели и разглеждане на множество резултати или варианти на бъдещи сценарии, които в методиката се наричат

[14] http://www.realoptionsvaluation.com/.

"динамичен план за вземане на управленски решения" или *"гъвкавост"*, която ще помогне на организациите по-добре да се адаптират или изменят своя курс в областта на ИС.

Метод на жизнения цикъл на изкуствените системи (*System Life Cycle Analysis - SLCA)* [15]

В основата на метода лежи измерването на "*идеалността*" на корпоративната система за защита на информацията – *съотношение на нейните полезни фактори към сумата на вредните фактори и тези за разплащане за изпълнението на полезните функции*. Оценката се предхожда от съвместна работа на аналитика и водещите специалисти, изследващи компанията, по съставянето на полезни, негативни и разходни фактори на бизнес-системата, без използване на система за сигурност и присвояването на определени теглови коефициенти. Създава се модел на изчисляване, описващ състоянието без система за сигурност. След това в модела се въвеждат описаните фактори, очакваните изменения и се правят пресмятания на нивото на развитие на компанията с корпоративна система за защита на информацията. По този начин се строят традиционните модели *Какво е* и *Какво ще бъде*, отчитайки влиянието на полезните, негативните и разходните фактори на бизнес-системата.

Методът SLCA се прилага на етапите на:

- предпроектната подготовка, за предварителна оценка на ефекта от внедряването на нова система за сигурност или за модернизация на съществуващата;
- разработка на техническото задание на АС в защитено изпълнение;
- провеждане на одит на ИС на предприятието, за проектна оценка на очаквания ефект;
- приемане на АС в защитено изпълнение на експлоатацията или при завършване периода на опитната експлоатация за потвърждаване на пресметнатия ефект, негово уточняване и получаване на нова *точка на отчитане* (ново ниво на организационно-технологическото развитие на компанията) за последващи оценки на ефекта от внедряването на технологии за сигурност.

Система на балансираните показатели (*Balanced Scorecard - BSC)*

Това е методика, в рамките на която традиционните показатели на финансовите отчети се обединяват с операционните параметри, като така се създава достатъчно обща схема, позволяваща да се оценят нематериалните активи: нивото на корпоративните иновации, степента на удовлетвореност на сътрудниците, ефективността на приложенията и т.н.

---

[15] *Петренко, С. А., Е. М. Терехова*. Оценка затрат на защиту информации...

Методиката за първи път е представена през 1990 г. от Дейвид Нортън, сега ръководител на *Balanced Scorecard Collaborative*, и Роберт Каплан, професор в *Harvard Business School*. Традиционната концепция BSC предполага формиране на т. нар. стратегически карти, групиращи целите и показателите в следните четири *категории*:[16]

- *финанси* - финансови цели за развитие и резултати от работата на компанията (печалба, рентабилност и т.н.);
- *клиенти и пазари* - цели за присъствие на пазара и показатели за качеството на обслужване на клиентите (завладяване на пазари и територии за продажба, време за изпълнение на поръчката и т.н.);
- *процеси* - изисквания към ефективността на процесите (стойност, време, количество грешки, рискове и т.н.);
- *развитие* - цели на търсене на нови технологии и повишаване квалификацията на персонала и т.н.

Между всички показатели съществуват причинно-следствени влияния. Например колкото по-висока е квалификацията на персонала и е подобра технологията за водене на бизнеса, толкова по-просто се поддържат бизнес-процесите. Това на свой ред спомага за по-качественото обслужване на клиентите и реализацията на конкурентните предимства, а следователно и за достигане на запланираните финансови показатели. По този начин крайната цел на функциониране за компанията са финансовите показатели, докато другите перспективи определят бъдещия й потенциал.

По подобен начин може да се определят ключовите показатели за функциониране на службите по ИС на компанията и да се задават перспективите за развитие на корпоративните системи за защита на информацията. Поради косвеното въздействие на технологиите за сигурност върху финансовите показатели на предприятието, те трябва да се разглеждат от гледна точка на приноса им в развитието на бизнеса.

Метод на очакваните загуби (*Annualized Loss Expectancy)*

Методът е основан на емпиричния опит на организацията и сведенията за заплахите, загубите от вируси, отражението на сервизните нападения и т.н. Изчисляват се загубите, които може да претърпи компанията, от нарушения на политиката за сигурност и се сравняват с инвестициите в сигурност, насочени към предотвратяване на нарушенията.

За да се *смекчат* очакваните загуби, компаниите трябва да инвестират средства в инструменти за осигуряване на сигурност: мрежови екрани, системи за откриване на нападения, антивируси и т.н. Трябва да се отбележи, че няма съвършена система за ИС. За определяне ефекта от нейното внедряване е необходимо да се изчисли *средногодишният показател на*

[16] Balanced Scorecard Basics, http://www.balancedscorecard.org/.

очакваните загуби (Annualized Loss Expectancy - ALE).[17] По оценки на експерти ефективността на правилно установена и настроена система за защита за предупреждение или намаляване на загубите от нарушаване на политиката по сигурност може да достигне 85%.

$AS = ALE * E - AC$, където:

AS (*Annual Saving*) са ежегодните спестявания;
ALE (*Annualised Loss Expectancy*) – показателят на очакваните загуби;
E – ефективността на системата за защита;
AC (*Annual Cost*) - ежегодните разходи за сигурност.

Метод за оценка на свойствата на системата за ИС (*Security Attribute Evaluation Method - SAEM* [18]

Методът е разработен в *Carnegie Melon University* и е основан на сравняването на различни архитектури на системи за ИС за финансова оценка на изгодите от тяхното внедряване.

SAEM се заключава в това, че оценявайки съществуващите рискове, могат да се предложат различни проекти на ИС, различаващи се по стойност и ефективност. Недостатък на метода е, че най-често сигурността се намира извън компетенциите на мениджърите, занимаващи се с оценката на ефективността, а специалистите по информационна сигурност рядко имат точни данни относно изгодите от технологията. Затова се налага те да се уповават на опита и интуицията си и на тази основа да вземат решения. Този метод обаче може за бъде използван за представяне на комплекс от разнообразни мерки по информационна сигурност и за поддържане вземането на решения при избора на едни или други мероприятия.

Метод за анализ на дървото на грешките (*Fault Tree Analysis - FTA)*

Това е нетрадиционен инструмент за оценка на изгодите. Целта на приложението на този метод е да се покаже в какво се състоят причините за нарушенията на политиката за сигурност и какви изглаждащи ответни мерки могат да бъдат прилагани. Последните са насочени към достигане на следните ефекти: *намаляване вероятността за настъпване на инцидент и/или на последствията, ако това все пак се случи*. Мерките, понижаващи вероятността, се наричат *профилактични*, а тези, намаляващи последствията - *лечебни* (например наличие на резервни режими на работа).

Метод на дисконтираните парични потоци (*Discounted Cash Flows*)

Бъдещите постъпления на парични средства (за намаляване на щетата) трябва да се *дисконтират*, т.е. да са приведени към текущата стойност. За целта се използва нормата за дисконтиране, чиято величина отразява риско-

[17] *Петренко, С. А., С. В. Симонов*. Экономически оправданная сигурность. Москва: "ДМК Пресс", 2003.
[18] Разработка и защита на бюджета за информационна сигурност. - CIO, 2006, N 8.

вете, свързани с обезценяването на парите поради инфлация и с възможност за неуспех на инвестиционния проект, който може да не доведе до очаквания ефект. С други думи, колкото по-високи са рисковете, свързани с проекта, толкова по-голяма е ставката за дисконтиране, която отразява и общото ниво на стойността на кредита за инвестиции.

Нерядко ставката за дисконтиране се определя от показателя *"среднопретеглена стойност на капитала"* (*Weighted Average Cost of Capital – WACC*). Това е средна норма на дохода на вложения капитал, която трябва да се изплати за неговото използване. Обикновено WACC се разглежда като минимална норма на отдаване, която трябва да бъде осигурена от инвестиционния проект.

За непосредствена оценка на ефективността на инвестициите се използва показателят *"чиста текуща стойност"* (*Net Present Value* – NPV). По същество това е текущата стойност на бъдещите парични потоци на инвестиционния проект с отчитане на дисконтирането и инвестициите. Този показател се пресмята по следната формула:

$$NPV = \sum_{i=1}^{N} \frac{CF_i}{(1+r)^i} - CF_0$$, където:

CF_i е чистият паричен поток за i -я период;

CF_0 – началните инвестиции;

r – дисконтовата норма (стойността на капитала, привлечен за инвестиционния проект).

При $NPV \geq 0$ се смята, че капиталовложението е ефективно. При сравняването на няколко проекта се приема онзи от тях, който има по-голямо значение за NPV.

За оценката на ефективността на инвестициите при създаването на система за защита на информацията е недостатъчно само определянето на показателите. Необходимо е още да се отчетат *рисковете, свързани с реализацията на проекта*. Това могат да бъдат рискове, свързани с конкретни доставчици на средства за защита на информация, или рискове, свързани с компетентността и опита на екипа, отговарящ за внедряването на системата.

Освен това е полезно да се проведе *анализ на чувствителността на получените показатели.*

Не трябва да се забравя и това, че не цялата щета от реализацията на заплахи за ИС може еднозначно да получи парично изражение – уронването на интелектуалната собственост на компанията може да доведе до такива последствия като загуба на пазарни позиции, загуба на постоянни и временни конкурентни предимства или намаляване стойността на търговската марка.

8.IV.2009 г.