

Zarządzanie organizacjami – finanse, produkcja, informacja

**Management of Organizations –
Finances, Production, Information**

**Redakcja naukowa
Honorata Howaniec, Wiesław Waszkielewicz**



Bielsko-Biała 2009

Szczegół.

Wstęp
Budżet I
FINANSOWE ASPEKTY Zarządzania przedsiębiorstwem

- 1.1. Sistem zarządzania zatrudnieniem jako ochrona pozytywnego potencjału dobrej jakości i etyczno-prawnego przekazywanego do końca 2009 r.
K. F. Kowalczyk, B. A. Szlakiro, Bielsko-Biała, Wydawnictwo Uniwersyteckie, 2009
1.2. Rynkowość zarządzania zatrudnieniem Bielsko-Biała, 2009, kwiecień 2010

Zarządzanie organizacjami - finanse, produkcja, informacja

1.3. Formy finansowania działalności gospodarczej jednostek budżetowych MONOGRAFIA

Management of Organizations - Finances, Production, Information

- 1.4. Rola sektora cywilnego i przedsiębiorstw MŚP
Anna Schubert, A. Szalik
Redakcja naukowa
1.5. Zarządzanie finansami i produkcją w przedsiębiorstwie
Rynek i Honorata Howaniec, Wiesław Waszkielewicz
1.6. Organizacja i zarządzanie produkcją
Honorata Waszkielewicz, Wiesław Waszkielewicz
1.7. Wieloletni rozwój gospodarki polskiej i międzynarodowej
w latach 2001-09
Jan Tadeusz Duda, Andrzej Augustyniak
1.8. Periodicity of Selected Metal Prices in London Metal Exchange
in The Light of 2008 World Financial Crisis
Jan Tadeusz Duda, Andrzej Augustyniak
1.9. Zarządzanie metaliami strategicznymi w perspektywie europejskiej
Tadeusz Duda, 2009
1.10. Zarządzanie metaliami strategicznymi w perspektywie europejskiej
Tadeusz Duda, 2009
1.11. Periodicity of Selected Metal Prices in London Metal Exchange
in The Light of 2008 World Financial Crisis
Jan Tadeusz Duda, Andrzej Augustyniak
1.12. Zarządzanie metaliami strategicznymi w perspektywie europejskiej
Tadeusz Duda, 2009
Bielsko-Biała, 2009

Redakcja naukowa:
dr hab. inż., prof. nadzw., Wiesław Waszkielewicz
dr inż. Honorata Howaniec

Recenzenci:
prof. nadzw. dr hab. Janusz Czekaj
prof. zw. dr hab. Adam Peszko
prof. zw. dr hab. inż. Jan T. Duda

Sekretarz Redakcji: mgr Grzegorz Zamorowski

Skład i łamanie: Janusz Rus

© Copyright by
Katedra Zarządzania WZiI ATH,
Katedra Marketingu i Zarządzania Produkcją WZ AGH,

ISBN 978-83-60714-79-9

Wydawnictwo
Akademii Techniczno-Humanistycznej

Bielsko-Biała, 2009

Spis treści

Wstęp	7
Rozdział I	
FINANSOWE ASPEKTY ZARZĄDZANIA PRZEDSIĘBIORSTWEM	
1.1. Система управления затратами как основа повышения эффективности деятельности металлургического предприятия, К. Ф. Ковальчук, И. А. Шапиро, Веслав Вашкевич	11
1.2. Efektywność zarządzania strumieniami finansowymi w uczelni publicznej w perspektywie zmian finansowania szkolnictwa wyższego, Małgorzata Jucha	25
1.3. Czynniki wpływające na strukturę kapitału przedsiębiorstwa w ocenie menedżerów, Grażyna Musialik	37
1.4. Formy finansowania przedsiębiorstw w aspekcie oceny struktury finansowania majątku w wybranym przedsiębiorstwie produkcyjnym, Iwetta Pardela	44
1.5. Małopolskie MSP korzystające z funduszy strukturalnych, Agnieszka Peszko	53
1.6. Zewnętrzne źródła finansowania projektów ekologicznych w małych i średnich polskich przedsiębiorstwach, Bogumiła Smolarz	63
1.7. Rola venture capital w finansowaniu działalności MŚP, Anna Sośnicka-Łajczak	74
1.8. Zarządzanie wartością reputacji firmy, Ryszard Budzik, Piotr Okrzesik, Małgorzata Jakubiec	82
1.9. Этапы антикризисного управления, Левандовский Владислав	92
1.10. Wieloczynnikowa predykcja matematyczna cen metali kolorowych w kryzysie roku 2008/9, Jan Tadeusz Duda, Andrzej Augustynek	98
1.11. Periodicity of Selected Metals Prices in London Metal Exchange in The Light of 2008 World Economy Crisis, Jan Tadeusz Duda, Andrzej Augustynek	112
1.12. Zastosowanie metod algorytmicznych w prognozowaniu szeregów finansowych, Tomasz Pełech-Pilichowski	123

Rozdział II**INŻYNIERIA PRODUKCJI, ORGANIZACJA PRACY
I INFORMACJA W ZARZĄDZANIU PRZEDSIĘBIORSTWEM**

2.1.	Procesowe podejście do projektowania ukierunowanych form struktury systemów wytwarzania, Kamil Czajka, Wiesław Waszkielewicz	135
2.2.	Koncepcja struktury h-chaotycznej wytwarzania, Marek Dudek	144
2.3.	Procedury zarządzania przepływem materiałów w przedsiębiorstwie przemysłowym, a wielkość zapasów produkcyjnych, Gabriela Mazur, Jacek Obrzud	153
2.4.	Повышение эффективности использования оборотных средств промышленного предприятия, Н. П. Козенкова, К. Ф. Ковальчук, Веслав Вашкелевич, Хонората Хованец .	161
2.5.	Rozwój i modele zarządzania jakością w administracji publicznej, Marcin Lis	174
2.6.	Synthesis of the Optimum Narrow-Band Non-Recursive Digital Filter, Kijko A. V., Petrov A. S.	187
2.7.	Problemy współczesnych form organizacji pracy w przedsiębiorstwie usługowym, Agnieszka Jagoda	193
2.8.	Advanced ergonomics analysis in automotive industry Branislav Mičeta, Ľuboslav Dulina	202
2.9.	Методы цифровой обработки информации в системах управления, Lyubomyr Petryshyn, Oleksiy Borysenko, Oleksandr Mal'ko	208
2.10.	Wywiad gospodarczy w systemie informacji przedsiębiorstwa, Marta Zembik	221
2.11.	Doskonalenie metodyki przeprowadzenia audytu z wykorzystaniem technologii komputerowych na Ukrainie, Wołodimir Szkwir, Iryna Borszczuk	230
2.12.	Dziennik ryzyka – zarys komputerowego wspomagania procesu zarządzania ryzykiem przedsięwzięć budowlanych, Aneta Madyda	239
2.13.	System elektronicznej komunikacji administracji publicznej województwa śląskiego, Konrad Sikora	253
2.14.	Wirtualizacja procesów biznesowych z wykorzystaniem semantycznych usług sieciowych, Ilona Pawełoszek-Korek	263
2.15.	Инвестиции в систему информационной безопасности, Сергей Охрименко	274
2.16.	Prevention From Penetration into Dynamic Database of Corporate Information Systems of Enterprises, V. Lahno, A.Petrov	282
	Noty o autorach	291

Contens

Introduction 7

Chapter I.**FINANCIAL ASPECTS OF ENTERPRISE MANAGEMENT**

1.1. Control System by Expenses as Basis of Increase Efficiency to Activity of Metallurgical Enterprise, К. Ф. Ковальчук, И. А. Шапиро, Веслав Вашкелевич	11
1.2. Effectiveness of Financial Flux Management in a Public University in the Prospect of Changes in the Financing of Higher Education, Małgorzata Jucha	25
1.3. Factors Influencing Corporate's Capital Structure in Opinions of Managers, Grażyna Musialik	37
1.4. Some Forms of Financing the Firm. Main Aspects of Examining the Structure of Financing in the Case of Manufacturing Company, Iwetta Pardela	44
1.5. Small and Midium Enterprises of Małopolska Region Benefiting from Structural Funds, Agnieszka Peszko	53
1.6. External Financial Sourcec of Ecological Projects in Small and Medium Polish Entepries, Bogumiła Smolarz	63
1.7. The Part of Venture Capital in the Financing of Small and Medium Enterprises Activities, Anna Sośnicka-Łajczak	74
1.8. Management of Enterprises' Goodwill Equity, Ryszard Budzik, Piotr Okrzesik, Małgorzata Jakubiec	82
1.9. Stages of Anti-Recessionary Management, Левандовский Владислав	92
1.10. Multifactor Mathematical Prediction of World Prices of Selected Non-iron Metals During the Crisis of 2008, Jan Tadeusz Duda, Andrzej Augustynek	98
1.11. Periodicity of Selected Metals Prices in London Metal Exchange in the Light of 2008 World Economy Crisis, Jan Tadeusz Duda, Andrzej Augustynek	112
1.12. An Application of Algorithmic Methods to Financial Time Series Forecasting, Tomasz Pełech-Pilichowski	123

Chapter II.

PRODUCTION ENGINEERING, WORK ORGANIZATION AND INFORMATION IN ENTERPRISE MANAGEMENT

2.1.	The Process-Oriented Approach for Designing Directed Manufacturing Systems Structures, Kamil Czajka, Wiesław Waszkiewicz	135
2.2.	H-Chaotic Concept of Manufacturing Structure, Marek Dudek	144
2.3.	The Material-Flow Management Procedures in Manufacturing Company With Reference to Level of Stock, Gabriela Mazur, Jacek Obrzud	153
2.4.	Increase of Efficiency of the Use of Circulating Assets of Industrial Enterprise, Н. П. Козенкова, К. Ф. Ковалчук, Веслав Вашкевич, Хонората Хованец	161
2.5.	Evolution and Models of Quality Management in Public Administration, Marcin Lis	174
2.6.	Synthesis of the Optimum Narrow-Band Non-Recursive Digital Filter, Kijko A. V., Petrov A. S.	187
2.7.	Modern Problems of Service Sector Work Organization, Agnieszka Jagoda	193
2.8.	Advanced Ergonomics Analysis in Automotive Industry, Branislav Mičeta, Ľuboslav Dulina	202
2.9.	Methods of Digital Information Processing in Management Systems, Lyubomyr Petryshyn, Oleksiy Borysenko, Oleksandr Mal'ko	208
2.10.	Business Intelligence as An Tool of An Economic Information System, Marta Zembik	221
2.11.	Development of Auditings Method by Using Computer Application, Wołodimir Szwir, Iryna Borszczuk	230
2.12.	The Risk Journal - the Proposal of Computer Support of the Risk Management Process in the Building Projects, Aneta Madyda	239
2.13.	The System of Electronic Communication of Public Administration in Silesia Voivodeship, Konrad Sikora.....	253
2.14.	Virtualization of Business Processes by Exploiting Semantic Web Services, Ilona Pawełoszek-Korek	263
2.15.	Investments in the System of Information Security, Сергей Охрименко	274
2.16.	Prevention from Penetration Into Dynamic Database of Corporate Information Systems of Enterprises, V. Lahno, A. Petrov	282
	Notes about authors	291

2.15.

ИНВЕСТИЦИИ В СИСТЕМУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сергей Охрименко

1. Введение

Сегодня возврат от инвестиций в информационные технологии стал темой повышенного интереса, причем особое внимание уделяется методам расчета возврата от инвестиций в систему информационной безопасности (СИБ) [5-9]

Под информационной безопасностью информационных систем понимается поддержание физической сохранности, доступности, конфиденциальности, достоверности и своевременности информации, а также гарантированной работоспособности средств, используемых для ввода, хранения, обработки и передачи данных. Проблема информационной безопасности носит комплексный характер и объединяет сочетание правовых, организационных и программно-технических мер. В последнее время отмечается пристальный интерес к экономическим аспектам проблемы информационной безопасности. Этот интерес объясняется не столько увеличением затрат на обеспечение информационной безопасности, которые отмечаются повсеместно, сколько необходимостью представлять экономические выкладки для разъяснения важности и целесообразности вложений в информационную безопасность для существующего бизнеса.

Экономика информационной безопасности (ЭИБ), как самостоятельное научное направление получило развитие в 90-х годах прошлого столетия. Истоками данного направления следует считать комплекс исследований и практических разработок, связанных с такими факторами, как:

- процессы совершенствования организационных форм использования вычислительной техники;
- заменой вычислительной базы и переходом к использованию новых информационных и коммуникационных технологий;

- разработкой операционных систем для персональных компьютеров;
- появлением специфических угроз (компьютерных вирусов);
- реализацией атак на информационные системы и другие.

«Идеальная» СИБ должна объединять в себе комплекс мер, таких как правовые, организационные, технические, экономические и морально-этические. Но создание именно «идеальной» системы возможно только по отношению к государственным информационным системам, чьи ресурсы защищаются специальными подразделениями. Применительно к деятельности коммерческих структур процессы проектирования, внедрения и эксплуатации СИБ сопряжены с огромными затратами, требуют наличия высококвалифицированных кадров и т.д., что является не всегда доступным.

2. Методики оценки

Практика оценки инвестиций в СИБ объединяет множество подходов, методов и методик. Традиционно обоснование расходов на безопасность было связано с расчетом «качественных» или «стратегических» показателей и доказывало, что без инвестирования в систему защиты информации компания (фирма) упускает более «осозаемые» выгоды. Существующие подходы можно условно разделить на две группы: макроэкономические и микроэкономические.

2.1. Макроэкономический подход

В числе основных методик инвестиционной привлекательности следует выделить три группы: традиционные финансовые, вероятностные методы и инструменты качественного анализа (эвристические).

Первая группа охватывает следующие:

- совокупная стоимость владения (TCO – Total Cost of Ownership) и дальнейшее развитие версии TCO - совокупной оценки возможностей (Total Value of Opportunity - TVO), которая должна оказать более заметное влияние на эффективность капиталовложений;
- рентабельность инвестиций (ROI – Return on Investment), и специализированная методика, ориентированная на систему информационной безопасности (ROSI – Retutn on Security Investment);
- экономическая привлекательность (EVA - Economic Value Added),
- чистая приведенная стоимость (NPV - Net Present Value),
- внутренняя норма рентабельности (IRR - Internal Rate of Return),
- быстрое экономическое обоснование (REJ - Rapid Economic Justification)
- совокупный экономический эффект (TEI - Total Economic Impact).

Вторая группа включает:

- справедливая цена опционов (ROV - Real Options Valuation)
- прикладная информационная экономика (AIE - Applied Information Economics)

Третья группа:

- система сбалансированных показателей (BSC - Balanced Scorecard)
- информационная экономика (IE - Information Economics)
- управление портфелем активов (Portfolio Management)
- система показателей ИТ (IT Scorecard)

Как отмечается в [23] «... до настоящего времени оценка инвестиционной привлекательности системы информационной безопасности затруднена из-за нехватки данных, недостаточности показателей эффективности и сложной природы системы безопасности. Многие руководители служб безопасности в настоящее время без инструментальных средств и данных, принимают решения, основываясь на опыте, суждениях и, чаще всего, знаниях, не подтвержденных статистическими данными и инструментальными средствами.»

2.2. Микроэкономический подход.

Группа микроэкономических показателей охватывает следующие:

- анализ минимизации затрат (CMA – Cost Minimization Analysis). Используется для сравнения стоимости двух и более методов устранения последствий с равной эффективностью. Данный метод требует оценки и расчета всех составляющих, определяющих затратную сторону – количество тестов, дополнительное оборудование и т.д.
- анализ «стоимость-эффективность» (CEA – Cost Effectiveness Analysis). Используется для сравнения разницы стоимости двух и более комплексов работ, эффективность которых различна, а результаты измеряются в одинаковых единицах измерения;
- анализ «затраты-выгода» (CBA – Cost Benefit Analysis). Применяется для определения финансовой выгоды по отношению к затратам. При этом и затраты и результаты выражаются в стоимостном выражении;
- метод ожидаемых потерь (ALE – Annualized Loss Expectancy) предусматривает определение потерь от нарушений политики безопасности и их сравнением с инвестициями в безопасность, направленными на предотвращение нарушений. В основу данного метода положен эмпирический опыт организаций и сведения об инцидентах (вторжениях, потерях от вирусов, отражении сервисных нападений и т.д.);
- метод оценки свойств системы безопасности (SAEM - Security Attribute Evaluation Method), основан на оценке существующих рисков и подготовке проектов по информационной безопасности, отличающихся стоимостью и эффективностью;
- анализ дерева ошибок (FTA - Fault Tree Analysis), предусматривает определение причин нарушения политики безопасности и выработку сглаживающих контмер. К последним относятся такие, как меры, снижающие вероятность инцидента (профилактические), снижающие последствия (лечебные);

- метод оценки угроз и рисков (TRA - Threat and Risk Assessment), предполагающий получение количественной оценки вероятностей наступления неблагоприятных событий и их последствий, для дальнейшего использования этих данных для определения ожидаемых потерь при отсутствии контрмер безопасности;
- моделирование угроз безопасности (STM – Security Threat Modeling). Данная методика базируется на анализе сценариев нападения, который определяет количество угроз безопасности, вычисление удельного веса критичности каждой угрозы, каналов воздействия на информационную систему и т.д.

По аналогии с медициной, представляется возможным использование дополнительного метода – анализ «стоимости болезни» (COI - Cost of Illness), используемый для учета и описания всех видов затрат по устранению последствий. Применительно к системе информационной безопасности «стоимость болезни» можно интерпретировать как «стоимость устранения инцидента». С помощью данного метода представляется возможным определение общих стоимостных границ комплекса мероприятий, выход за пределы которых свидетельствует о недостаточности проводимых мероприятий, либо их избыточности.

3. Расчет затрат

В основу приведенных методик положены расчеты затрат на обеспечение информационной безопасности. Они могут быть прямыми, непрямыми и нематериальными. Прямые затраты включают расходы на устранение последствий, дополнительные исследования и обследования компонент информационной системы, оплату работы привлекаемых экспертов, а также стоимость устранения побочных эффектов. Непрямые затраты – расходы издержки, связанные со снижением работоспособности информационной системы, потерей производительности, отказами отдельных сервисов и т.д. Все это может быть определено как «недополучение» прибыли.

Нематериальные затраты – субъективные факторы, влияющие на климат в организации (психологическое, эмоциональное и социальное состояние).

Эксплуатационные затраты (затраты на обслуживание и работу системы) включают:

1. Затраты на сетевое управление - расходы административного персонала на решение задач, ассоциируемых с управлением сетью и клиентами:
 - затраты на определение причины неисправности и решение проблемы (ремонт), после того как поступило сообщение о неисправности в сети;
 - регулярные затраты на измерение сетевого трафика и планирование его оптимизации;

- регулярные затраты на настройку производительности сетевых компонентов и межкомпонентных соединений;
 - временные затраты, связанные с добавлением, перемещением, удалением пользователей и изменением прав доступа к сети;
 - затраты на поддержку сетевых и клиентских операционных систем, включая установку, настройку и инсталляцию драйверов;
 - затраты на поддержание работоспособности сети и клиентов, наподобие диагностики, проверок и прочих задач, которые не попадают в категории, указанные выше;
 - затраты на поддержку пользователя, поддержки производителей, не попадающие в перечисленные выше категории;
2. Затраты на управление системой - расходы на управление приложениями, имуществом и миграциями:
 - затраты, связанные с исследованием и планированием проекта новых компьютерных систем, сетевых и коммуникационных компонент, затраты на выбор различных стратегий и конфигураций;
 - затраты, связанные с оценкой и покупкой новых компьютеров, сетевых компонент, коммуникационных устройств и программного обеспечения, определение поставщика, модели и получение финансов;
 - затраты, связанные с управлением, контролем за лицензиями, дистрибуцией и конфигурированием программного обеспечения по сети;
 - затраты, связанные со сбором информации, относящейся к имуществу, и включающие в себя инвентаризацию, контроль закупок и отслеживание конфигураций имущества;
 - затраты на управление программным обеспечением сети, включающее в себя контроль версий, доступа и запуска;
 - затраты, связанные с контролем за системой с целью обнаружения и предотвращения нарушений правил безопасности, вирусных атак и мероприятия по восстановлению после нарушений;
 - затраты, связанные с конфигурированием новых решений или перенастройкой существующих решений (решение включает в себя компоненты системы, топологию, местоположение, а также любые физические или логические замену и инсталляцию);
 - затраты, связанные с установкой дополнительного оборудования или модернизацией (за исключением программной модернизации)
 3. Затраты на управление устройствами хранения данных - расходы на задачи, связанные с управлением и контролем за данными и их хранением в сети:
 - затраты, связанные с организацией, оптимизацией и восстановлением файлов в сети;
 - затраты, связанные с контролем и проверкой оптимизации хранящихся данных;
 - затраты, связанные с обеспечением доступа к данным и устройствам хранения информации;

- затраты по конфигурированию, управлению, оптимизации и поддержке систем архивирования и резервного копирования;
- затраты на создание, испытание, управление и поддержку планов прогнозирования и восстановления неисправностей;
- затраты по управлению средствами хранения данных и репозиторием в реальном времени.

Отдельной и наиболее сложной проблемой является моделирование и расчет затрат на устранение последствий несанкционированного воздействия на ресурсы информационной системы. В научной литературе дискутируется вопрос относительно содержания терминов «несанкционированное воздействие», «несанкционированный доступ», инцидент, информационная агрессия, нападение, информационная акция и др. Рассмотрим основные из них [1,2,4].

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и(или) правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Информационная акция (ИА) – совокупность действий, приводящая к изменению информационного поля. Выделяют три типа информационных акций:

- ИА предпринятая на своем информационном поле с целью обеспечения эффективной информационной поддержки целевому режиму функционирования системы (внутренняя ИА, определяемая как прямое информационное управление);
- ИА предпринятая на общем информационном поле с целью воздействия на выбранный элемент (информационная атака);
- ИА предпринятая на общем информационном поле с целью обеспечения эффективной информационной поддержки целевому режиму функционирования системы (информационная защита).

Примерами ИА могут выступать:

- информирование – передача части информационной совокупности в пользование другой стороны;
- информационное давление – проведение информационных акций без санкций объекта воздействия;
- тиражирование информации – процесс распространения информационной совокупности;

- информационное нападение – информационная акция, предпринятая в общем информационном поле с целью противодействия;
- информационное обслуживание – проведение информационной акции с целью изменения информационной совокупности другой стороны;
- информационный прессинг – резкое увеличение интенсивности применения информационного воздействия;
- информационная агрессия – не объявленная информационная акция.

Считаем необходимым отметить, что приведенные определения требуют разработки соответствующей методики расчета затрат на устранение последствий информационного воздействия.

Общая стоимость устранения последствий может изменяться под влиянием различных объективных и субъективных факторов. Прежде всего, это относится к характеристике информационной системы (архитектура, состав вычислительной и коммуникационной техники, используемого программного обеспечения, особенности организации вычислительного процесса и др.), стадии зрелости организации, сопутствующие нежелательные последствия. В настоящее время СИБ сталкивается с реализацией атак на информационные системы. Можно рассматривать атаку как стохастический процесс планирования действий нападающей стороны, результаты которого в целом зависят от успешности предыдущих и ряда случайных факторов. Формально эти действия могут быть представлены как набор множества состояний информационной системы, множества действий нападающей стороны, функции переходов, начальное состояние информационной системы и множество конечных состояний.

Класс реализуемой атаки может быть представлен следующими наборами:

- атакующий объект (внешний и внутренний или инсайдер);
- атакуемый ресурс (по расположению – узловой или сетевой; по типу – пользовательский, системный, вычислительный и ресурсы СИБ);
- воздействие на ресурс (сбор информации, получение прав пользователя, получение прав администратора, нарушение целостности, нарушение работоспособности, нарушение доступности);
- характер атаки (распределенная, нераспределенная).

Обоснование расходов на информационную безопасность должно включать в себя следующие утверждения:

- расходы на безопасность являются составляющей стоимости ведения бизнеса;
- расходы на безопасность родственны расходам на страхование;
- безопасность – один из аспектов управления рисками;
- нежелание вкладывать денежные средства в безопасность означает нежелание следовать общим тенденциям развития информационных технологий.

4. Заключение

Приведенные показатели ни в коей мере не исчерпывают всего многообразия подходов к оценке инвестиционной привлекательности СИБ. Дальнейшее развитие теории и практики экономики СИБ может быть связано с разработкой методических положений по определению моделей нарушителя, идентификацией угроз безопасности, расчетом информационных рисков и формированием комплексной методики управления рисками. Необходимо также отдельное самостоятельное направление исследований для разработки адекватных экономико-математических моделей, описывающих взаимодействие компонент информационной системы при реализации разнообразных инцидентов.

Литература

1. Герасименко В.А. *Основы защиты информации в автоматизированных системах обработки данных*. – М., ВИНТИ, N 1080-В-91, 1991.
2. ГОСТ Р 50922-96. *Защита информации. Основные термины и определения*. –М., Госстандарт России, 1996.
3. *Анализ безопасности управления доступом и информационными потоками в компьютерных системах* –М., Радио и связь, 2006.
4. *Информационная безопасность систем организационного управления*. – М., Наука, 2006.
5. L.A.Gordon, M.P.Loeb. *The Economic of Information Security Investments*. ACM Transaction on Information and System Security, 5, No 4, November 2002.
6. Malicious Software (Malware): *A Security Threat in the Internet Economy*. Ministerial Background Report. DSTI/ICCP/REG (2007)5/Final.
7. Rachel Rue, Shari Lawrence Pfleeger and David Ortiz. *A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making*. 2007 Workshop on the Economics of Information Security.
8. Thomas. *Total Cost of Cyber (In)security – Integrating operational security metrics into business decision-making*. Mini-Meticon, February 5, 2007.
9. Yue Chen, Barry Boehm, Luke Sheppard. *Measuring Security Investment Benefit for Off the Shelf Software Systems- A Stakeholder Value Driven Approach*.

INVESTMENTS IN THE SYSTEM OF INFORMATION SECURITY

Summary

Material, characterizing practice of estimation of investment attractiveness of the system of informative security, presented in the article. Two going is considered of the estimation of investments - macro and micro. Composition of expenses of the system of informative security is resulted (operating and managements).