НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ "ЗАХИСТ ІНФОРМАЦІЇ" №2, 2002

УДК 681.3

Стишенко И.К., Богатырев А.И.

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности любого государства. Национальная безопасность государства существенным образом зависит от обеспечения информационной безопасности и эта зависимость будет возрастать.

Под информационной безопасностью государства понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении страны.

Интересы государства в информационной сфере заключаются в создании условий для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.

На основе национальных интересов в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов в информационной сфере:

- Первая составляющая национальных интересов включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- Вторая составляющая включает в себя информационное обеспечение государственной политики, связанное с доведением до общественности достоверной информации о государственной политике, ее официальной позиции по социально значимым событиям общественной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
- Третья составляющая включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- Четвертая составляющая включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность не сводится исключительно к защите информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита информации стоит по важности отнюдь не на первом месте.

Необходимость системы информационной безопасности.

Понятие "информация" сегодня употребляется весьма широко и разносторонне. Наверное, невозможно найти такую область деятельности человека, где бы оно не использовалось. Информационные потоки огромны, скорость их нарастает каждодневно, они буквально захлестывают людей. Объем научных знаний, не говоря о прочих, скорость которых несоизмеримо выше, по оценке специалистов удваивается, каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком теории и практики информации — информационным веком, что в свою очередь обуславливает переход человечества от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество, и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственной деятельности. Информация обладает качеством и количеством, имеет себестоимость и цену. Количество информации может определяется по разному. Это может быть количество машинописных листов, количество занимаемых на носителе или переданных по каналу связи байт, количество пикселей изображения и так далее. Себестоимость информации определяется количеством затраченной на ее производство энергии (умственных усилий), финансовых и материальных затрат на ее документирование, хранение, обеспечение сохранности, обработку и передачу по каналам связи. Цена информации, как и остальных товаров, складывается из себестоимости и величины прибыли от ее реализации. Реализация информации с извлечением прибыли может происходить в результате следующих действий:

- продажа информации;
- материализация произведенной или приобрéтенной (купленной) информации в продукте или технологии;
- использование информации в процессе принятия решения.

Из этого следует, что информация обладает свойствами товара, и, следовательно, как и любой товар она может участвовать в товарообороте и являться объектом права, иметь производителя, собственника, владельца и потребителя. С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект. С точки зрения обладателя — сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту ценной информации.

Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами. Особое место отводится информационным ресурсам в условиях рыночной экономики. В конкурентной борьбе широко распространены разнообразные действия, направленные на получение конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. На сегодняшний день примерно 47% охраняемых сведений добывается в результате промышленного шпионажа. А в 60% случаев утери лишь 20% имеющейся коммерческой информации приводила к банкротству фирм. Вывод напрашивается сам. Защите информации от неправомерного овладения ею, необходимо отводить весьма значительное место. И здесь не обойтись разовыми мерами, будь то эпизодические мероприятия, частичное использование средств защиты или привлечение некоторых специалистов по защите информации. Необходим четко продуманный, качественно спланированный и профессионально проводимый комплекс мер по защите информации. Необходима грамотно и профессионально отлаженная система информационной защиты. И чем раньше это будет воспринято предпринимателем, бизнесменом, руководителем фирмы, тем дешевле ему обойдется создание системы информационной безопасности. С развитием рыночных отношений и перехода от индустриального общества к информационному, цены на услуги по качественной защите информации несоизмеримо возрастут. Ибо основным правилом XXI века будет правило: кто владеет информацией, тот владеет миром.

Информация с точки зрения информационной безопасности обладает следующими категориями:

- конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена;
- целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
- аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией автора сообщения
- апеллируемость – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается "откреститься" от своих слов, подписанных им однажды.

В отношении информационных систем применяются другие категории:

- надежность – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;
- точность – гарантия точного и полного выполнения всех команд;
- контроль доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются;
- контролируемость – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса;

- контроль идентификации – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает;
- устойчивость к умышленным сбоям – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Виды угроз информационной безопасности

- По своей общей направленности угрозы информационной безопасности подразделяются на следующие виды:
- *угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности (ограничение свободы слова и доступа граждан к информации, разрушение системы ценностей, духовного здоровья личности, общества);*
- *угрозы информационному обеспечению государственной политики (ограничение возможностей органов государственной власти принимать адекватные решения, манипулирование общественным мнением со стороны финансово-политических кругов);*
- *угрозы развитию индустрии информации, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов (искажение информационных ресурсов, низкий уровень интегрированности государства в мировое информационное пространство);*
- *угрозы безопасности информационных и телекоммуникационных средств и систем (нарушение штатного режима функционирования или разрушения критически важных информационных сетей и систем управления, несанкционированная утечка информации с ограниченным доступом).*
- *Основными угрозами безопасности информационных и телекоммуникационных средств и систем могут являться:*
- *противоправные сбор и использование информации;*
- *нарушения технологии обработки информации;*
- *внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; разработка и распространение программ, нарушающих нормальное функционирование информационных и телекоммуникационных систем, в том числе систем защиты информации;*
- *уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;*
- *воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;*
- *компрометация ключей и средств криптографической защиты информации;*
- *утечка информации по техническим каналам;*
- *внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;*
- *уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;*

- *перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;*
- *использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии информационной инфраструктуры;*
- *несанкционированный доступ к информации, находящейся в банках и базах данных;*

нарушение законных ограничений на распространение информации.

Общие методы обеспечения информационной безопасности

Общие методы обеспечения информационной безопасности разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности являются:

- создание и совершенствование системы обеспечения информационной безопасности;
- усиление правоприменительной деятельности органов исполнительной власти, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационных и телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности;

Для аналізу цього питання багатокритеріальність оцінки мережі зручно кваліфікувати як невизначеність цілей і підходити до нього з єдиних позицій аналізу і класифікації невизначеностей. Почнемо з аналізу невизначеності цілей внаслідок багатокритеріальності.

1. Невизначеність цілей

При дослідженні багатокритеріальних задач необхідно визначити спосіб завдання та обліку визначальних елементів принципу вибору. До визначальних елементів принципу вибору відносяться поняття нормалізації, згортки, пріоритету. Для більш глибокого вивчення цього питання необхідно сформулювати систему аксіом і властивостей, яким повинні відповідати принципи вибору. Ми розглянемо конкретні принципи вибору, а також торкнемося проблеми формування системи аксіом.

Приведемо визначення зазначених понять.

Нормалізація .

Нехай F – простір цільових функціоналів f_i. Під способом нормалізації розуміється однозначне відображення $f_i \rightarrow F$, що перетворить цільовий функціонал f_i в інший елемент простору F.

У таблиці 1 приведені основні способи нормалізації.

Таблиця 1

Нормалізація	Математичний вираз
Зведення до безрозмірних величин	$f_i(\cdot)/\rho[f_i(\cdot)]$
Зміна інгредієнта	$- f_i(\cdot),\ 1/ f_i(\cdot)$
Природна нормалізація	$\lambda_f = [f_i(x) - \min_x f_i(x)] / [\max_x f_i(x) - \min_x f_i(x)]$
Нормалізація порівняння	$f_i(x) / \max_x f_i(x)$
Нормалізація Савиджа	$\max_x f_i(x) - f_i(x)$
Нормалізація усередненням	$f_i(\cdot) / \sum_i fi(\cdot)$

Згортка.

Згорткою компоненту багатоцільового показника $f_i \in F$ називається відображення $g \in \{F \in R^1\}$, що перетворює сукупність компонентів f_i у скалярний цільовий показник $g(f_i(x))$.

Основні види згорток:

1. Підсумовування критеріїв f_i з ваговими коефіцієнтами α_I чи «економічний» спосіб.

$$g(f_i(x)) = \sum_i \alpha_i f_i(x)$$

2. Мінімізаційні.

$$g(f_i(x)) = \min_i (\alpha_i f_i(x) + \beta_i)$$

3. Функції Кобба – Дугласа.

$$g(f_i(x)) = \prod_i (\alpha_i f_i(x))^{\beta_i}$$

4. Спосіб переходу до якісних показників шляхом розбивки векторів $\{f_i\}$ на задовільні і незадовільні.

Задовільними вважаються вектори $\{f_i\}$, для яких

$$f_i \geq f_i^0 \tag{1}$$

Згортка має вид

$$\left.\begin{array}{l} g(f_i(x)) = 1, \text{ якщо має зміст (1)} \\ g(f_i(x)) = 0, \text{ якщо не виконується (1)} \end{array}\right\} \tag{2}$$

Звичайно, дуже не просто вибрати вектори f_i^0, тому в цьому випадку підкреслюється свобода вибору f_i^0 особою, що приймає рішення **(ОПР)**.

Згортка (2) може бути розширена для більш точного опису якісних процесів. Для цього замість двох значень згортки 0,1 введемо базову шкалу значень на сегменті $A \in [0,1]$ і функцію приналежності розмитої множини

$$M_A(f_i^0) : \{f_i^0\} \to A$$

Тоді умови (1) запишуться у вигляді

$$f_i \geq f_i^0 M_A(f_i^0)$$

і відповідно згортка

$$g(f_i(x)) = \min_i M_A(f_i^0)$$

Базова шкала показує оцінки процесу ОПР і є відображенням простору критеріїв на сегмент А. Відзначимо, що масштаб шкали може бути будь-який, і у тому числі охоплювати і негативні значення.

5.Спосіб послідовного досягнення частинних цілей

Облік виконання наступної операції починається тільки тоді, коли досягнуті вже абсолютні максимуми критеріїв ефективності операцій

$$g(f_i(x)) = f_i(x) + \sum_i f_i(x)$$

Практична реалізація цього критерію проводиться, якщо є впевненість у досягненні верхньої межі критерію кожної попередньої операції. Наприклад, послідовне нарощення мережі без зміни топологічної структури за критерієм максимізації пропускної спроможності, а також оцінка воєнних дій по заняттю опорних пунктів вдало описуються цим критерієм.

6.Логічне об'єднання критеріїв.

Це згортання використовується для критеріїв якісного типу, що приймають значення 0,1. Звичайно розглядаються два випадки:

сумарна ціль полягає у виконанні всіх часткових критеріїв (кон'юнкція):

$$g(f_i(x)) = \prod_i f_i(x)$$

сумарна ціль полягає у виконанні хоча б однієї з часткових цілей (диз'юнкція):

$$g(f_i(x)) = 1 - \prod_i (1 - f_i(x)).$$

Аналогічно пункту 4 замість двох значень 0,1 можна розглядати розмиту логіку з функціями приналежності $M_A(f_i(x))$ і відповідною базовою шкалою. Тоді згортки запишуться у вигляді:

$$g(f_i(x)) = \prod_i f_i(x) M_A(f_i)$$

$$g(f_i(x)) = 1 - \prod_i (1 - f_i(x)) M_A(f_i)$$

Введені дії з критеріями утворюють повний простір, тобто зможуть відбити всю широту залежностей при формуванні цільової згортки [5].

Пріоритет. Поняття пріоритету основується на порівнянні цільових критеріїв. На жаль, до цього часу відсутні точні означення пріоритету, відповідні усвідомленню сутності багатоцільового підходу в теорії оптимізації, основані на чіткому розрізненні зрівняємості по важливості, перевазі та ефективності цільових критеріїв. Звичайно, при розгляді пріоритету, із-за відсутності точного розрізнення важливості, значимості та ефективності при заданні багатоцільових структур, можливо використовувати лише одну з можливих варіацій відношення пріоритету. Один з підходів заключається у тому, що відношення пріоритету може бути визначено як бінарне відношення порядку R зрівняння елементів простору F в тому розумінні, що має місце одна з умов:

1. f_i краще f_k за R; (f_i R f_k).
2. f_k краще f_i за R; (f_k R f_i).
3. f_i еквівалентно f_k за R; (f_i R f_k Λ f_k R f_i).
4. f_i не краще f_k за R; (f_i $\overline{R}$ f_k).
5. f_k не краще f_i за R; (f_k $\overline{R}$ f_i).
6. f_i не гірше f_k за R; (f_i Rf_i V (f_i R$f_к$ Λ $f_к$ Rf_i)).
7. f_k не гірше f_i за R; ($f_к$ Rf_i V ($f_к$ Rf_i Λ f_i R$f_к$)).
8. f_i та f_k незрівненні за $R(\overline{f_i R f_k}) \Lambda R(\overline{f_k R f_i}) \Lambda (\overline{f_i R f_k \Lambda f_k R f_i})$

Відношення пріоритету може бути також визначено у формі більш складних відношень порядку, які народжуються початковими бінарними порядками. При їх заданні слід діяти з особливою обережністю, тому що необхідно враховувати узгоджене завдання пріоритету.

Принцип вибору. Принципом вибору є таке формування відношення порядку, при якому проведений вибір нормалізації, згортки та пріоритету. Задання принципу вибору дає можливість визначити, як розуміється рішення задачі багатоцільової оптимізації та визначити множину оптимальних елементів. Основні принципи вибору зведені у таблиці 2 [6]. Приведені принципи вибору не розглядають проблему задання та обліку пріоритету. Повне рішення задачі можливе тільки при умові побудови чіткої, непротирічної системи аксіом принципів вибору. Основні системи аксіом сформульовані Ерроу [7], Сєном [8], Нешем [9], Мілнором [10], Ерроу-Гурвіцем [11].

Таблиця 2.

Принцип вибору	Умова оптимальності
Домінантності R^{dom}	$Fi(x_0) \geq fi(x), \forall^x \in x, \forall^i \in [1, n]$
Часткової домінантності	$\exists k_1,\ldots,k_8 \in [1,n] : fk_i(x_0) \geq fk_i(x), \forall^x \in x, \forall k^i, 1<n$
Парето $\hat{R}^{dom}$	$\bar{\exists} x \in X : \{f_i(x) \geq f_i(x_0), \forall^i\} \cap \{\exists j : fj(x) > fj(x0)\}$
Слейтера	$\bar{\exists} x \in X : f_i(x) > f_i(x_0), \forall^i \in [1, n]$
Власно ефективності Джеффрі	$\bar{\exists} x : f_i(x) > f_i(x_0), \forall i$ $\exists \mu>0 : \frac{f_i(x) - f_i x_0}{f_j(x_0) - f_j x} \leq \mu$ $\forall i, \forall x \in \{x : f_i(x)>f_i(x_0)\} \exists j \in \{fj(x) < fj(x_0)\}$
Невласно ефективності Джеффрі	$\bar{\exists} x : f_i(x) > f_i(x_0), \forall i, \forall \mu>0, \exists k,$ $\exists x \in \{x : f_i(x) > f_i(x_0)\}$ $\frac{f_k(x) - f_k(x_0)}{f_j(x_0) - f_j(x)} < \mu, \forall j : \{f_j(x) < f_j(x_0)\}$
Рівності	$fi(x_0) = fk(x_0), \forall_{i,k}$
Суммарної ефективності	$\sum_i f_i(x_0) \geq \sum_i f(x), \forall x$
Неша	$\prod_i f_s(x_0) \geq \prod_i f_i(x), \forall x$
Компромісна	$\exists \alpha i : \sum_i \alpha_i f_i(x_0) = \max_x \sum_i \alpha_i f_i(x)$
Домінуючого результату	$\max_i f_i(x_0) \geq \max_i f_i(x), \forall x$
Гарантованого результату	$\min_i f_i(x_0) \geq \min_i f_i(x), \forall x$
Найменшого відхілу	$\|f(x_0) - f^*\| \leq \|f(x) - f^*\|, \forall x, f^*=\{f_i^*\}, f_i^* = \max_x f_i(x), \forall i$
λ- критерія	$X_0 \in x\lambda_0 : \lambda_0 = \max_{0\leq\lambda\leq1} (\lambda : x_\lambda \neq \varnothing), x_\lambda = \{x: \lambda_f(x, \lambda) \geq \lambda, \forall i\}$
α-критерія Гурвіца	$x_0 : (\alpha \min_i \lambda_f(x_0, i) + (1 - \alpha) \max_i \lambda_f(x_0, i)) \geq (\alpha \min_i \lambda_f(x, i) + (1 - \alpha) \max_i \lambda_f(x, i)), \forall x$
Максимум функції невизначеності	$x_0 : H(f(x_0)) \geq H(f(x))$

Система аксіом Ерроу містить п'ять природних аксіом, які містять у собі так званий парадокс Ерроу, зміст якого в тому, що не існує порядка R, який задовільняє цим п'яти аксіомам.

Досить зрозумілим є бажання змінити формулювання цих аксіом таким чином щоб існувало відношення порядку R, яке задовільняє ці умови. Запропонована Сеном зміна аксіом призвела до того, що вона виконується для принципу вибору тоді і тільки тоді, коли він тривіальний, тобто коли він є принципом домінування. Таким чином оскільки була отримана негативна відповідь на рахунок існування в классі відносин порядку принципу вибору (відмінного від домінування), задовільняючого сформульованій Сеном системі аксіом, були прийняті спроби по розробці нових систем аксіом та обгрунтування для них існування принципів вибору.

Аксіоматика Неша містить чотири аксіоми та задовільняє принципу вибору Неша

Аксіоматика Мілнора складається з трьох аксіом. Цій системі аксіом задовільня принцип вибору

$$R(f) = \min_i f_i(x)$$

При цьому одна з аксіом, по суті, є умовою, що елементи домінують, і н належать множині оптимальних по принципу вибору R(f) елементів.

Система аксіом Ерроу-Гурвіца містить чотири аксіоми. Цій системі задовільня принцип гарантованого результату.

Системи аксіом Сена, Неша, Мілнора, Ерроу-Гурвіца спрямовані на рішенн парадоксу Ерроу. Це вдається зробити ціною значного віддалення від початковс аксіоматики Ерроу.

*Як же можна здійснити вибір "найкращим" чином? Один з підходів заключаєтьс*я в зрівнянні порядків для принципів вибору.

Визначення 1. Будемо вважати, що відношення порядку R_1, для нечітко множини $F(\mu)$ з функцією приналежності $\mu \in [0, 1]$ сильніше за відношення порядку R2 $(R1 \triangleright R2)$, якщо не пустий перетин множин

$$F_1(\mu) = \{f_0 \in F(\mu) : f_0 R_1 f, \forall f \in F(\mu), \forall \mu \in [0, 1]\},$$
$$F_2(\mu) = \{f_0 \in F(\mu) : f_0 R_2 f, \forall f \in F(\mu), \forall \mu \in [0, 1]\},$$

і якщо

$$F_1(\mu) \le F_2(\mu), \forall \mu \in [0,1]$$

$$R_1 \triangleright R_2 \rightarrow \{ (F_1(\mu) \cap F_2(\mu) \neq \varnothing, \ \forall \mu \in [0,1]) \cap (F_1(\mu) \le F_2(\mu), \forall \mu \in [0,1])\}.$$

Визначення 2. Відношення порядку R сильніше за кожного R_k (k=1, …, n) дл непарної множини, якщо

$$\{ R_1 \triangleright R_k\} \Lambda \{ F_0(\mu) \cap F_k(\mu)\} \neq \varnothing$$

тобто

$$F_0(\mu) \le F_k(\mu), \forall \mu \in [0,1],$$

де

$$F_0(\mu) = \{f_0 \in F(\mu): f_0 R f, \ \forall f \in F(\mu), \forall \mu \in [0,1]\},$$
$$Fk(\mu) = \{f_0 \in F(\mu): f_0 R_k f, \ \forall f \in F(\mu), \forall \mu \in [0,1]\}.$$

Визначення 3. Відношення порядку R сильніше сукупності $\{R_k\}$, k=1, …, n дл нечіткої множини $F(\mu)$, якщо

$$\{R \triangleright R_k\} \Lambda F_0(\mu) \cap \{\bigcap_k F_k(\mu)\} \neq \varnothing,$$

$$F^0(\mu) \le \bigcap_k F_k(\mu), \forall^k, \ \forall \mu [0,1].$$

Проблема вибору по багатоцільовому критерію виникає тому, що, як правило, пуста множина

$$F_0(\mu) = \{f^0 \in F(\mu) : f^0 \, R^{dom} \, f, \forall f \in F(\mu), \forall \mu \in [0,1]\}$$

найкращих по R^{dom} елементів.

Однак близьке до R^{dom} відношення порядку R^{dom} / $\hat{R}^{dom}$ являється звичайним, оскільки передбачається, що задача багатоцільової оптимизації невироджена, тобто множина оптимальних по Парето елементів f^0 не пуста, а оптимальні по Парето елементи $f_0 \in F(\mu)$ являються найкращими по R^{dom} / $\hat{R}^{dom}$, проблема вибора оптимального по багатоцільовому показнику елемента і виникає в силу того, що множина достатньо представлена .

Введення поняття $\triangleright$ на відношеннях порядка R дозволяє проводити порівняння принципів вибору R(f, μ) тобто визначити, чи існують для заданого принципу вибору R(f, μ) інші принципи вибору, в яких відношення порядку, які їм відповідають, сильніше R(f, μ). Крім того, для конкретно заданих пар принципу вибору можливо встановлювати, який з них сильніший.

2. Природна невизначеність

При наявності природної невизначеності задані параметри процесу x(t) та цільова функція f, але задані неточно - вони містять невизначений параметр ά

$$x \rightarrow x(t, \acute{\alpha})$$
$$f \rightarrow f(x, t, \acute{\alpha})$$

Якщо ніякої інформації про ά ми не маємо, то результат оптимізації вільний. Виникають природні невизначеності в наслідок таких факторів:

Невизначеність, пов'язана з незнанням конкретних значень випадкових величин або функцій, для яких відомі статистичні та вірогідні властивості з тим чи іншем ступенем деталізації (закони розподілу, кореляційні функції і. т. д.), або задана область зміни ά ∈ A.

Невизначеність, пов'язана з незнанням виду деяких детермінованих функцій, які описують процеси. Приводить до необхідності апроксимацій.

Невизначеність, пов'язана з незнанням деяких факторів процесу. Призводить до неповних моделей.

Невизначеність, пов'язана з технічною неможливістю точно врахувати всі фактори, які впливають на процес, однак ці фактори достовірно відомі.

Невизначеність, пов'язана з нестійкістю та з біфуркаціями систем.

Невизначеність, пов'язана з новими явищами.

Невизначеність, пов'язана з невідомими діями іншої сторони. Призводить до конфліктів. Приведений перелік можна розвивати і уточнювати.

Одним з основних принципів при вивченні природних невизначеностей є принцип гарантованого результату. Він заключається в наступному.

Так як для любого x

$$\min_{\alpha} f(x, \acute{\alpha}) \le f(x, \acute{\alpha})$$

то і для любого ά

$$f^0 = \max_{x} \min_{\alpha} f(x,\alpha) \le \max_{x} f(x,\alpha)$$

Число f^0 має назву гарантованої оцінки, а відповідне рішення x_0 – гарантуючою стратегією, у тому значенні, що яким би не було значення параметру невиявності ά, вибір x_0 гарантує, що при любому ά значення цільової функції буде не менше, чим f^0.

Гарантовану оцінку можливо поліпшити, якщо прийняти рішення, пов'язані з визначеним ризиком. Тут виникають дві ситуації: вибір проводиться багаторазово і вибір являється однократною операцією. В першому випадку ми задаємося деяким імовірнісним розподіленням випадкової величини ά, в другому - використовуємо формалізм розмитих множин.

Задача прийняття рішень в умовах природної невизначеності може бути зведена до задачі прийняття рішень в умовах невизначеності цілей. Насправді цільова умова

$$f(x, \acute{\alpha}) \rightarrow \max , \acute{\alpha} \in A$$

еквівалентна нескінченому числу критеріїв

$$\begin{aligned} &f(x, \acute{\alpha}_1) \rightarrow \max , && \acute{\alpha}_1 \in A \\ &f(x, \acute{\alpha}_2) \rightarrow \max , && \acute{\alpha}_2 \in A \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &f(x, \acute{\alpha}_n) \rightarrow \max , && \acute{\alpha}_n \in A \end{aligned}$$

З деякою достовірністю можна обмежитись n критеріями і вирішувати задачу оптимізації для конкретних значень $\acute{\alpha}_i$, вибравши нормалізацію, згортку, пріоритет, або побудувавши Парето – оптимальну область.

В цій класифікації особливе місце займає конфлікт. При функіонуванні комп'ютерних мереж, при наявності верогідносного характеру інформаційних потоків, конфлікти у вузлах неминучі і від того, наскільки вдало цей конфлікт може бути рзв'язано, наскільки вдало може бути побудована маршрутизація інформаційних потоків залежить якість функціонування мережі. Тому зупинимося на класифікації конфліктів більш детально.

Введемо поняття інтенсивності взаємодії інформаційних потоків x. Цільовий критерій першої сторони, яка керує інформаційним потоком U_1 означимо $f_1(x_1, f_2)$, цільовий кретерій другої сторони з потоком U_2 - $f_2(x_2, f_1)$.

Тоді $$x_1=\delta f_1(x_1 f_2)/ \delta f_2, \quad x_2=\delta f_2(x_2 f_1)/ \delta f_1$$

Таким чином, для x_1 ефективність f_1 є функціонал від функції $f_2(x_2)$, а для x_2 - функціонал від $f_1(x_1)$.

Під впливом взаємодії ефективності сторін змінюються, це і є основою класифікації конфлікту [12]

1.При $x_1=0$, $x_2=0$ системи нейтральні, взаємодії нема, цілі сумісні та незалежні.

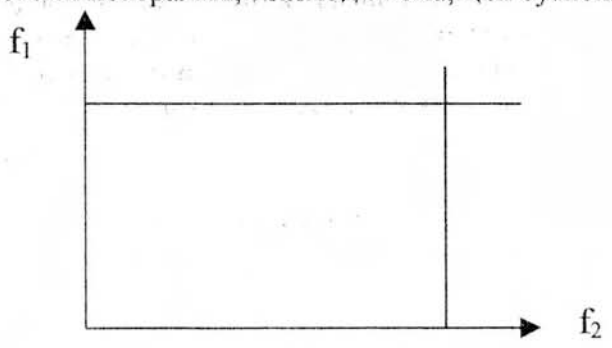


Рис. 1. Нейтралітет

2. При $x_1>0$, $x_2>0$ на всій осі

$$\max f_1 \Leftrightarrow \max f_2$$

системи складають єдність

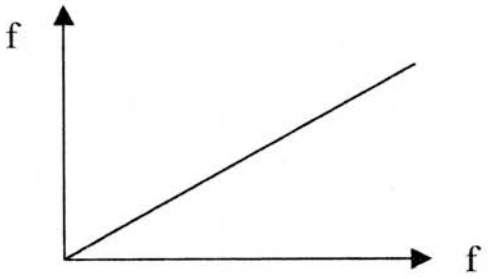


Рис. 2. Єдність

3. При $x_1>0$, $x_2>0$ на деякому сегменті $f_1 \neq 0$, $f_2 \neq 0$

$$\max f_1 \Leftrightarrow \max f_2$$

досягається симбіоз

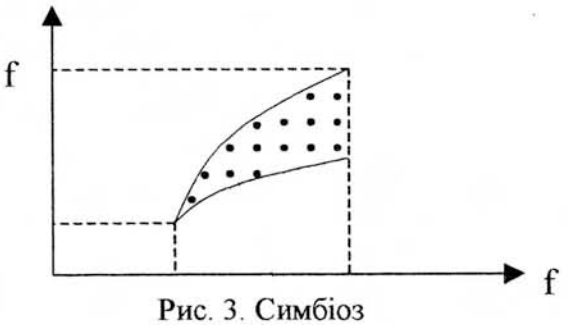


Рис. 3. Симбіоз

4. При $x_1>0$, $x_2>0$ на всій осі

$$\max f_1 \neq \max f_2$$

буде співдружність

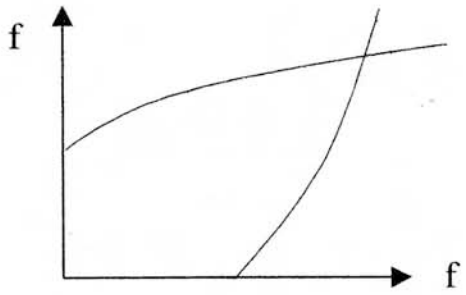


Рис. 4. Співдружність

5. При $x_1>0$, $x_2>0$ на деякому сегменті $x_1 \leq 0$, $x_2 \leq 0$ – за межами цього сегменту та $\max f_1 \neq \max f_2$

відбувається коаліція

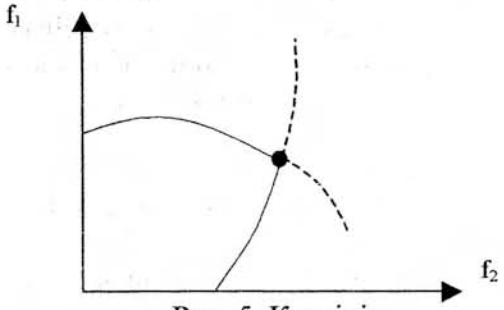


Рис. 5. Коаліція

При $x_1<0$, $x_2<0$ за межами сегмента системи супротиводіючі.

6. При $x_1<0$, $x_2<0$ на всій осі

$$\max f_1 \Leftrightarrow \min f_2$$

системи антигоністичні

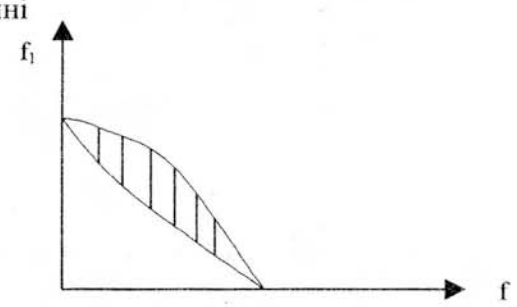


Рис. 6. Антагонізм

7. Коли X1 < 0, X2 < 0 на всій осі

$$\max f1 \Leftrightarrow \min f2$$
$$\max f2 \Leftrightarrow \min f1$$

буде сувора суперечність

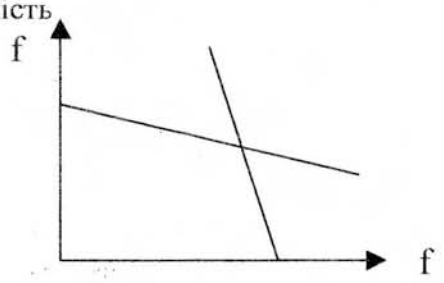


Рис. 7. Сувора суперечність

8. Коли X1 < 0, X2 < 0 на сегменті, X1 > 0, X2 > 0 поза ним та

$$\max f1 \Leftrightarrow \min f2$$
$$\max f2 \Leftrightarrow \min f1$$

є несувора суперечність

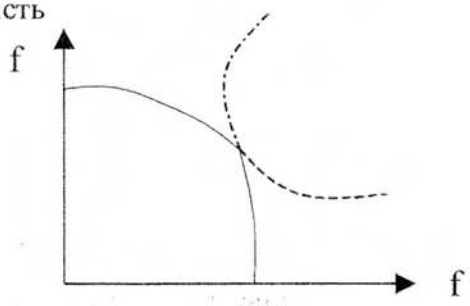


Рис. 8. - Несувора суперечність

Для богатоцільових систем критеріальна класифікація ускладнюється, тому що по деяким цілям системи можуть бути спільно діючими, по іншим - протидіючими.

Повне дослідження конфлікту передбачає дослідження наступних питань.

1. Як відбувався б конфлікт при повній освідомленості сторін?

2. Як реально, тобто з урахуванням обмежень за технічним, часовим, та пріоритетним ресурсами може діяти f12?

3. Як реально може діяти f22 ?

4. Як відбувався б конфлікт, якби f1 володіла повною інформацією про ситуацію, а f2 - неповною?

5. Як розвивався б конфлікт, якби f2 володіла повною інформацією про ситуацію, а f1 - неповною?

На основі різультатів такого дослідження визначається цінність (актуальність) інформації і необхідність такого перерозподілу сторонами своїх ресурсів, під час якого частина з них витрачається на отримання додаткової інформації про ситуацію, що веде до знешкодженню конфлікта.

Повернемось тепер до розгляду комп'ютерної мережі.

Нехай задана топологія мережі, яка описується графом **G**.

Нехай задана матриця інформаційних потоків між кожною парою вузлів

$$\Lambda = \left\| \Lambda_{ij} \right\|,$$

матриця вартостей оренди каналів

$$C = \left\| C_{ij} \right\|.$$

Необхідно визначити кількість і тип каналів зв'язку n_{rh} в кожному з'єднанні (r,h) зі швидкістю передачі V_{rh}

$$N = \left\| n_{rh} \right\|$$

і величини потоків у кожному з'єднанні (r,h)

$$F = \left\| f_{rh} \right\|$$

Так, щоб

$$f_1(n_{rh}) = \sum_2 \sum_h C_{rh} n_{rh} \to \min \tag{3}$$

$$f_1(n_{rh}) = \sum_2 \sum_h V_{rh} n_{rh} \to \max \tag{4}$$

При наступних обмеженнях

$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij} \tag{5}$$

$$T_{ij} \le \tau_{кр} \tag{6}$$

$$f_{rh} \le V_{rh} n_{rh} \tag{7}$$

В такій постановці задача є багатокритеріальною і для того щоб було ясно в якому змісті розуміється рішення задачі необхідно сформулювати цільову структуру, а саме вирішити проблему принципу вибору для критеріїв (3), (4). Відзначимо, що критерії конфліктуючі, з однаковим пріоритетом. У зв'язку з тим що критерії паритетні, то не підходять принципи вибору які основані на домінантності. Для нашого випадку конфліктуючих критеріїв підходять принципи вибору Парето, Неша, гарантованого результату, компромісу. Конфлікт, який має місце в нашій задачі не є антагоністичним. Його може бути кваліфіковано як нестроге супротивництво. Тому принцип вибору Неша, який визначає рівновагому ситуацію для антагоністичних критеріїв, та принцип гарантованого результату, який також використовується в умовах антагонізму і дає оцінку знизу можливих оптимальних рішень також нам не підходить. Залишається принцип вибору Парето та принцип компромісу. Відповідно до визначень 1- 3 принцип вибору Парето для нашої задачі генерує більш сильне відношення порядку на множині всіх можливих з'єднань (r,h) , ніж принцип компромісу. Його ми і визначимо в якості принципу вибору.

Для побудови Парето-оптимального рішення розглянемо критеріальний простір E^2_{fo} В цьому просторі необхідно побудувати множину досягаємості G_f., яка є образом множини можливих з'єднань n_{rh}. Іншими словами кожній точці n_{rh} в просторі з'єднань співвідношення

$$f_1 = f_1(n_{rh}), \quad f_2 = f_2(n_{rh})$$

ставлять у відповідність деяку точку критеріального простору

$$f \in G_f .$$

Множина G_f називається множиною досягаємості. Для нашої задачі G_f обмежено так як значення C_{rh} та V_{rh} обмежені, а змінні n_{rh} можуть змінюватися на кінцевих

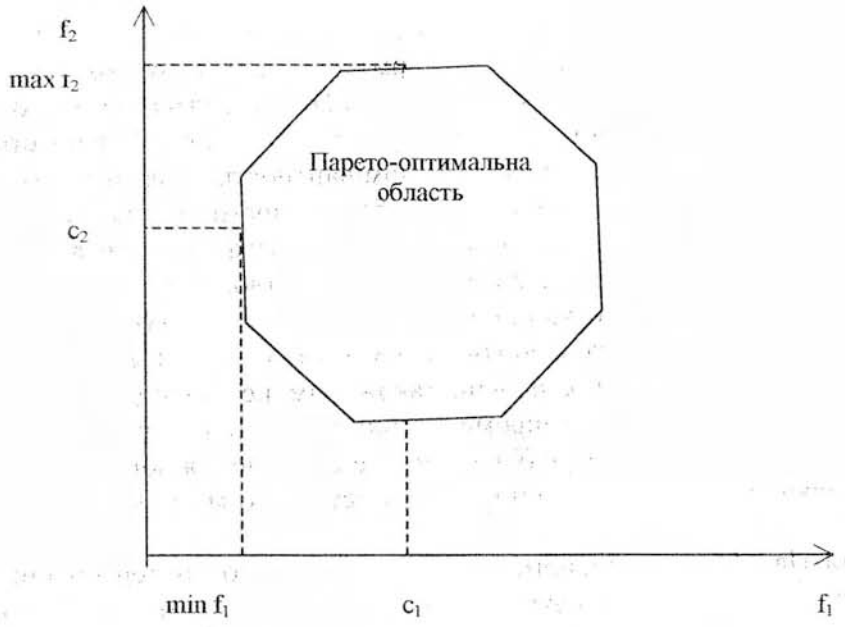
інтервалах $[a_{rh}, b_{rh}]$. В залежності від лінійності умов (3) – (5), (7) множина G_f поліедральна [13] та, відповідно випукла і замкнута. Вершинами багатокутника G_f можуть бути тільки ті точки критеріального простору координати яких відповідають значенням $n_{rh}=a_{rh}$, $n_{rh}=b_{rh}$. Позначимо через P_f множину точок, які оптимальні по Парето. Вона складається із підмножини граничних точок множини G_f і є реберно звязаною. Для побудови множини Парето поступимо наступним чином. Зафіксуємо деякі допустимі значення критеріїв f_1 і $f_2 \in G_f$.

$$f_1 = c_1, f_2 = c_2$$

Вирішимо дві оптимізаційні задачі

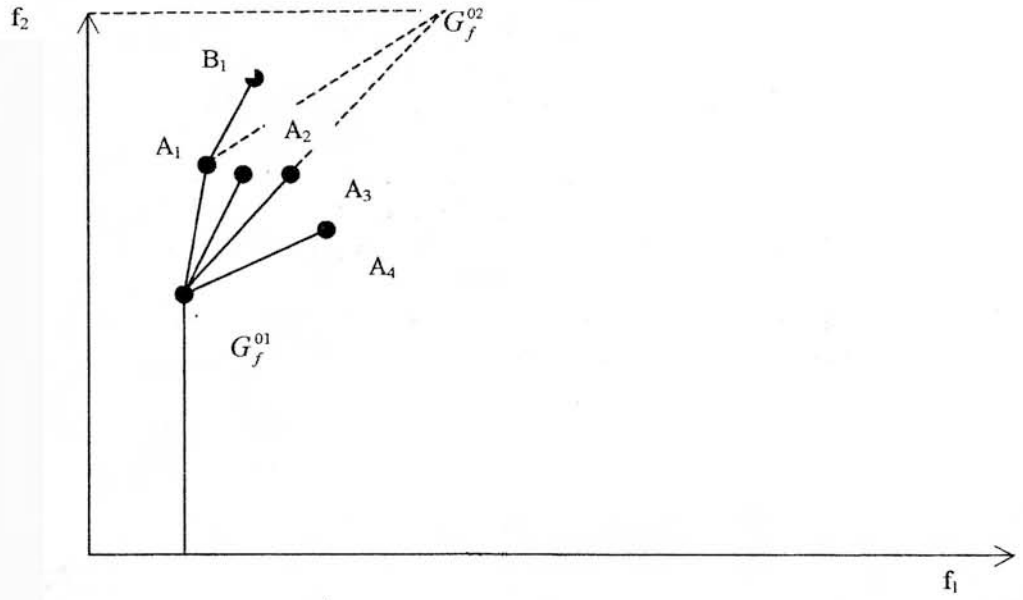
$$1.\ f_1(n_{rh}) \to \min$$
$$f_2(n_{rh}) = c_2$$
$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij}$$
$$f_{rh} \le V_{rh} n_{rh}$$
$$2.\ f_1(n_{rh}) = c_1$$
$$f_2(n_{rh}) \to \max$$
$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij}$$
$$f_{rh} \le V_{rh} n_{rh}$$

Вирішивши ці задачі, визначимо точки G_f^{01} та G_f^{02}. За опорні точки $F_1=\{\min f_1\ c_2\}$ та $F_2=\{c_1, \max f_2\}$ необхідно прийняти саму ліву точку багатокутника G_f та саму верхню його точку. Якщо точки G_f^{01} та G_f^{02} задовільняють цим вимогам приймаємо їх за опорні.



З'єднавши точки G_f^{01}, G_f^{02} прямою одержимо перше приближення множини Парето. Істиною множиною Парето є ломана лінія, яка з'єднує точки G_f^{01} G_f^{02} та, яка є границею області G_f і лежить вище та лівіше прямої G_f^{01} та G_f^{02}. Складові ломаної будемо будувати відправляючись від точки G_f, послідовно міняючи та фіксуючи значення констант C_1, C_2. Перша складова шукаємої ломаної вибирається з відрізків, які

виходять із точки G_f^{01}. Всі ці відрізки належать області G_f та характеризуються зміною значення якої-небудь одної змінної. Серед відрізків, які виходять із точки G_f^{01} вибирається той, який з прямою G_f^{01} G_f^{02} складає найбільший кут.



Таким чином, для знаходження точки G_f^{02} необхідно вирішити задачі 3, 4, які аналогічні задачам 1,2.

3. $f_1(n_{rh}) \to \min$

$$f_2(n_{rh}) = c_3$$

$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij}$$

$$f_{rh} \le V_{rh} n_{rh}$$

4. $f_1(n_{rh}) = c_4$

$$f_2(n_{rh}) \to \max$$

$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij}$$

$$f_{rh} \le V_{rh} n_{rh}$$

Ломану $G_f^{01} A_1 G_f^{02}$ можна вважати другим приближенням множини Парето, відрізок $G_f^{01} A_1$ є частиною множини Парето, а відрізок $A_1 G_f^{02}$ потребує подальшого уточнення за тим же алгоритмом.

Множина ефективних варіантів визначається вершинами багатокутника, які належать множині Парето.

Такий підхід не виділяє єдиного рішення, але він дозволяє відкидати неефективні варіанти та значно звужувати множину можливих альтернатив , залишаючи остаточний вибір варіанту за особою, яка приймає рішення.

Список літератури:

1. Tanenbaum A.S. Computer Networks. 1981
2. Stallings W. Data Computer Communications, N-Y, 1985.
3. Клейнрок Л. Вычислительные системы с очередями. М., Мир, 1979.

4. Hayes I.F. Modeling and Analysis of Computer Cammunications Networks, N-Y, 1984.

5. Гермейер Ю.Б. Введение в теорию исследования операций. М. "Наука", 1971.

6. Хоменюк В.Б. Элементы теории многоцелевой оптимизации. М. "Наука", 1983.

7. Arrow K.J. Rational choice functions and orderings. Econometrica. 1959, vol.26, p.121-127.

8. Sen A.K. Choice functions and revealed preference. Rev. Econ. Stud. , 1971, vol. 38, p. 307-317.

9. Нэш Д. Бескаалиционные игры. В кн.: Матричные игры. М., Физматиз, 1961.

10. Milnor J. Games against nature. In: Decision processes., 1954.

11. Arrow K.J. Hurwicz Y. An optimality criterion for decisionmaking under ignorance. In: Uncertainty and expectation in economics. Oxford, 1977

12. Дружинин В.В. , Конторов Д.С. , Конторов М.Д. Введение в теорию конфликта., М. "Радио и связь", 1989.

13. Подиновский В.Б., Нагин В.Д. Парето-оптимальные решения многокритериальных задач М. "Наука", 1982

Надійшла 14.01.2002
Після доработки 27.02.2002

УДК 681.3

Анкудович Г.Г., Катерноза К.А.

АНАЛИТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ СИГНАЛОВ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВОДОК ЭЛЕМЕНТОВ ЛВС АИС ГНС УКРАИНЫ.

Анализ состояния дел в области защиты информации показывает, что в промышленно развитых странах мира уже сложилась вполне оформившаяся инфраструктура защиты информации (ЗИ) в системах обработки данных. И тем не менее, количество фактов злоумышленных действий над информацией не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. В этом смысле Украина не является, к сожалению, исключением.

Среди всех возможных каналов утечки информации наибольшую опасность в Украине в ближайшее время, очевидно, будут представлять технические каналы. Такое представление основывается на следующих факторах:

- наличие в Украине большого числа технически грамотных специалистов, знания и навыки которых не востребованы вследствие тяжелого экономического положения;
- выход на украинский рынок фирм других стран – производителей аппаратуры для технического шпионажа;
- недостаточное внимание, а чаще всего просто игнорирование проблем безопасности информации со стороны руководящего состава министерств, ведомств и организаций.

Сегодня уже ни для кого не секрет, что наряду с такими «обычными» техническими каналами утечки информации, как установка радиомикрофонов, подключение к телефонной линии связи, акустическое подслушивание, дистанционное фотографирование и т.д., существует ещё и радиотехнический канал утечки информации из средств вычислительной техники.

Проблема утечки информации из вычислительной техники через побочные электромагнитные излучения и наводки (ПЭМИН) известна уже давно. Однако