АВТОМАТИЗАЦІЯ
КОМП'ЮТЕРИЗАЦІЯ
ІНФОРМАТИЗАЦІЯ

П. Біленчук, А. Кофанов, О. Кобилянський, В. Міщенко
СИСТЕМНА ІНФОРМАТИЗАЦІЯ ДІЯЛЬНОСТІ ОРГАНІВ ДІЗНАННЯ ТА ДОСУДОВОГО СЛІДСТВА: СИСТЕМОЛОГІЯ, КІБЕРНЕТИКА, КОНСОЛІДОВАНА АНАЛІТИКА, БЕЗПЕКА

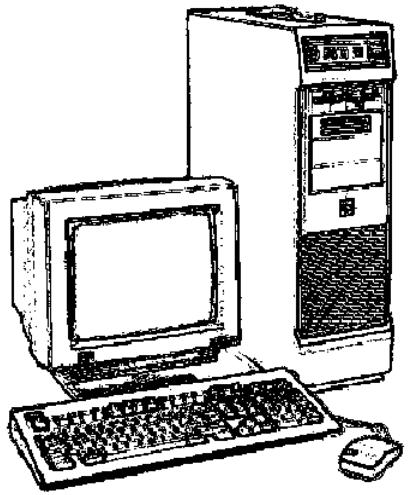
- П. Біленчук, А. Кофанов, О. Кобилянський
КРИМІНАЛІСТИЧНА ІНФОРМАЦІЙНО-КОМП'ЮТЕРНА АНАЛІТИКА: ХАРАКТЕРИСТИКА, СИСТЕМНА КЛАСИФІКАЦІЯ, РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ
- П. Біленчук, А. Кофанов, О. Кобилянський
АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ СИСТЕМИ ОРГАНІВ ПРАВОПОРЯДКУ УКРАЇНИ: ХАРАКТЕРИСТИКА, СИСТЕМНА КЛАСИФІКАЦІЯ, РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ
- П. Біленчук, А. Кофанов, О. Кобилянський
ІНПОЛ: ІНФОРМАЦІЙНА СИСТЕМА ПОЛІЦІЇФРН
- П. Біленчук, А. Кофанов, О. Кобилянський
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КОМП'ЮТЕРНИХ ЗЛОЧИНІВ, ВЧИНЕНИХ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський
КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ У КРЕДИТНО-ФІНАНСОВІЙ ІНДУСТРІЇ: КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

П.Д. БІЛЕНЧУК
А.В. КОФАНОВ
О.Л. КОБИЛЯНСЬКИЙ
В.Б. МІЩЕНКО

СИСТЕМНА ІНФОРМАТИЗАЦІЯ ДІЯЛЬНОСТІ ОРГАНІВ ДІЗНАННЯ ТА ДОСУДОВОГО СЛІДСТВА:

СИСТЕМОЛОГІЯ, КІБЕРНЕТИКА, КОНСОЛІДОВАНА АНАЛІТИКА, БЕЗПЕКА

Довідкове, інформаційно-аналітичне і комунікаційне забезпечення запобігання, протидії, розслідування злочинів



«НАУКОВА БІБЛІОТЕКА КРИМІНАЛІСТА» презентує підручники, монографії, навчальні посібники в таких галузях знань:

- Серія „Людина, право, суспільство”
- Серія „Економіка, фінанси, право”
- Серія „Безпека людини, суспільства, держави”
- Серія „Національна і міжнародна безпека”
- Серія „Міжнародне співробітництво”
- Серія „Мас-медіа”
- Серія „Криміналістична освіта XXI століття”
- Серія „Криміналістична наука в цивільному, господарському та

- Серія „Міжнародна і вітчизняна злочинність”
- Серія „Запобігання, протидія, розслідування злочинів”
- Серія „Автоматизація, комп’ютеризація, інформатизація”
- Серія „Зброєзнавство і мисливствознавство”
- Серія „Інформація+Інтелект+Інновації”
- Серія „Електронна фотографія та відеозапис”
- Серія „Криміналістичне забезпечення органів правопорядку”
- Серія „Археологія, архітектура, історія, культура, спадщина”
- Серія „Власність, земля, право”

Відгуки, рекомендації та пропозиції просимо надсилати за адресою:
03150, Україна, м. Київ,
вул. П.Любченка, 15, оф. 219
або електронною поштою:
E-mail: peregin@mail.ru
Тел. (067) 573-83-07
Тел./факс: (044) 468-31-21

Навчальне видання

Петро Дмитрович БІЛЕНЧУК
Андрій Віталійович КОФАНОВ
Олег Леонідович КОБИЛЯНСЬКИЙ
Василь Борисович МІЩЕНКО

СИСТЕМНА ІНФОРМАТИЗАЦІЯ ДІЯЛЬНОСТІ ОРГАНІВ ДІЗНАННЯ ТА ДОСУДОВОГО СЛІДСТВА:
СИСТЕМОЛОГІЯ, КІБЕРНЕТИКА, КОНСОЛІДОВАНА АНАЛІТИКА, БЕЗПЕКА

Монографія

Підписано до друку 08.09.2010.
Формат 60×84. Папір офсетний.
Тираж 300 прим.

Видавництво „КИЙ”
Адреса: 0436, Київ-136,
вул. Гречка, 13, кім. 216.

Свідоцтво про внесення суб’єкта видавничої справи
до Державного реєстру видавців, виготовників
і розповсюджувачів видавничої продукції
серія ДК № 1168 від 24.12.2002 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПІДГОТОВКИ СЛІДЧИХ І КРИМІНАЛІСТІВ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ КРИМІНАЛІСТИКИ

П.Д. БІЛЕНЧУК
А.В. КОФАНОВ
О.Л. КОБИЛЯНСЬКИЙ
В.Б. МІЩЕНКО

СИСТЕМНА ІНФОРМАТИЗАЦІЯ ДІЯЛЬНОСТІ ОРГАНІВ ДІЗНАННЯ ТА ДОСУДОВОГО СЛІДСТВА:
СИСТЕМОЛОГІЯ, КІБЕРНЕТИКА, КОНСОЛІДОВАНА АНАЛІТИКА, БЕЗПЕКА

Монографія

Серію засновано у 2000 році А.В. Кофановим

Київ 2010

ББК 67.52я73
Б 61

Схвалено та затверджено кафедрою криміналістичної техніки ННІПСК КНУВС та рекомендовано до друку вченою радою Європейського університету управління, безпеки та інформаційно-правових технологій (протокол № 10 від 07.09.2010 року).

Рецензенти:
М.Т. Задояний – кандидат юридичних наук, доцент
В.В. Кравчук – кандидат економічних наук, доцент
В.В. Піксотов – кандидат технічних наук, доцент

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Міщенко В.Б.
Б 61 Системна інформатизація діяльності органів дізнання та досудового слідства: системологія, кібернетика, консолідована аналітика, безпека. – Монографія. – Київ: КИЙ, 2010. – 80 с. – (Серія „Автоматизація, комп'ютеризація, інформатизація").

У монографічному дослідженні аналізуються пріоритетні напрями інформатизації органів досудового слідства.

Для студентів і викладачів юридичних навчальних закладів.

ББК 67.52я73

51. *Саницький В.А., Карацюба А.М., Святобог В.В. та ін.* Система інформаційного забезпечення ОВС України: Навчально-практичний посібник / За ред. Л.В. Бородича. – К., 2000. – - 144 с: іл., табл.

52. *Семенюк Э.П.* Информация, как фактор повышения устойчивости развития // Междунар. форум по информатизации, 2001, Т. 36, № 1. – С. 3-10.

53. Системна інформатизація правоохоронної діяльності: Монографія. – Кн. 1. За ред. В. Дурдинця, В. Євдокимова, М. Швеця. – К.: НДЦПІ АПрН України, 2006. – 287 с.

54. Системна інформатизація правоохоронної діяльності / За ред. В. Дурдинця, М. Швеця. – К.: НДЦПІ АПрН України, 2007. – 382 с.

55. *Сляднева Н.А.* Информационно-аналитическая деятельность: проблемы и перспективы // Информационные ресурсы России. М. – 2001. – № 3 (57). – С. 14.

56. *Соколов А.В., Степанюк О.М*. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург; Арлит, 2002. – 496 с.

57. *Сунь-Цзы* Трактаты о военном искусстве / Сунь-Цзы, У-Цзы; Пер с кит., предисл. и коммент. Н.И. Конрада. – М.:ООО "Издательство АСТ"; СПб.: Terra Fantastica, 2002. – 558 с.

58. *Хохлов Е., Бурыгин Н.* Приоритетные идеи в области управления (Руководство для управляющих, советников высшей администрации и научных работников). – К., "ЛИБРА"-НМПЦА. – 1993. – С. 62-65.

35. *Міщенко В.Б.* Захист інформації в сучасних умовах // Удосконалення системи воєнно-наукової інформації ЗС України: Матеріали науково-практичної конференції. м. Київ, 28.5.2002. – К.: в/ч А0202. – С. 64-70.

36. *Міщенко В.Б.* Національна безпека України: сучасні інформаційні технології та можливі джерела небезпеки. / В.Б. Міщенко, О.І. Мотлях, П.Д. Біленчук та ін. // Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – С. 45-70.

37. *Міщенко В.Б.* Аналітичний підхід до забезпечення безпеки інформації. // Друга міжнародна конференція "Інформаційні технології в банківській та страховій справі": Збірник наукових праць. – К.: BeeZone, 2003. – С. 62-64.

38. *Минкина В.А.* От библиографии техники к информационному управлению: на пути к интеллектуальному преобразованию информации // Научно-техническая информация. – 2003. – № 6. – С. 2-7.

39. *Минкина В.А.* От информационного обеспечения к информационному управлению деятельности организации // Научно-техническая информация. – 2002. – №4. Сер. 1. – С. 19-23.

40. *Нестеренко О.В.* Єдина державна система електронних інформаційних ресурсів // Науково-технічна інформація. – 2003. – № 4. – С. 3-9.

41. *Осинський Л.М.. Міщенко В.Б.* Стаття на спеціальну тему // Науково-технічний збірник в/ч А1906. – К., 2001. – №2. – С. 30-34.

42. *Пархоменко А.В.* Управление научно-технической информацией и знаниями – ключ к развитию общества // 10th International Seminar "Scientific and Technical information in Central and Eastern Europe" Zakopane, 10-12 may 2001.

43. *Пархоменко В.Д., Пархоменко А.В.* Научно-методические основы информационно-аналитического обеспечения принятия решений // Труди V Міжнар. науково-практичної конф. „Інформація, аналіз, прогноз – стратегічні важелі державного управління". – К. УкрІНТЕІ. – 2001. – С 26-35.

44. *Пархоменко В.Д., Гончаренко А.П, Пархоменко О.В.* Проблеми ресурсного забезпечення в системі прийняття управлінських рішень // Матеріали III Міжнародної наук.-практ. конф. „Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління". – К.: УкрІНТЕІ. – 2002. – С. 28-32.

45. *Пархоменко О.В., Гончаренко А.П.* Деякі аспекти створення аналітичних блоків інформації // Науково-технічна інформація. – 2000. – № 4. – С. 19-20.

46. *Пархоменко О.В.* Класифікація та ідентифікація джерел інформації в аналітичній роботі // Науково-технічна інформація. – 2001. – № 1. – С. 29-31.

47. *Пирятинська С.Ф., Гончаренко А.П., Пархоменко О.В.* Наукові і організаційні проблеми управління інформаційними ресурсами // Науково-технічна інформація. – 2001. – № 3. – С. 31-34.

48. *Плэтт В.* Стратегическая разведка. Основные принципы. – М.: Издательский дом "ФОРУМ", 1997. – 376 с.

49. Програма інформатизації органів внутрішніх справ України на 2000-2010 роки. – К., Управління оперативної інформації МВС України, 1999.

50. *Ронин Р.* Своя разведка. – Минск: "Харвест", 1997. – С. 6-61.

ЗМІСТ

17. *Вертузаєв М.С., Юрченко О.М.* Захисті інформації в комп'ютерах від несанкціонованого доступу: Навчальний посібник / за ред. С.Г. Лаптєва. – К.: В-во Європ. Ун-ту, 2001. – 321 с.

18. Вступ до інформаційної культури та інформаційного права / Брижко В.М., Гавловський В.Д., Калюжний Р.А. та ін. – Ужгород: 1ВА, 2003. – 239 с.

19. *Гнип О.М.* Методи створення електронних каталогів інформаційних ресурсів INTERNET // Удосконалення системи воєнно-наукової інформації Збройних Сил України : Матеріали наук.-практ. конференції, м. Київ, 28 трав. 2002 р. – К.: в/ч А0202, 2002. – С. 70-75.

20. *Гуриев М.А.* Вопросы формирования информационных ресурсов руководителей высшего уровня // Информационные ресурсы России. – 2001. – № 2 (57). – С. 11-13.

21. *Давыдов Ю.* Тайна фирмы. – К.: "Фирма Колир-2", 1993. – 176 с.

22. *Добров Г.М.* и др. Экспертные оценки в научно-техническом прогнозировании. – К.: Наукова думка, 1974. – 160 с.

23. *Домарев В.В*. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС"", 2001. – 688 с.

24. *Доронин А.* Информационный мир в прицеле спецслужб. // Солдат удачи. – 2001. – № 4 [79]. – С. 39-41.

25. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. // Відомості Верховної Ради України. – 1998. – № 27-28. Ст. 181.

26. *Кохановсъка О.В.* Правове регулювання у сфері інформаційних відносин. – К.: Національна академія внутрішніх справ України, 2001. – 212 с.

27. *Крулькевич М.И., Сынкова Е.М.* Информационная деятельность в организациях. – Донецк, 2001. – 176 с.

28. *Малицький Б.А., Попович О.С., Соловйов В.П.* Перспективні напрями науково-технічного та інноваційного розвитку України. – К.: Фенікс, 2006. – 208 с.

29. *Малиновсъкий Б.М.* Відома і невідома історія інформаційних технологій в Україні. – К.: Видавничий дім „Академперіодика", 2001. – 213 с.

30. *Мінченко А.В., Галас О.Р.* Правова інформатика. Інформація та інформаційне забезпечення правоохоронних органів: Навчальний посібник. – Арістей, 2003. – 436 с.

31. *Міщенко В.Б*. Національна безпека України: сучасні інформаційні технології та можливі джерела безпеки. // Вісник Академії праці та соціальних відносин ФП України. – К.: АПСВ ФПУ. – 1998. – № 1. – С. 61-72.

32. *Міщенко В.Б*. Використання інформаційних технологій для забезпечення прийняття рішення в банківській та страховій установі. // Інформаційні технології в банківській та страховій справі. Збірник наукових праць. – К.: BeeZone, 2002. – С. 22-27.

33. *Міщенко В.Б*. Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2002 № 2 (19). – С. 217-223.

34. *Міщенко В.Б*. Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2000. – № 3 (12). – С. 190-196.

ВИКОРИСТАНА І РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. *Бауес (B.Bowes)* Европейская модель обработки информации и доступа к ней Европейского совета информационных ассоциаций. Размышления и виды на будущее потребителей профессиональной информации // Международный форум по информации и документации. – 1997. – № 3 (т. 22).

2. *Бачило И.Л.* Право собственности на информационные ресурсы // Информационные ресурсы России. – 2001. – № 2. – С. 29-33.

3. *Белкин СВ.* Информатика и аналитика социологического мониторинга инновационного развития региона // НТИ. Сер. 1. – 2005. – № 5. – С. 2-12.

4. *Біленчук Д.П., Біленчук П.Д., Котляревський О.І.* Комп'ютерний злочинець: поняття, характеристика, класифікація // Вісник АПСВ, 1998, № 2. – С. 193-202.

5. *Біленчук Д.П., Котляревський О.І.* Інформаційна злочинність // Міліція України, 1999, № 1-2. – С. 31.

6. *Біленчук Д.П., Біленчук П.Д., Котляревський О.І.* Організована комп'ютерна злочинність // Суд в Україні: боротьба з корупцією, організованою злочинністю і захист прав людини. – К.: 1999, Т. 12. – С. 467-483.

7. *Біленчук П.Д., Зубань М.А.* Комп'ютерні злочини. – Київ, 1994. – 72 с.

8. *Біленчук П.Д., Котляревський О.І., Кофанов А.В.* Портрет комп'ютерного злочинця. – Київ, 1997. – 48 с.

9. *Біленчук П.Д. Котляревський О.І.* Основи комп'ютерної криміналістики // Криміналістика. Підручник. – Київ, 1998. – 416 с.

10. *Біленчук П.Д., Міщенко В.Б, Борисова Л.В.* Аналіз та прогноз стану безпеки об'єкту обчислювальної техніки. // Открытые информационные и компьютерные интегрированные технологии: Сб. научн. трудов. – Х.: НАКУ "ХАИ", 2002. – С. 127-135.

11. *Биленчук П.Д., Джужа А.Н.* Использование достижений науки и техники в деятельности органов внутренних дел. – К.: РИО МВД УССР, 1982. – 20 с.

12. *Биленчук П.Д., Лукьянова О.Н., Романенко В.М.* Компьютерная психофизиологическая диагностика личности и использование ее результатов в деятельности органов внутренних дел. – К.: РИО МВД УССР, 1988. – 78 с.

13. *Бірюков В.В.* Научные и практические основы использования компьютерных технологий для фиксации криминалистически значимой информации. – Луганск, 2002.

14. *Братко-Кутинський О.* Феномен України. – К.: газета "Вечірній Київ"; Українська академія оригінальних ідей, 1996. – 304 с.

15. *Брижко В.М., Марченко Л.С.* Від інформації до інформації // 36. наук. пр. Державного науково-дослідного інституту інформатизації та моделювання економіки. – К., 1996. – С. 16-24.

16. 1С: Бухгалтерия. Версія 7.7. Руководство пользователя. – М., Фирма "1С", 2001.

РОЗДІЛ 1
ДОКТРИНАЛЬНІ ЗАСАДИ ДОВІДКОВОГО, АНАЛІТИЧНОГО І КОМУНІКАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ДОСУДОВОГО СЛІДСТВА: АВТОМАТИЗАЦІЯ, СИСТЕМОЛОГІЯ, КІБЕРНЕТИКА, ІНФОРМАТИКА

1.1. Єдина інформаційно-комп'ютерна система по забезпеченню запобігання, протидії і розслідування злочинів

УКАЗ
ПРЕЗИДЕНТА УКРАЇНИ

Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю

З метою поліпшення координації організаційних, оперативно-розшукових, правових та інформаційних заходів правоохоронних органів щодо боротьби зі злочинністю, підвищення рівня роботи в цій сфері **постановляю**:

1. Визнати за необхідне створення Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю (далі – Єдина комп'ютерна система).

2. Кабінету Міністрів України забезпечити здійснення заходів щодо створення Єдиної комп'ютерної системи, в тому числі:

– утворення у двотижневий строк Міжвідомчої координаційної групи з питань створення і функціонування Єдиної комп'ютерної системи із включенням до її складу представників Апарату Ради національної безпеки і оборони України, Служби безпеки України, Міністерства внутрішніх справ України, Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України та Генеральної прокуратури України;

– розроблення і подання в чотиримісячний строк зазначеною Міжвідомчою координаційною групою проектів програми створення і функціонування Єдиної комп'ютерної системи та положення про цю Систему;

– вирішення в установленому порядку питань фінансування заходів щодо створення і функціонування Єдиної комп'ютерної системи.

3. Апарату Ради національної безпеки і оборони України забезпечувати діяльність Міжвідомчої координаційної групи з питань створення і функціонування Єдиної комп'ютерної системи, утвореної Кабінетом Міністрів України.

Президент України В.ЮЩЕНКО
м. Київ, 31 січня 2006 року № 80/2006

1.2. Теоретико-методологічні засади інформаційно-аналітичного і комп'ютерно-комунікаційного забезпечення діяльності органів досудового слідства

Вдосконаленню діяльності правоохоронних органів присвячена низка спеціальних нормативно-правових актів, програм, і зокрема Указ Президента України «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю».

Втілюючи в життя ці завдання, багато зроблено щодо дослідження, проектування і впровадження галузевої комп'ютеризованої системи МВС України як складової частини загальнодержавної системи.

Програма націлена на розроблення та впровадження комп'ютеризованих інформаційних систем у правоохоронних органах.

Основною її метою є створення інформаційно-комп'ютерних систем, що забезпечують:

– підвищення рівня керівництва підрозділами правоохоронних органів;

– зниження впливу суб'єктивних чинників при виробленні рішень, що приймаються за заявами і повідомленнями громадян;

– контроль дотримання законності;

– зниження трудомісткості і підвищення культури обробки інформації;

– повніше використання фондів і джерел інформації в попередженні правопорушень, розшуку злочинців, що переховуються, розшуку осіб, зниклих безвісти, і в інших випадках;

– раціональну розстановку сил і засобів, підвищення ефективності взаємодії підрозділів;

– підвищення якості розробки відомчих нормативних актів та вирішення інших завдань.

Для реалізації цих цілей здійснено і здійснюється:

– розробка теоретичних засад побудови комп'ютеризованої системи оперативного управління в органах внутрішніх справ;

– моделювання вирішення завдань синхронізації в складних системах організаційного управління;

– уніфікація документообігу, раціоналізація вирішення завдань оперативного управління;

– розробка методів і засобів вирішення спеціальних пошукових, розпізнавальних та інших завдань в інтересах штабів, чергових частин, карного розшуку, профілактики, слідства, боротьби з економічними злочинами, хабарництвом, раціоналізації патрульно-постової служби та інших підрозділів.

Методологічний підхід до вирішення проблеми викладений в проектах на різних рівнях деталізації і представлено у вигляді:

– загальна схема, основні поняття (подання на рівні змістовного моделювання);

– блок-схема моделі автоматизованого управління, що включає підсистеми: планування, облік, аналіз, прогнозування та їх взаємозв'язок (опис на рівні представлення макроекономічних моделей);

– модель комп'ютеризованої системи управління (опис з використанням

– на місцевості (в будівлі), де розташовано об'єкт, відсутні об'єкти, що містять в собі небезпечні сили і створюють реальну загрозу об'єкту від техногенних катастроф або стихійних лих, або, за наявності таких, відпрацьовані ефективні механізми запобігання негативним явищам чи мінімізації збитків для об'єкту внаслідок їх виникнення.

Література

1. *Соколов А.В., Степанюк О.М*. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург; Арлит, 2002. – 496 с.

2. *Вертузаєв М.С., Юрченко О.М.* Захисті інформації в комп'ютерах від несанкціонованого доступу: Навчальний посібник / за ред. С.Г. Лаптєва. – К.: В-во Європ. Ун-ту, 2001. – 321 с.

3. *Домарев В.В*. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС"", 2001. – 688 с.

4. *Міщенко В.Б*. Національна безпека України: сучасні інформаційні технології та можливі джерела безпеки. // Вісник Академії праці та соціальних відносин ФП України. – К.: АПСВ ФПУ. – 1998. – № 1. – С. 61-72.

5. *Біленчук П.Д., Міщенко В.Б, Борисова Л.В.* Аналіз та прогноз стану безпеки об'єкту обчислювальної техніки. // Открытые информационные и компьютерные интегрированные технологии: Сб. научн. трудов. – Х.: НАКУ "ХАИ", 2002. – С. 127-135.

6. *Осинський Л.М.. Міщенко В.Б.* Стаття на спеціальну тему // Науково-технічний збірник в/ч А1906. – К., 2001. – №2. – С. 30-34.

7. *Хохлов Е., Бурыгин Н.* Приоритетные идеи в области управления (Руководство для управляющих, советников высшей администрации и научных работников). – К., "ЛИБРА"-НМПЦА. – 1993. – С. 62-65.

8. *Добров Г.М*. и др. Экспертные оценки в научно-техническом прогнозировании. – К.: Наукова думка, 1974. – 160 с.

9. *Міщенко В.Б*. Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2002 № 2 (19). – С. 217-223.

10. *Міщенко В.Б*. Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2000. – № 3 (12). – С. 190-196.

11. *Міщенко В.Б*. Захист інформації в сучасних умовах // Удосконалення системи воєнно-наукової інформації ЗС України: Матеріали науково-практичної конференції. м. Київ, 28.5.2002. – К.: в/ч А0202. – С. 64-70.

12. *Міщенко В.Б*. Національна безпека України: сучасні інформаційні технології та можливі джерела небезпеки. / В.Б. Міщенко, О.І. Мотлях, П.Д. Біленчук та ін. // Комп'ютерна злочинність: навчальний посібн. – К.: Атіка, 2002. – С. 45-70.

13. *Міщенко В.Б*. Аналітичний підхід до забезпечення безпеки інформації. // Друга міжнародна конференція "Інформаційні технології в банківській та страховій справі": Збірник наукових праць. – К.: BeeZone, 2003. – С. 62-64.

d1 – політичні чинники:

– вища державна влада, національне законодавство та підзаконні акти чітко окреслюють дозволені та недозволені діяння і порядок запобігання останнім, а також оперативно реагують на зміни у зовнішній або внутрішній ситуації;

– військово-політична обстановка в державі (регіоні) регламентована системою договорів і угод, наявні дієві механізми для їх дотримання і впровадження в життя;

d2 – техногенні чинники:

– технічний стан загальних ліній і обладнання енергопостачання, телекомунікацій та зв'язку виключає або суттєво знижує імовірність виникнення проблем із збереженістю інформації, вразливі місця у вказаному обладнанні знаходяться під контролем, наявні ефективні сили та засоби для запобігання проблемам та успішної ліквідації їх наслідків;

– параметри напруги, частоти, струму постійно знаходяться у допустимих межах, наявні засоби для їх успішного регулювання;

– електромагнітні поля та шуми, викликані роботою промислового та побутового електрообладнання екрануються і не впливають на роботу засобів обробки, зберігання та передачі інформації;

d3 – соціальні чинники:

– діяльність супротивника та/або криміналітету, спрямована на нанесення збитків об'єкту (персоналу, обладнанню) та/або його СУОІ, а також на заволодіння інформацією, знаходиться під постійною профілактикою спецслужб та правоохоронних органів, будь-які спроби ворожої діяльності щодо об'єкту обчислювальної техніки, його персоналу, устаткування і т.д. своєчасно викриваються та оперативно і успішно нейтралізуються;

– діяльність партійних, профспілкових, етнічних, релігійних та їм подібних угруповань, наслідком якої може бути нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації знаходиться під постійною профілактикою спецслужб та правоохоронних органів, будь-які спроби ворожої діяльності щодо об'єкту обчислювальної техніки, його персоналу, устаткування і т.д. своєчасно викриваються та оперативно і успішно нейтралізуються;

– соціальний стан широких мас населення і персоналу задовільний, наявні дієві механізми соціальних гарантій, матеріальна винагорода за працю (службу) як персоналу об'єкту, так і місцевому населенню, своєчасна і за обсягами гарантує сталий прожитковий рівень не нижчий з середній у державі (регіоні);

d4 – природні (географічні) чинники:

– на місцевості (в будівлі), де розташовано об'єкт відсутні або контрольовані такі природні або штучні елементи, які сприяють успішному веденню прихованого спостереження і розвідки, несанкціонованому проникненню всередину об'єкта, раптовому нападу на об'єкт та персонал;

формальної мови);

– машинна модель системи оперативного управління для вирішення конкретних завдань управління (опис на рівні засобів програмування, термінології організації і технології електронної обробки даних);

– конкретні практичні застосування моделі комп'ютеризованої системи оперативного управління.

З позицій системного підходу в проекті розглядаються:

– система органів державного управління і завдання підвищення рівня управління на основі застосування сучасних методів і засобів інформаційно-обчислювальної техніки;

– місце і призначення органів внутрішніх справ у системі органів державного управління;

– основні завдання структурних підрозділів органів внутрішніх справ;

– проблеми оперативного управління в підрозділах органів внутрішніх справ, специфіка вирішуваних завдань;

– основні принципи побудови комп'ютеризованої системи управління як сучасного засобу підвищення рівня керівництва підрозділами органів внутрішніх справ;

– комплексна програма створення галузевої комп'ютеризованої системи управління;

– використання досвіду створення сучасних систем обробки даних у світовій практиці та їх значення в підвищенні ефективності та якості оперативного управління органами охорони громадського правопорядку;

– основні концептуальні засади побудови системи оперативного управління;

– методологія побудови моделі системи оперативного управління;

– метод вирішення завдань синхронізації;

– основні набори із комплексу універсально-збірних елементів: «планування», «облік», «аналіз», «прогнозування»;

– принципи побудови типової інформаційно-пошукової (довідкової) системи колективного користування, призначеної для обслуговування входів і виходів автоматизованої системи оперативного управління, та інші питання.

1.3. Інформаційно-комп'ютерне та комунікаційне забезпечення органів досудового слідства: ресурси, функціональні можливості, електронні послуги і продукти

1.3.1. Державна програма комп'ютеризованої інформаційної системи органів внутрішніх справ України на 2007-2012 роки

Державна програма комп'ютеризованою інформаційної системи органів внутрішніх справ України на 2007-2012 роки

Найменування заходу	Відповідальні за виконання	Строк виконання	Орієнтовний обсяг фінансування, тис. грн.	У тому числі за роками:					
				2007	2008	2009	2010	2011	2012
Формування та актуалізація інформаційних ресурсів									
Розробка моделі інтегрованих інформаційних ресурсів з розподіленням в межах регіонального та центрального рівнів з урахуванням потреб ОВС в інформаційно-аналітичному забезпеченні оперативно-службової діяльності та Законів про інформацію і захисті персональних даних	НАВСУ, ДІТ	2007							
Створення та впровадження автоматизованих систем інформації обміну та реплікації даних між рівнями інтеграції та функціональними спеціалізованими інформаційними системами	ДІТ, УІТ (ВІТ)	2007	1300	1300					
Створення та впровадження програмного забезпечення функціональних робочих місць співробітників галузевих служб для введення, експлуатації та використання інформаційних ресурсів регіонального та центрального рівнів.	ДІТ, УІТ (ВІТ)	2009							

– діяльність релігійних угруповань, наслідком якої може бути нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації;

b4 – природні (географічні) чинники:
– на місцевості (в будівлі), де розташовано об'єкт наявні природні (рослинність, каміння, рельєф місцевості тощо) або штучні (огорожі, стовпи, опори, тунелі, вікна, двері, люки і т.д) елементи, які сприяють успішному веденню прихованого спостереження і розвідки, несанкціонованому проникненню всередину об'єкта, раптовому нападу на об'єкт та персонал;
– на місцевості (в будівлі), де розташовано об'єкт, наявні об'єкти, що містять в собі небезпечні сили і створюють реальну загрозу об'єкту від техногенних катастроф (сховища небезпечних матеріалів, небезпечні виробництва, греблі, водосховища і т.д.) або стихійних лих (повені, зсуву, каменепаду тощо);

b5 – несанкціонований доступ:
– до документів та машинних носіїв інформації;
– до окремого робочого місця;
– до обчислювальної мережі;

b6 – перехоплення даних:
– акустичним способом;
– візуальним способом;
– перехоплення електромагнітних випромінювань апаратури.

Нейтральні або випадкові параметри середовища

c – нейтральні або випадкові параметри середовища.

До випадкових чинників відносять такі, чий вплив на інформацію не піддається достовірному прогнозуванню, а в окремих випадках неможливо передбачити саму наявність цих чинників. В поєднанні з впливом інших чинників, вплив випадкових чинників (який окремо може не завдавати шкоди) може викликати не передбачувані наслідки.

Потенційні джерела не передбачуваного впливу:
– метеорологічні: раптові зміни в метеорологічній (гідрологічній) обстановці;
– природні і техногенні: непрогнозовані катастрофи, аварії, стихійні лиха, чий небезпечний радіус (смуга) захоплює місце розташування об'єкту;
– зовнішньо-соціальні: вибухи соціальної активності населення (громадська непокора, кримінально карані діяння тощо), не спрямовані безпосередньо проти об'єкту, персоналу та системи інформації;
– внутрішньо-соціальні: непередбачувані зміни в майновому (сімейному) стані осіб з числа персоналу об'єкту та в діяльності і стані об'єктів-партнерів.

Сприятливі параметри середовища

d – сприятливі параметри середовища.

залежно від обсягів інформації, або звичайними засобами (шляхом організаційних заходів), або за допомогою спеціальних апаратних систем. Порядок копіювання має забезпечувати 100% гарантії збереження, як мінімум, всіх змін в даних, здійснених на будь-яких момент часу.

Обов'язково: джерела безперебійного живлення, які необхідно підбирати залежно від загальної кількості електронно-обчислювальної техніки та вимог до захисту інформації.

Контроль за «вірусами» повинен здійснюватись виконавцями в частині, що їх стосується, а в цілому – окремо виділеною штатною чи нештатною посадовою особою. Необхідно вести каталог «вірусів» та «антивірусів», здійснювати поновлення антивірусних програм серед виконавців, контролювати входи в локальну мережу із корпоративних та глобальних на предмет появи «вірусів».

Активно протидіючі системі ворожі параметри середовища

B – активно протидіючі системі ворожі параметри середовища:

b1 – політичні чинники:

– непередбачуваність вищої державної влади і національного законодавства;

– непередбачуваність, корумпованість тощо посадових осіб місцевих органів влади;

– непередбачуваність військово-політичної обстановки в державі (регіоні);

b2 – техногенні чинники:

– незадовільний технічний стан загальних ліній і обладнання енергопостачання, телекомунікацій та зв'язку, наявність вразливих місць у вказаному обладнанні;

– нестійкі параметри напруги, частоти, струму;

– електромагнітні поля та шуми, викликані роботою промислового та побутового електрообладнання;

b3 – соціальні чинники:

– негативне ставлення громадськості, преси, політичних та суспільних організацій, партій і рухів;

– діяльність конкурентів (розвідок), спрямована на нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації, а також на заволодіння інформацією;

– діяльність криміналітету, спрямована на нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації;

– діяльність етнічних угруповань, наслідком якої може бути нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації;

– діяльність профспілкових та їм подібних угруповань, наслідком якої може бути нанесення збитків об'єкту (персоналу, обладнанню) та/або його системі інформації;

Розробка та впровадження програм конвертації до інтегрованого банку даних інформаційних масивів інших міністерств та відомств необхідних для виконання завдань інформаційно-аналітичного забезпечення ОВС.	Галузеві служби МВС	2010	140	80	20	20	20		
Розробка та впровадження аналітичних систем збору інформаційних відомостей із глобальної мережі Internet.	ДІТ	2008	150	85	25	10	20		
Міжнародна та міжвідомча інформаційна взаємодія									
Розробка та впровадження програмно-технологічного забезпечення обміну інформаційними ресурсами в межах визначених договорами з правоохоронними органами країн СНД (МІБ).	ДІТ	2007	200	200					
Створення функціональних робочих місць національного сегменту віртуального центру ГУАМ по боротьбі з тероризмом, організованою злочинністю та іншими небезпечними видами злочинів	ДІТ								
Поетапне впровадження міжвідомчої системи збору та аналізу даних щодо незаконного обігу наркотиків (БУМАД)	ДІТ								
Створення та впровадження єдиної інформаційно – телекомунікаційної системи правоохоронних органів з питань боротьби зі злочинністю (на виконання Указу Президента України від 31 січня 2006 року №80 «Про Єдину комп'ютерну систему правоохоронних органів з питань боротьби зі злочинністю»).	ДІТ								

Створення та впровадження функціонального вузла МВС України у складі інтегрованої міжвідомчої інформаційно-телекомунікаційної системи щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон «Аркан»	ДІТ								
Створення та впровадження центрального банку даних єдиного державного номерного обліку вогнепальної зброї ДБД «Арсенал».	ДІТ	2007	360	360					
Комп'ютерне озброєння співробітників органів внутрішніх справ України	ДІТ, (Г)УМВС		465 660,0	68970	68970	68970	66250	66250	66 250
Установка нових та модернізація серверних комплексів (Г)УМВС та центрального апарату	ДІТ, (Г)УМВС	2009	8 160,0	2720	2720	2720	-	-	-
МВС України відповідно до збільшення обсягів даних та розширення мережі користувачів									
Забезпечення (Г)УМВС областей, підпорядкованих їм міськрайлінорганів та центрального апарату МВС України комп'ютерною та оргтехнікою відповідно до функціонального призначення та подальшого навантаження співробітників по окремим напрямкам діяльності	ДІТ, (Г)УМВС	2012	397 500,0	66250	66250	66250	66250	66250	66 250
Поетапне створення функціональних підсистем та автоматизованих робочих місць відповідно до завдань та функцій користувачів інтегрованої інформаційно-пошукової системи МВС України		2012							
Розбудова мережі передачі даних, створення локальних та корпоративних мереж загального використання	ДІТ, УЗ (Г)УМВС		137 685,0	35 295	41 970	40 270	12 550	7 600	-

Технічні засоби.(Q5)

Витік конфіденційної інформації може відбуватися при користуванні засобами зв'язку. Застосовувати незахищені особливим чином канали зв'язку при передачі держтаємниці заборонено взагалі. В той самий час не можна виключити ведення по відкритим каналам зв'язку переговорів із згадування інших конфіденційних відомостей. Тому при веденні телефонних переговорів спершу необхідно надійно ідентифікувати співбесідника. Сама ж телефонна лінія має періодично перевірятися на предмет захищеності від несанкціонованого знімання інформації. Для передачі даних різної важливості застосовувати різні канали (лінії) зв'язку.

Під контролем треба тримати місця підключення об'єкту до загальних мереж зв'язку, електроживлення тощо (місце підключення та контрольні значення робочих параметрів – струму, напруги, частоти та ін.). На об'єктах із значною кількістю телефонних абонентів доцільно влаштувати внутрішню АТС із контрольованим виходом на місто.

Внутрішню мережу електроживлення необхідно відв'язувати від загальної через систему спеціальних шумових фільтрів, а також використовувати джерела безперебійного живлення. Ці заходи, крім захисту інформації від перехоплення, крім того, знижують можливість втрат даних на ЕОМ через збої в електропостачанні (падіння чи скачок напруги, частоти шуми і т.д.).

При веденні переговорів по бездротовому зв'язку, який найбільше потерпає від перехоплення, необхідно вживати заходів шифрування інформації, залежно від значення інформації гарантованої або тимчасової стійкості.

Засоби обчислювальної техніки (Q6)

Всі без винятку засоби ЕОТ повинні бути придбані в офіційних представників з відповідними гарантійними документами на вироби. Апаратуру, призначену для обробки найважливіших відомостей, крім того, необхідно перевірити на предмет відсутності випромінювань та розвідувальних засобів. Кабельне господарство мережі (якщо така є) має бути по можливості, екроване та недоступне для сторонніх осіб. Для зберігання та/або обробки даних різного рівня важливості застосовувати різні ЕОМ.

Для прокладення мереж максимально застосовувати оптично-волоконні лінії зв'язку, які не випромінюють і тому унеможливлюється незаконне перехоплення інформації в ефірі, а також постановка шумів та завад.

Програмне забезпечення – виняткова ліцензійне. При виборі операційних систем (особливо мережевих) перевагу варто віддавати системам сімейства UNIX, як таким, що мають невеликі порівняно з Windows обсяги початкових кодів (текстів програм) і, як наслідок більш стійкі при роботі та при аварійних ситуаціях на техніці. Так, Кабінет міністрів України постановою від 10 вересня 2003 р. № 1433 затверджує «Порядок використання комп'ютерних програм в органах виконавчої влади», який передбачає як використання ліцензійної продукції, так і суворий облік застосованих засобів.

Обов'язково передбачити порядок резервного копіювання, реалізованого,

кримінальні чинники середовища.

Територія(Q41)

Обов'язково має бути контрольована зона для унеможливлення ефективного прихованого спостереження за об'єктом, ведення технічної розвідки та/або раптового нападу. Ця зона має перевищувати охоронювану територію, яка, в свою чергу, на місцевості в багатьох випадках може бути відсутня.

Для якісного спостереження за контрольованою зоною з неї мають бути усунуті всі можливі перешкоди, як це, зокрема, передбачено Статутом гарнізонної та вартової служб ЗС України.

Приміщення(Q42)

Планування сходів, коридорів, горищ, підвалів; розташування вікон, дверей, душників мають бути досліджені на предмет можливого несанкціонованого проникнення всередину, знімання інформації технічними засобами та встановлення технічних розвідувальних засобів. Лінії електроживлення, зв'язку, сигналізації мають бути екрановані для унеможливлення електромагнітного впливу від працюючих засобів обчислювальної техніки. Всі відводи комунікацій за межі об'єкту повинні бути відомими і знаходитися під контролем, те саме стосується розподільчих щитків, коробок тощо. Лінії водогону, опалення, вентиляції і т.д. мають бути екрановані як від електромагнітних, так і від акустичних впливів (від розмов, нарад, переговорів тощо).

В приміщенні для проведення конфіденційних нарад (переговорів) не повинно бути ніяких зайвих електронних та електричних приладів; стіни, а особливо вікна і двері, не повинні межувати з неконтрольованим простором; приміщення має охоронятись, а доступ (в т.ч. для технічних потреб: прибирання, ремонт, підготовка до роботи) – суворо обмежуватись; для захисту від технічних розвідувальних засобів здійснювати, принаймні на час наради, екранування приміщення або випромінювання радіозавад, які за амплітудою та частотою перекриватимуть робочі діапазони можливих розвідувальних засобів (у т.ч. потаємно пронесених агентами з числа учасників наради), а мережа електричного живлення та інших комунікацій повинна бути відв'язана від загальної; крім планових перевірок на предмет наявності розвідувальних засобів, такі перевірки необхідно проводити перед кожною нарадою і після неї.

Режим роботи приміщень(Q43)

На охоронюваній території та в приміщеннях необхідно передбачати різні зони доступу для відвідувачів та персоналу, а персонал, в свою чергу теж повинен мати свої зони відповідальності відповідно до своїх функціональних обов'язків.

Недопущення сторонніх осіб до робочих приміщень. Для цього найкраще поєднувати пильність працюючого в приміщенні персоналу із застосуванням технічних засобів охорони. Щоб не переобтяжувати охорону, необхідно для кожного приміщення визначити «закритий і відкритий» режими залежно від пори дня (тижня) і мінімізувати обсяги таємних робіт шляхом виділення їх найважливішої частини.

Розробка та впровадження типових проектів локальних мереж міськрайлінорганів, галузевих служб (Г)УМВС, структурних підрозділів ОВС	ДІТ, (Г)УМВС	2009	27 840,0	9 280	9 280	9 280	-	-	-
Розробка проекту створення єдиної цифрової відомчої телекомунікаційної мережі МВС України (чотири етапи)	УЗ, ДІТ	2008	3 400, 0	1 700	1 700	-	-	-	-
Організація каналів зв'язку рівнів МВС– (Г)УМВС, (Г)УМВС– відокремлений підрозділ (Г)УМВС, (Г)УМВС– підпорядкований міськралінорган	ДІТ, УЗ, (Г)УМВС	2009	16 320, 0	5 440	5 440	5 440	-	-	-
Поетапна розбудова і модернізація єдиної цифрової відомчої телекомунікаційної мережі передачі даних ОВС Створення центрального та регіональних вузлів управління мережею, контролю підключень, адміністрування, моніторингу	УЗ, ДІТ, (Г)УМВС	2009	39 000, 0	13 000	13 000	13 000	-	-	-
Створення та експлуатація єдиного WEB-порталу МВС України, системи загального доступу, авторизованого доступу до інформаційних ресурсів відомчого використання та КСЗІ при організації такого доступу	ДІТ, (Г)УМВС	2010	19 800,0	4 950	4 950	4 950	4 950	-	-
Створення та запровадження системи електронного документообігу в системі МВС України	ДІТ, ДДЗР (Г)УМВС	2011	31 325,0	925,0	7 600	7 600	7 600	7 600	-
Розробка та впровадження комплексних систем захисту інформації в інформаційних під системах органів внутрішніх справ України.	ЦТЗІ, ДІТ, ГУБОЗ, ДДАІ, ДДГІРФО	2010	111 200						
Обстеження та визначення необхідного класу захисту інформації в інформаційних підсистемах ОВС, які потребують створення КСЗІ.			500	500					

Розробка типових технічних завдань та робочих проектів для створення КСЗІ в однотипних інформаційних системах.			2000	1000	1000				
Створення КСЗІ інформаційно-телекомунікаційних систем, які підключено до Національної системи конфіденційної інформації			2 000	1 000	1 000				
Створення КСЗІ інформаційних систем центрального рівня (МВС України)			4 600	500	500	1200	1200	1200	
Створення КСЗІ інформаційних систем регіонального (обласного ГУСВС, УМВС) рівня.			66 000	7 000	9000	10000	20000	20 000	10000
Створення КСЗІ Єдиної цифрової відомчої телекомунікаційної мережі МВС України.			25 000	5000	10000	10000			
Проведення державних експертиз відповідності КСЗІ.			1 100	100	200	200	200	200	200
Удосконалення законодавчої бази на підставі аналізу світового досвіду функціонування інформаційних систем правоохоронних органів.									
Узагальнення світового досвіду законодавчого та нормативного регулювання інформаційного забезпечення правоохоронної діяльності		2009	300	100	100	100			
Здійснення комплексного аналізу нормативної бази України у соціальній та інформаційній сферах		2009	150	50	50	50			
Підготовка узгодженого нормативного акту, що регулює відносини у сфері інформаційного забезпечення		2009	150	50	50	50			
Розробка проектів нормативних актів МВС України з питань побудови, функціонування та розвитку інформаційних систем органів внутрішніх справ		2010							

можливість організації вибрати оптимальні форми обліку конфіденційних документів. Керівні документи щодо захисту держтаємниць відпрацьовані на державному рівні.

І документи нетаємного діловодства можуть послужити на користь зловмисникам, особливо в разі систематизування і аналізу значної кількості таких документів (За авторитетними джерелами, державні спецслужби до 80% інформації про супротивника отримують через збирання і аналіз різноманітних відкритих видань). Тому обов'язково необхідно вжити заходів щодо впорядкування обліку, поводження, збереження, знищення та пересилки нетаємних документів. Найкраще здійснювати знищення непотрібних документів в кінці кожного робочого дня у встановленому належними чином обладнаному місці. Відповідальним за своєчасне прийняття на облік, збереження створеного (відпрацьованого) документа, а також за знищення непотрібного, має бути кожен виконавець в частині, що його стосується.

На всіх документах і матеріалах (машинних носіях), що містять конфіденційні відомості обов'язково мають бути особливі позначки, так звані грифи. Ці грифи 1) не повинні співпадати із прийнятими в сфері захисту державної таємниці (якщо тільки захищувана інформація не є такою); 2) мають бути зрозумілими лише персоналу і не притягувати увагу сторонніх осіб, випадково потрапивши їм на очі (наприклад, символи, значки, цифрові позначки і т.д); 3) кількість ступенів обмеження доступу (а, отже, і грифів) має бути такою, щоб із будь-якого матеріалу було можливо вичленити найважливіше і надати найвищого грифу. (За даними американських фахівців завелика кількість таємних матеріалів приводить до зниження пильності персоналу.)

В умовах, що постійно змінюються, відповідно змінюються і види та обсяги відомостей, що можуть становити таємницю, а також і персонал, який працює з конфіденційними відомостями. В таких умовах практично неможливо забезпечити кожного виконавця спеціально обладнаним виділеним приміщенням, як це необхідно із документами, що містять державну таємницю. Виходом із становища є «політика чистих столів»: у відсутність працівника на його робочому місці не повинно бути ніяких документів. Втілення в життя такого принципу потребує обладнання кожного робочого місця сейфом, надійною шафою (бажано вогнетривкою) або столом із надійними замками на ящиках. Проте для зберігання найважливіших матеріалів і для роботи з ними необхідно дійсно виділяти особливі обладнані приміщення і дотримуватися особливих заходів безпеки. Необхідно також передбачити планові і раптові перевірки поводження (зберігання, пересилка, обробка) персоналу із документами, матеріалами та машинними носіями інформації, як конфіденційної, так і, умовно кажучи, відкритої.

Територія і приміщення (Q4)

При підборі приміщення найбільше значення має, перш за все, його майбутнє призначення. Відповідно до цього оцінюється його розміщення в загальній будові чи на місцевості, наявність в ньому пожежо- і вибухонебезпечного майна (устаткування, матеріалів та ін.) та соціальні і

передбачити надійний (в плані запобігання загрози інформації), але не громіздкий (щоб не гальмувати загальну справу) механізм ознайомлення цієї особи з потрібними відомостями. Наприклад, керівник, який прийматиме рішення про допуск до нового обсягу відомостей, повинен мати дієвий алгоритм визначення цього обсягу і гранично допустимого терміну допуску до нього, тобто не дати можливості сторонній особі, лише тимчасово допущеній до даного обсягу (виду) інформації, створити цілісну картину стану речей.

Перепускний режим необхідно організовувати так, щоб кожен працівник, відповідно до своєї посади мав чітко визначену сфери свого перебування і спілкування на об'єкті, вийти за які без дозволу він би не мав права. Такі обмеження можна здійснювати за допомогою системи відзнак для персоналу, які (відзнаки) служать перепустками всередині об'єкту і володар певної відзнаки має право спілкуватися лише з тим працівником, який має таку саму відзнаку. Тобто, здійснюється дроблення інформації за рівнями і спеціалізаціями виконавців та обігом її в системі діловодства, що не дозволяє сторонньому отримати цілісну картину.

Проведення переговорів (Q32)

На переговорах часто відбувається значний виток інформації, яка має комерційну цінність. Головні причини тому: невміння правильно рекламувати, неправильне розуміння престижу фахівця і фірми, недооцінка здатності партнерів вести розвідувальну діяльність. Найважливішу роль відіграє саме навчання та виховання персоналу. Кожна допущена до переговорів особа повинна мати чітко окреслені межі компетенції в плані надання партнерові інформації, а також вміти розпізнати спроби партнера в переговорах спонукати до розголосу конфіденційної інформації або завербування на свій бік. Нарешті, кожен працівник, який проводить переговори має усвідомлювати, що серйозне ставлення з боку будь-якого партнеру можливе лише в тому разі, якщо цей партнер переконається у здатності та вмінні організації й її персоналу зберігати довірену таємницю.

Доцільно не виставляти на переговори (симпозіуми, семінари та ін.) тільки одного працівника, їх має бути 2-3 особи; після проведення переговорів кожен із делегатів повинен скласти докладний письмовий звіт.

При веденні таємних нарад або переговорів присутніми мають бути лише ті працівники, кому це необхідно за напрямом діяльності. Тобто, при зміні питання в порядку денному наради (переговорів), всі незадіяні особи мають бути негайно видалені з приміщення. (Може бути поєднане з розмежуванням доступу (Q31))

Організація діловодства (Q33)

Діловодство – організація порядку поводження з носіями інформації (у т.ч. конфіденційної), такими як документи, креслення, схеми, кінофотоматеріали, машинні носії для ЕОМ і т.д. За правильної організації діловодства можливість витоку інформації значно знижується.

В разі наявності на об'єкті конфіденційної документації обов'язково має бути виділене в окремий елемент таємне діловодство. На ринку України існують різноманітні посібники з організації такої діяльності, які надають

Створення системи підготовки та перепідготовки співробітників в умовах поступового розвитку та удосконалення інформаційних технологій									
Розбудова системи підготовки фахівців з питань інформатизації органів внутрішніх справ									
Розробка навчальних програм для факультетів інформатизації ОВС									
Створення та технічне оснащення навчальних закладів органів внутрішніх справ		2012	600	100	100	100	100	100	100
Створення системи перепідготовки та підвищення кваліфікації співробітників ОВС в галузі ведення та використання загальних та функціональних інформаційних систем, а також технічних спеціалістів, розробників програмно-технічного забезпечення									
Створення та технічне оснащення навчальних класів в УМВС областей для проведення занять в системі службової підготовки		2012	600	100	100	100	100	100	100
Впровадження комп'ютеризованих інформаційних систем									
Розробка та впровадження інформаційних систем реєстрації заяв та повідомлень громадян та управління силами і засобами реагування	ГШ, ДІТ	2009	3000	2000	500	500			
Створення інтегрованих інформаційно-аналітичних систем районного, обласного та центрального рівнів	ДІТ, УМВС	2009	600	300	150	150			
Впровадження прикладного програмного забезпечення, що дозволяє здійснювати комплексний аналіз інформації та надавати його в текстовому та графічному вигляді, ведення інформаційно-аналітичної	ДІТ, УМВС	2009	400	200	100	100			

Впровадження новітніх розробок з комплексної ідентифікації об'єктів обліку	ДІТ, УМВС	212	1200	600	200	100	100	100	100
Модернізація програмного забезпечення АДІС "Дакто"	ДІТ	2007	450	450					
Дооснащення спеціалізованого центрального сервера баз даних АДІС "Дакто"	ДІТ	2007	350	350					
Створення обласних автоматизованих банків дактилоскопічної інформації інформаційної служб. Придбання технічних засобів та програмного забезпечення повнофункціональних автоматизованих робочих місць для центрального та регіональних рівнів	ДІТ	2012	42000	7000	7000	7000	7000	7000	7000
ВСЬОГО ПО РОКАХ			1351540	236955	251975	248160	186340	176400	140000

Департамент інформаційних технологій МВС України

1.3.2. Основні інформаційні ресурси органів правопорядку України в Інтернеті

Найменування	Призначення і функціональні можливості
Сайт Міністерства внутрішніх справ України	(www.centrmia.gov.ua)
Сайт Служби безпеки України	(www.sbu.gov.ua)
Сайт Генеральної прокуратури України	(www.gp.gov.ua)
Сайт Державної податкової адміністрації України	(www.visnuk.com.ua)
Сайт Державної митної служби України	(www.castoms.gov.ua)
Сайт Адміністрації Державної прикордонної служби України	(www.pvu.gov.ua)

захисту практично всіх конфіденційних відомостей, крім державних).

Індивідуальний контракт (Q13)

Індивідуальні обов'язки з питань збереження таємниці необхідно включати в контракт (трудовий договір) при зарахуванні працівника на роботу. Таке зобов'язання може бути або окремим пунктом або додатком до контракту. Вважається, що саме другий варіант здійснює потужний психологічний вплив на працівника в плані посилення почуття пильності і відповідальності.

Інструкції (Q14)

Інструкції по захисту конфіденційних відомостей можуть мати форму окремого керівного документа, так і низки документів, охоплюючих тільки певну сферу (робота на ЕОМ, робота з документами, перепускний режим та ін.) На дрібних об'єктах належні рекомендації можуть доводитися до виконавців у формі наказів керівника або вивчення загальновживаних посібників.

В будь-якому разі має бути регламентовано:

– порядок і процедура віднесення матеріалів, документів, виробів до таємних;

– правила доступу до конфіденційних відомостей, наявних на об'єкті;

– обов'язки та обмеження, покладені на виконавця, допущеного до такого роду відомостей (робіт);

– правила поводження (діловодство, облік, зберігання, розмноження, пересилка і т.д) з відповідними матеріалами, документами, виробами;

– порядок допуску представників інших організацій до конфіденційних відомостей та передачі ім таких відомостей;

– відповідальність винних в розголошенні конфіденційних відомостей та (або) порушення встановлених правил.

Персонал(Q2)

Як вже зазначалося, робота з персоналом займає провідне місце в захисті конфіденційних відомостей. Основні принципи мають бути такими:

– перевірка майбутнього працівника перед прийняттям на роботу та оформлення належних зобв'язань в разі прийняття;

– виховання і навчання працівника протягом всього періоду його роботи на даному об'єкті, морально-психологічний вплив на нього, в тому числі застосування матеріального заохочення за сприяння успішному функціонуванню системи безпеки;

– контроль за виконанням вимог безпеки та чітко відлагоджена система адміністративного впливу на порушників і лояльних працівників.

Організація роботи об'єкту (Q3)

Розмежування доступу(Q31)

Повністю позбавити працівника доступу до конфіденційних відомостей неможливо. Проте роботу необхідно організувати так, щоб кожен працівник міг мати доступ тільки до тих відомостей, які необхідні для його службової діяльності.

В разі тимчасового виконання працівником іншої роботи (посади), варто

Q43 – Режим роботи приміщень;
5. Q5 – Технічні засоби;
6.Q6 – Засоби обчислювальної техніки;

Нормативно-правова база(Q1)

Статут (Q11)

Діяльність будь-якої організації має бути юридично оформленою. Оскільки запорукою успішного функціонування будь-якої військової чи цивільної організації є саме здатність захистити свої таємниці, першочерговим завданням є розробка відповідних внутрішніх нормативних документів.

Статут організації визначає як поле її діяльності, так і обов'язки керівників та їх компетенцію. Тому саме в статуті необхідно окремо обумовити право самої організації на захист конфіденційних відомостей, так і обов'язки посадових осіб в плані втілення такого захисту. І саме в статуті мають бути передбачені такі структурні підрозділи, які забезпечуватимуть захист конфіденційних відомостей на об'єкті:

– служба охорони. Фізичний захист території, приміщень, устаткування, майна, керівництва, провідних фахівців, сировини, продукції і т.д. як в неробочий так і в робочий час; забезпечення виконання персоналом та відвідувачами режимних заходів; збирання та подання відповідним посадовим особам фактів, які мають значення для безпеки інформації на фірмі.

– служба збирання інформації (розвідка). Збирання конфіденційної і неконфіденційної інформації про середовище перебування (ринок сировини, збуту), потенційних і фактичних конкурентів (супротивників, зловмисників), а також постачальників, суміжників і посередників; проведення зовнішніх заходів для сприяння функціонування об'єкта.

– служба захисту конфіденційних відомостей (контррозвідка). Контроль за дотриманням режимних заходів; забезпечення безпеки (у т.ч. інформаційної) об'єкту та його устаткування і майна, керівництва та провідних фахівців; виявлення підготовки різних акцій, спрямованих проти об'єкту (персоналу) та протидія цим акціям; випрацювання та втілення заходів щодо захисту каналів зв'язку, інших технічних засобів обробки, зберігання та пересилки інформації, протидія можливій технічній розвідці; контроль за обсановкою в колективі та в навколишньому соціумі в місці розташування об'єкту; збирання та узагальнення фактів, які можуть бути важливими в плані безпеки об'єкта.

Колективний договір(Q12)

Цей документ згідно чинного законодавства України має щорічно укладатися між керівництвом і колективом організації. В ньому необхідно передбачити взаємні зобов'язання сторін з питань захисту таємниці: порядок доступу до конфіденційних відомостей та роботи з ними; можливі обмеження в правах персоналу, зайнятого на відповідних роботах та обов'язкову компенсацію таких обмежень; відповідальність осіб, порушивших встановлений порядок (питання складне через відсутність законодавчого

1.4. Довідкове й інформаційно-аналітичне забезпечення діяльності органів дізнання та досудового слідства.

1.4.1. Автоматизація довідкової інформації.

Провідну роль в системі інформаційного забезпечення правоохоронних органів відіграє інформаційна підсистема забезпечення їх оперативно-розшукової діяльності. Оперативно-розшукова діяльність підтримується використанням інтегрованого банку даних, який складається з відомостей про:

– осіб криміногенних категорій;

– раніше засуджених та осіб, які притягуються до кримінальної відповідальності (в тому числі неповнолітні) за вчинення умисних злочинів;

– осіб, які допускають немедичне вживання наркотичних засобів, психотропних речовин і перебувають на диспансерному обліку;

– психічно хворих, які становлять небезпеку для оточуючих;

– утримувачів притонів;

– осіб, які займаються проституцією;

– осіб, затриманих за бродяжництво;

– інших категорій осіб, які перебувають на обліку в органах внутрішніх справ і схильні до вчинення злочинів;

– викрадені транспортні засоби;

– викрадені мобільні телефони;

– зареєстровану в Дозвільній системі Міністерства внутрішніх справ України мисливську, спортивну, газову зброю громадян і організацій, табельну зброю ОВС, МО, Держприкордонслужби, СБУ, Держмитслужби, Державного департаменту з питань виконання покарань, Управління державної охорони, а також викрадену, вилучену номерну стрілецьку зброю);

– розшук злочинців та держборжників по Україні та країнах СНД, безвісти зниклих;

– викрадені, вилучені предмети антикваріату;

– втрачені паспорти.

Крім того, для інформаційно-аналітичного забезпечення оперативних підрозділів ОВС використовується підсистема «Оріон» обласного та центрального рівнів, яка містить систематизовані, оперативні відомості стосовно осіб та тяжких злочинів, вчинених на території України.

1.4.2. Інтегрований банк даних розшукового призначення «Оріон»

Провідну роль в системі інформаційного забезпечення правоохоронних органів відіграє інформаційна підсистема забезпечення їх оперативно-розшукової діяльності. Оперативно-розшукова діяльність підтримується використанням інтегрованого банку даних, який складається з відомостей про:

– осіб криміногенних категорій;

– раніше засуджених та осіб, які притягуються до кримінальної відповідальності (в тому числі неповнолітні) за вчинення умисних злочинів;

– осіб, які допускають немедичне вживання наркотичних засобів, психотропних речовині перебувають на диспансерному обліку;

– психічно хворих, які становлять небезпеку для оточуючих;
– утримувачів притонів;
– осіб, які займаються проституцією;
– осіб, затриманих за бродяжництво;
– інших категорій осіб, які перебувають на обліку в органах внутрішніх справ і схильні до вчинення злочинів;
– викрадені транспортні засоби;
– викрадені мобільні телефони;
– зареєстровану в Дозвільній системі Міністерства внутрішніх справ України мисливську, спортивну, газову зброю громадян і організацій, табельну зброю ОВС, МО, Держприкордонслужби, СБУ, Держмитслужби, Державного департаменту з питань виконання покарань, Управління державної охорони, а також викрадену, вилучену номерну стрілецьку зброю);
– розшук злочинців та держборжників по Україні та країнах СНД, безвісти зниклих;
– викрадені, вилучені предмети антикваріату;
– втрачені паспорти.

Крім того, для інформаційно-аналітичного забезпечення оперативних підрозділів ОВС використовується підсистема «Оріон» обласного та центрального рівнів, яка містить систематизовані, оперативні відомості стосовно осіб та тяжких злочинів, вчинених на території України.

Наказом МВС від 26.03.02 № 301 визначена поступова комп'ютеризація обласних ОДК. На даний час всі УМВС забезпечують ведення оперативно-довідкового обліку шляхом використання єдиного для всіх структур програмного забезпечення.

Ефективність впровадження інформаційних технологій на сучасному рівні значною мірою залежить від інструменту, що використовується. Таким інструментом є комплекс програмно-технічних, комунікаційних та технологічних засобів. За цільовими програмами розвитку удосконалюється парк комп'ютерної техніки, створено корпоративну мережу до рівня УМВС областей, впроваджуються програмно-технологічні системи, які поєднують розрізнені, часто дублюючі відомчі обліки в єдину інформаційну систему ОВС. На сьогодні відомчою електронною поштою та комп'ютерними системами обробки інформаційних запитів охоплено практично всі органи внутрішніх справ.

та засобів захисту інформації.

Як об'єкт, так і його система інформації є занадто складними для їх одномоментного формалізованого опису. Тому опис і оцінювання необхідно проводити шляхом ітерацій (наближень), поступово відтворюючи істинну картину. При цьому не можна ігнорувати той факт, що спрощення опису складної системи полегшує розрахунки, але зменшує точність самого опису.

На першій ітерації достатньо оцінити системи О та І, вважаючи складаючи їх підмножини параметрів простими елементами. На другій ітерації оцінюються підмножини, а їх показники збираються для узагальненої оцінки.

Функціональний опис

а) Функції об'єкту (загальний випадок):
– прийом вхідних даних (інформації);
– аналіз вхідних даних (інформації);
– узагальнення вхідних даних (інформації);
– обробка вхідних даних (інформації) або прийняття рішень на їх основі;
– -накопичення, зберігання і облік даних (ведення архіву);
– видача вихідної інформації отримувачу або доведення прийнятих рішень виконавцям та керівним органам;
– захист даних, їх носіїв та обладнання для обробки та зберігання даних від агресивних чинників.

б) Функції системи інформації (загальний випадок):
– визначення важливості (грифу таємності, вартості, пріоритетності тощо) для вхідної, вихідної та внутрішньої інформації (проводжуваних робіт) притаманно даному об'єкту;
– визначення носіїв інформації (виконавців робіт, робочого устаткування) на кожному з рівнів важливості та етапів проходження інформації;
– пошук та визначення діючих або потенційних каналів витоку важливих даних та/або нанесення інших збитків інформації;
– розробка заходів протидії агресивним чинникам.

Системний опис вимог, які висуваються до об'єкту та системи інформації

Q – множина власних параметрів системи.
1. Q1 – Нормативно-правова база:
Q11 – Статут;
Q12 – Колективний договір;
Q13 – Індивідуальний контракт;
Q14 – Інструкції.
2. Q2 – Персонал;
3. Q3 – Організація роботи об'єкту:
Q31 – Розмежування доступу;
Q32 – Проведення переговорів;
Q33 – Організація діловодства;
4. Q4 – Територія і приміщення:
Q41 – Територія;
Q42 – Приміщення;

Так, першу категорію присвоюють об’єктам, де обігає інформація з грифом «Особливої важливості» (державна таємниця); другу – з грифом «Цілком таємно» (державна таємниця); третю – з грифом «Таємно» (державна таємниця); а також інформація, яка становить іншу передбачену законом таємницю, розголошення якої завдає шкоду особі, суспільству і державі; четверту – для конфіденційної інформації.

Оскільки важливі для життєдіяльності особи, суспільства або держави відомості можуть не мати обмеження за доступом, то питання стоїть не стільки про закриття цієї інформації від перехоплення чи розголошення, скільки про захист її від втрат або спотворення. Тобто, юридичних підстав застосовувати до категоріювання об’єктів, що містять інформацію такого роду, нема. В цьому разі варто застосовувати альтернативну класифікацію.

Для обґрунтованого захисту інформації на точковоих об’єктах обчислювальної техніки ці об’єкти відповідно до їх призначення, а також обсягів і важливості оброблюваної ними інформації можна поділити на такі основні категорії:

Категорія А. До цієї категорії відносяться такі об’єкти обчислювальної техніки, в яких зберігається та/або обробляється інформація, яка має значення в галузях державного управління, оборони, науки, економіки, фінансів, зв’язку та життєзабезпечення населення в масштабах держави.

Категорія В. До цієї категорії відносяться такі об’єкти обчислювальної техніки, в яких зберігається та/або обробляється інформація, яка має значення в галузях державного управління, оборони, науки, економіки, фінансів, зв’язку та життєзабезпечення населення в масштабах регіону (населеного пункту).

Категорія С. До цієї категорії відносяться такі об’єкти обчислювальної техніки, в яких зберігається та/або обробляється інформація, яка має життєво важливе значення для нормального функціонування підприємства, установи, організації тощо, які не підпадають під перші дві категорії.

Категорія D. До цієї категорії відносяться об’єкти обчислювальної техніки, в яких зберігається та/або обробляється інформація, що є власністю або надбанням окремої фізичної особи і при цьому не підпадає під перші три категорії.

Загальна специфікація на об’єкт та його систему інформації

Одним із варіантів опису об’єкту може бути множина, запропонована в наукових дослідженнях (Структурний опис):

O*={{Q},{b},{c},{d}}.

Тут Q – множина власних параметрів системи, b – активно протидіючі системі ворожі параметри середовища, c – нейтральні або випадкові параметри середовища, d – сприятливі параметри середовища.

Аналогічно паралельно необхідно розглядати систему інформації, що перебуває в обігу на даному об’єкті:

I*={{W},{E},{Z}}.

Тут W – вага оброблюваної інформації (важливість проводжуваних робіт), E – множина всіх можливих загроз для інформації (множина всіх можливих каналів витоку інформації), Z – множина всіх можливих способів

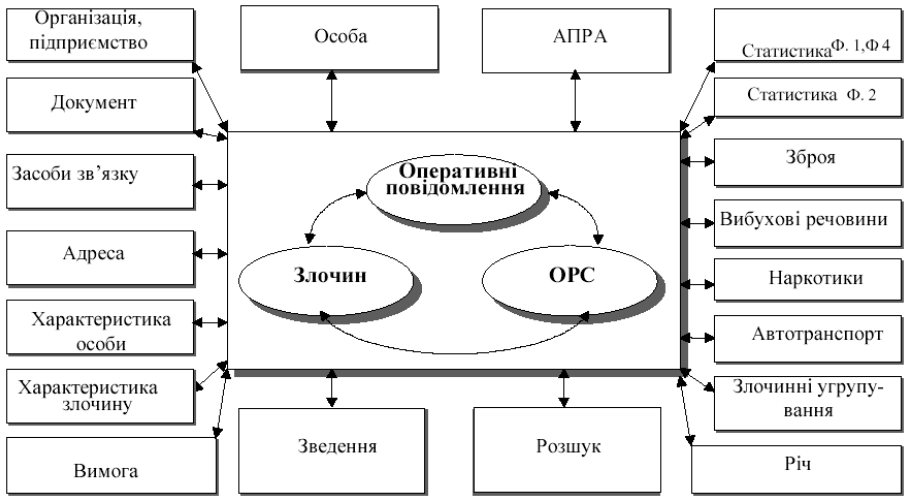
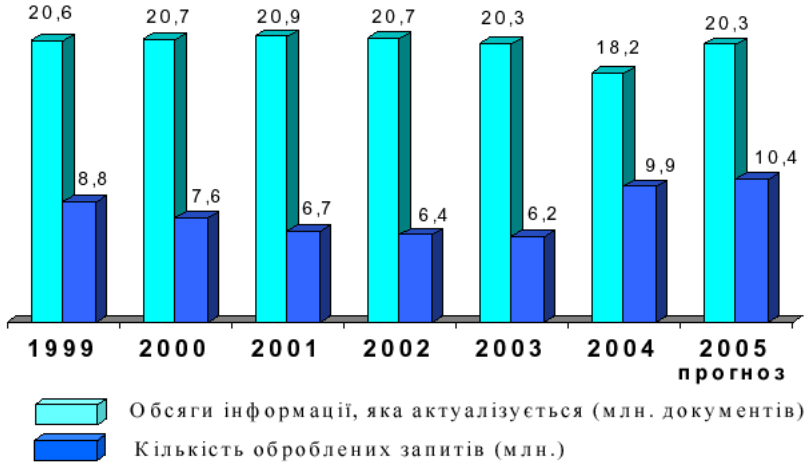


Рис. 1. Структура інтегрованого банку даних «Оріон»

1.4.3 Оперативно-довідкові картотеки

Оперативно-довідкові фонди інформації



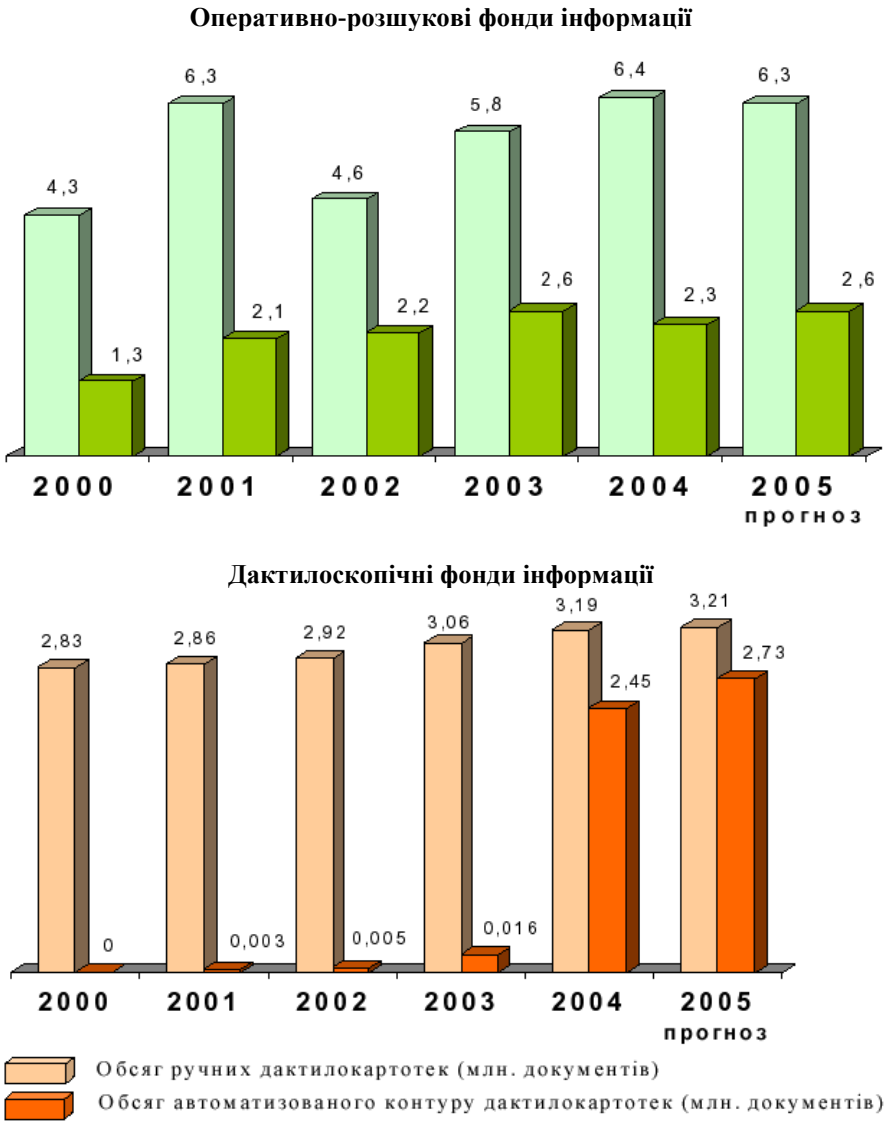


Рис. 3. Динаміка зростання обсягів банків даних та їх використання

1.4.4. Призначення і тенденції розвитку комунікаційно-аналітичного забезпечення діяльності органів досудового слідства

Впровадження сучасних інформаційних технологій сприяє широкому використанню персональної комп'ютерної техніки, поширенню сфери її застосування. В результаті цього виникли певні позитивні тенденції, серед

скоординувати зусилля різнопрофільних фахівців в єдиному цілісному комплексі.

У зв'язку з вище викладеним Під *загрозою для інформації* розумітимемо такий навмисний, ненавмисний або випадковий вплив, діяння чи бездіяльність окремих осіб, організованих угруповань, технічних засобів, природних явищ та інших чинників, наслідком яких може бути викрадення, витік, перехоплення, спотворення або знищення (повне або часткове) інформаційних ресурсів, які знаходяться в обігу на даному об'єкті або створення сприятливих умов для втілення такого.

Докладніше, загрозу для інформації у собі містять:

– цілеспрямовані дії технічних засобів з метою викрадення, перехоплення, спотворення або знищення (повне або часткове) інформаційних ресурсів;

– цілеспрямовані дії окремих осіб або угруповань (з числа персоналу об'єкту або зовнішніх агентів) з тією самою метою (може бути в поєднанні з п. 1);

– нецілеспрямовані дії персоналу чи сторонніх осіб (нестача кваліфікації, низький рівень виховання, недбалість), наслідком чого може бути втрата, перехоплення, викрадення, спотворення або знищення інформації як зацікавленими силами, так і випадковими чинниками або створення сприятливих умов для цього;

– випадкові впливи ЕМ-полів природного та штучного походження, катастрофи, стихійні лиха, коливання напруги та частоти в промисловій мережі, несправності апаратури тощо із перерахованими вище наслідками.

Таким чином даний об'єкт є захищеним в інформаційному відношенні, якщо внаслідок вживаних організаційно-технічних заходів виконується хоча б одна з таких умов:

– цілеспрямований або випадковий вплив на об'єкт, наслідком якого може бути втрата, перехоплення, викрадення, спотворення або знищення інформації як зацікавленими силами, так і випадковими чинниками або створення сприятливих умов для цього, є неможливим apriori ("профілактика");

– всі спроби такого впливу успішно нівелюються з якістю, не гірше заданої, за допомогою організаційно-технічних заходів, які можуть проводитися на рівні окремого об'єкта або на більш вищому рівні ("оборона");

– втрати в ефективності діяльності об'єкту внаслідок успішної реалізації агресивного впливу не перевищують певного окремо встановленого відсотку ("запас міцності").

Класифікація об'єктів обчислювальної техніки та вимоги до їх інформаційної безпеки

На сьогодні в Україні діє Тимчасове положення про категоріювання об'єктів (ТПКО-95), затверджене наказом Державної служби України з питань захисту інформації від 10 липня 1995 року № 35. Відповідно до п. 2.4 даного Положення встановлено чотири категорії об'єктів, для яких правовий режим доступу до інформації, що циркулює в них, регулюється державою.

прогнозировании. – К.: Наукова думка, 1974. – 160 с.

17. *Міщенко В.Б.* Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2002 № 2 (19). – С. 217-223.

18. *Міщенко В.Б.* Стаття на спеціальну тему // Зб. наук. Праць в/ч А0202. – К., 2000. – № 3 (12). – С. 190-196.

19. *Міщенко В.Б.* Захист інформації в сучасних умовах // Удосконалення системи воєнно-наукової інформації ЗС України: Матеріали науково-практичної конференції. м. Київ, 28.5.2002. – К.: в/ч А0202. – С. 64-70.

20. *Міщенко В.Б.* Національна безпека України: сучасні інформаційні технології та можливі джерела небезпеки. / В.Б. Міщенко, О.І. Мотлях, П.Д. Біленчук та ін. // Комп'ютерна злочинність: навчальний посібн. – К.: Атіка, 2002. – С. 45-70.

21. *Міщенко В.Б.* Аналітичний підхід до забезпечення безпеки інформації. // Друга міжнародна конференція "Інформаційні технології в банківській та страховій справі": Збірник наукових праць. – К.: BeeZone, 2003. – С. 62-64.

4.2. Верифікація захищеності систем і банків даних органів дізнання та досудового слідства

Загальновідомо, що будь-який об'єкт обчислювальної техніки складається із приміщення (або сукупності їх) із відповідними архітектурними і технічними характеристиками, допоміжного і забезпечуючого обладнання (сигналізація, лінії електромережі, зв'язку, опалення, вентиляції тощо), загального обладнання (меблі, сховища та інше офісне устаткування), власне комп'ютерного обладнання. В цьому середовищі працює персонал, різний за своїм походженням, особистим рисами, соціальним та службовим статусом, рівнем підготовки, кваліфікації, досвіду роботи. На об'єкт впливають позитивні та негативні чинники; існують також чинники випадкові або нейтральні, тобто такі, дію яких заздалегідь визначити неможливо. До об'єкту для подальшої обробки та зберігання (передачі) потрапляють певні дані, різні за обсягом, важливістю (ступенем секретності) і формою подання; всередині вони накопичуються, трансформуються тощо; на виході отримуємо результати і т.д. Остаточний критерій вартості об'єкту, в даній методиці – захищеність даної системи інформації на даному об'єкті обчислювальної техніки, є функцією від усіх перерахованих вище аргументів. Іншими словами, оцінюючи захищеність до уваги необхідно брати до уваги всі чинники, які можуть сприяти або зашкодити збереженню даних від всіх можливих загроз. Такий підхід до оцінювання захищеності інформації називатимемо об'єктно-орієнтованим.

Забезпечення безпеки інформації на об'єкті обчислювальної техніки є багатогранним завданням, проте два із всіх можливих напрямів є найважливішими: безпека персоналу та захист інформації у власне комп'ютерному представленні. Внаслідок такого розподілу сил постала така практика, коли питанням захисту інформації на об'єктах та у технічних засобах зайняті одні структури, а добором, перевіркою та контролем особового складу – інші. Тому є необхідним науково обґрунтовано

яких:

– загальне підвищення рівня комп'ютерної грамотності працівників міліції;

– розширення переліку комп'ютеризованих інформаційних підсистем;

– поширення «географії» використання сучасних засобів комп'ютерної техніки в діяльності усіх ланок ОВС;

– розповсюдження технологій безпаперової обробки даних;

– створення комп'ютерної мережі обміну інформацією.

Разом з цим, застосування комп'ютерної техніки при несистемному визначенні її місця та ролі в інформаційному забезпеченні подекуди має і негативні наслідки, а саме:

– низький рівень інтеграції інформаційних підсистем;

– дублювання функцій інформаційних підрозділів у галузевих службах;

– нераціональне використання коштів на придбання та розробку програмно-технічних комп'ютеризованих інформаційних підсистем;

– порушення режиму таємності та незахищеність банків даних.

Зазначені реалії сучасного стану інформаційного забезпечення ОВС знижують ефективність інформаційної підтримки боротьби зі злочинністю, що зумовлює подальше відставання у цих питаннях від розвинутих країн світу.

Тим часом збільшення обсягів інформації, що надходить і переробляється, вимагає підвищення ефективності роботи всіх служб МВС за рахунок використання сучасних засобів комп'ютерної техніки, новітніх інформаційних технологій, удосконалення системи інформаційного забезпечення оперативно-службової діяльності органів внутрішніх справ.

Основною метою системної інформатизації органів внутрішніх справ України є всебічна інформаційна підтримка діяльності ОВС у боротьбі зі злочинністю на основі комплексу організаційних, нормативно-правових, технічних, програмних та інших заходів.

Головним призначенням системи інформаційного забезпечення ОВС є:

– забезпечення можливості своєчасного отримання достовірної інформації у повному, систематизованому та зручному в користуванні вигляді працівниками та підрозділами ОВС для розкриття, розслідування, попередження злочинів і розшуку злочинців;

– збір та обробка оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності ОВС;

– забезпечення ефективної інформаційної взаємодії усіх галузевих служб ОВС України, інших правоохоронних органів та державних установ;

– забезпечення надійного захисту інформації від несанкціонованого доступу.

Вирішення питань сучасного інформаційного забезпечення досягається такими шляхами:

– впровадження єдиної політики інформаційного забезпечення;

– створення багатоцільових інформаційних підсистем діяльності ОВС;

– удосконалення організаційно-кадрового забезпечення інформаційних підрозділів;

– інтеграції та систематизації інформаційних підсистем ОВС на всіх рівнях;

– розбудови інформаційної мережі;

– створення умов для ефективного функціонування інформаційних банків даних, забезпечення їх повноти, достовірності, актуальності, безпеки та законності;

– переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою;

– поширення мережі комп'ютеризованих робочих місць користувачів інформаційних підсистем;

– подальшої комп'ютеризації інформаційних фондів;

– впровадження сучасних інформаційних технологій.

Література

1. Системна інформатизація правоохоронної діяльності: Монографія. – Кн. 1. За ред. В. Дурдинця, В. Євдокимова, М. Швеця. – К.: НДЦПІ АПрН України, 2006. – 287 с.

2. Системна інформатизація правоохоронної діяльності / За ред. В. Дурдинця, М. Швеця. – К.: НДЦПІ АПрН України, 2007. – 382 с.

3. Мінченко А.В., Галас О.Р. Правова інформатика. Інформація та інформаційне забезпечення правоохоронних органів: Навчальний посібник. – Арістей, 2003. – 436 с.

На думку авторів, використання запропонованого алгоритму у вигляді програмного комплексу дозволить посадовій особі допомогти обгрунтовано розробити практичні заходи для досягнення потрібного рівня безпеки інформації на конкретному об'єкті.

Література

1. *Соколов А.В., Степанюк О.М*. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург; Арлит, 2002. – 496 с.

2. *Сунь-Цзы* Трактаты о военном искусстве / Сунь-Цзы, У-Цзы; Пер с кит., предисл. и коммент. Н.И. Конрада. – М.:ООО "Издательство АСТ"; СПб.: Terra Fantastica, 2002. – 558 с.

3. *Братко-Кутинський О.* Феномен України. – К.: газета "Вечірній Київ"; Українська академія оригінальних ідей, 1996. – 304 с.

4. *Вертузаєв М.С., Юрченко О.М.* Захисті інформації в комп'ютерах від несанкціонованого доступу: Навчальний посібник / за ред. С.Г. Лаптєва. – К.: В-во Європ. Ун-ту, 2001. – 321 с.

5. *Домарев В.В*. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС"", 2001. – 688 с.

6. *Гнип О.М.* Методи створення електронних каталогів інформаційних ресурсів INTERNET // Удосконалення системи воєнно-наукової інформації Збройних Сил України : Матеріали наук.-практ. конференції, м. Київ, 28 трав. 2002 р. – К.: в/ч А0202, 2002. – С. 70-75.

7. *Міщенко В.Б*. Національна безпека України: сучасні інформаційні технології та можливі джерела безпеки. // Вісник Академії праці та соціальних відносин ФП України. – К.: АПСВ ФПУ. – 1998. – № 1. – С. 61-72.

8. *Міщенко В.Б*. Використання інформаційних технологій для забезпечення прийняття рішення в банківській та страховій установі. // Інформаційні технології в банківській та страховій справі. Збірник наукових праць. – К.: BeeZone, 2002. – С. 22-27.

9. *Давыдов Ю.* Тайна фирмы. – К.: "Фирма Колир-2", 1993. – 176 с.

10. *Ронин Р.* Своя разведка. – Минск: "Харвест", 1997. – С. 6-61.

11. *Доронин А.* Информационный мир в прицеле спецслужб. // Солдат удачи. – 2001. – № 4 [79]. – С. 39-41.

12. *Плэтт В.* Стратегическая разведка. Основные принципы. – М.: Издательский дом "ФОРУМ", 1997. – 376 с.

13. *Біленчук П.Д., Міщенко В.Б, Борисова Л.В.* Аналіз та прогноз стану безпеки об'єкту обчислювальної техніки. // Открытые информационные и компьютерные интегрированные технологии: Сб. научн. трудов. – Х.: НАКУ "ХАИ", 2002. – С. 127-135.

14. *Осинський Л.М.. Міщенко В.Б.* Стаття на спеціальну тему // Науково-технічний збірник в/ч А1906. – К., 2001. – №2. – С. 30-34.

15. *Хохлов Е., Бурыгин Н.* Приоритетные идеи в области управления (Руководство для управляющих, советников высшей администрации и научных работников). – К., "ЛИБРА"-НМПЦА. – 1993. – С. 62-65.

16. *Добров Г.М*. и др. Экспертные оценки в научно-техническом

Таблиця 3

Перший варіант

Найменув модуля	Пріоритет підмнож.	Вага елементу (W)	Можливі значення оцінок модулів				Показник рядку
			"5"	"4"	"3"	"2"	
a_2	1,00	0,13	1	0	0	0	0,63
a_4	3,00	0,38	0	1	0	0	1,50
a_5	4,00	0,50	1	0	0	0	2,50
	0,00	0,00	0	0	0	0	0,00
УЗАГАЛЬНЕНИЙ ПОКАЗНИК МАТРИЦІ							**4,63**

Другий варіант

Найменув модуля	Пріоритет підмнож.	Вага елементу (W)	Можливі значення оцінок модулів				Показник рядку
			"5"	"4"	"3"	"2"	
a_1	1,00	0,14	1	0	0	0	0,71
a^3	2,00	0,29	0	1	0	0	1,14
a_5	4,00	0,57	0	0	1	0	1,71
	0,00	0,00	0	0	0	0	0,00
УЗАГАЛЬНЕНИЙ ПОКАЗНИК МАТРИЦІ							**3,57**

Третій варіант

Найменув модуля	Пріоритет підмнож.	Вага елементу (W)	Можливі значення оцінок модулів				Показник рядку
			"5"	"4"	"3"	"2"	
a_1	1,00	0,10	1	0	0	0	0,50
a_2	1,00	0,10	0	1	0	0	0,40
a_5	4,00	0,40	0	0	1	0	1,20
A_6	4,00	0,40	1	0	0	0	2,00
УЗАГАЛЬНЕНИЙ ПОКАЗНИК МАТРИЦІ							**4,10**

Четвертий варіант

Найменув модуля	Пріоритет підмнож.	Вага елементу (W)	Можливі значення оцінок модулів				Показник рядку
			"5"	"4"	"3"	"2"	
a_1	1,00	0,13	1	0	0	0	0,63
a_4	3,00	0,38	0	1	0	0	1,50
a_5	4,00	0,50	0	1	0	0	2,00
	0,00	0,00	0	0	0	0	0,00
УЗАГАЛЬНЕНИЙ ПОКАЗНИК МАТРИЦІ							**4,13**

В процесі впорядкованого застосування (дослідної експлуатації) даного алгоритму на підставі статистичних або розрахункових даних можна виявити залежність розглянутих вище показників від часу. Така залежність може мати періодичний характер. Тоді можна побудувати кускову (ступінчато-лінійну) функцію, в якій аргумент (час t) є безперервним, а функція (рівень *L*) – кінцевою рахованою величиною, аналогічно кінцевою рахованою множиною буде множина значень можливих відхилень *L*.

Наведений алгоритм не охоплює всі можливі ситуації; він враховує лише найтиповіші з них і носить емпіричний характер. Тому алгоритм потребує подальшого дослідження і, за необхідності, доопрацювання залежно від особливостей часткових випадків.

РОЗДІЛ 2
ЕЛЕКТРОННА КОРПОРАТИВНА МЕРЕЖА ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ: СИСТЕМИ, БАНКИ ДАНИХ

2.1. Правове регулювання та організаційне забезпечення використання електронної корпоративної мережі органами дізнання та досудового слідства.

Нормативно-правову базу системи інформаційного забезпечення ОВС України складають: Конституція України, Кримінальний і Кримінально-процесуальний кодекси України, закони України «Про міліцію», «Про оперативно-розшукову діяльність», «Про державну статистику в Україні», «Про інформацію», «Про дорожній рух», «Про державну таємницю», «Про захист інформації в автоматизованих системах», «Про корупцію», накази МВС, ГУМВС, УМВС, УМВСТ України та інші документи, що регламентують засади використання інформації у боротьбі зі злочинністю.

Розвиток та впровадження новітніх телекомунікаційних, інформаційних технологій ініційовано відповідними указами Президента та Уряду, відомчими нормативними актами:

– Указ Президента від 20.10.2005 № 1497 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій»;

– Указ Президента від 31.01.2006 № 80/2006 «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю».

Наказом МВС України від 02.02.2006 № 112 затверджено Програму створення єдиної цифрової відомчої телекомунікаційної мережі МВС України з метою суттєвого покращання управління органами і підрозділами внутрішніх справ.

У системі МВС України нормативно-правове регулювання передбачає використання трьох груп нормативно-правових документів:

– закони України, укази Президента України, постанови Кабінету Міністрів України;

– накази та розпорядження міністра внутрішніх справ, рішення колегії міністерства;

– накази керівництва ГУМВС, УМВС, УМВСТ. Нормативно-правова база в галузі інформаційної діяльності забезпечує інтеграцію і сумісність баз даних регулює процеси збору, накопичення та передачі інформації в системі ОВС, затверджує правила щодо виконання технологічних процесів роботи з інформаційними банками даних, з визначенням відповідних термінів проходження інформації, вимог до оформлення даних (повнота, достовірність, актуальність тощо), використання інформації у службовій діяльності та персоналізує відповідальність за дотримання цих правил.

Розробка нормативно-правової бази в галузі інформаційного забезпечення проводиться інформаційною службою разом із Головним штабом МВС України із залученням фахівців галузевих служб.

Накази стосовно розробки та впровадження інформаційних підсистем і

технологій розробляються безпосередньо інформаційною службою МВС України. Накази щодо організаційної, кадрової, матеріально-технічної підтримки інформаційного забезпечення можуть розроблятися інформаційними підрозділами та галузевими службами ГУМВС, УМВС, УМВСТ за погодженням з ДІТ МВС України.

Нормативно-правові акти щодо системи інформаційного забезпечення узгоджуються зі змінами у чинному законодавстві, його поточний стан відображається в службово-довідкових обліках системи.

Виконання завдань щодо інформаційного забезпечення та дотримання стратегії його подальшого розвитку покладається на інформаційну службу ОВС, яка складається з інформаційних підрозділів МВС, ГУМВС, УМВС, УМВСТ, міськрайлінорганів та галузевих інформаційних підрозділів, що їй підпорядковуються у питаннях дотримання єдиної інформаційної політики.

Інформаційні підрозділи відповідно до рівня ОВС (центральний, другий, третій, галузевий) у своєму складі передбачають відділи (відділення, групи, фахівців) за усіма напрямами роботи інформаційного забезпечення, а саме:

– оперативної інформації;

– оперативно-розшукової роботи з цілодобовим функціонуванням чергових інформаційних груп;

– оперативно-довідкової інформації;

– технічного обслуговування комп'ютерних інформаційних підсистем та засобів оперативної поліграфії;

– супроводу та адміністрування інформаційних підсистем та банків даних;

– супроводу комп'ютерних мереж та телекомунікаційних систем;

– впровадження нових інформаційних технологій;

– збору та обробки статистичної інформації;

– архівної роботи;

– матеріально-технічного забезпечення.

Ці підрозділи комплектуються фахівцями у необхідній кількості, яка визначається окремо для кожного органу відповідно до стану злочинності та загальної чисельності працівників ОВС. Інформаційна служба на відповідних рівнях представлена такими підрозділами:

– на рівні МВС України – Департамент інформаційних технологій;

– на рівні ГУМВС, УМВС – управління (відділи) оперативної інформації;

– на рівні УМВСТ – відділення (групи) оперативної інформації міськрайлінорганів;

– у галузевих службах – відділи та відділення (групи) обробки інформації.

Однією з основних умов розвитку інформаційного забезпечення та підвищення його ефективності в діяльності ОВС є зміцнення інформаційних підрозділів у міськрайлінорганах. Оптимальна чисельність цих підрозділів становить не менше 3-5 фахівців залежно від напрямів роботи. Призначення керівників інформаційних підрозділів узгоджується з інформаційною службою відповідного рівня.

Організаційні заходи передбачають створення відповідних умов для забезпечення функціонування цих підрозділів – надання необхідних приміщень, обладнаних відповідною комп'ютерною та оргтехнікою,

ООТ в даних умовах інформації певної важливості в певних обсягах;

2) відпрацьовувати пропозиції і плани з покращення захищеності ООТ або зниження (профілактики) зовнішніх загроз.

З огляду на значне коло охоплюваних при оцінці елементів і чинників, в процесі практичного застосування даного алгоритму може виникнути потреба в накладенні обмежень та допущень на окремі досліджувані елементи для більш змістовного дослідження тих елементів, які становлять найбільший інтерес.

Застосуємо наведений алгоритм для вибору найкращого із чотирьох отриманих на попередньому етапі варіантів комплектації

Приклад 4.

На попередньому етапі ми отримали такі можливі варіанти комплектування системи захисту: $h_1 = \{a_2, a_4, a_5\}$; $h_2 = \{ a_1, a_3, a_5\}$; $h_3 = \{ a_3, a_4, a_5\}$; $h_4 = \{ a_1, a_2, a_5, a_6\}$.

Потрібно, використовуючи формули (13-22), визначити найкращий з них.

РІШЕННЯ.

Нехай за результатами попередніх експертиз, встановлені такі рівні пріоритетності для вибраних модулів:

a_1, a_2 – перший (найнижчий); a_3 – другий; a_4 – третій; a_5, a_6 – четвертий (найвищий). За своїми показниками кожен із них отримав свою оцінку за бальною шкалою, обчислену за формулами (13-16). Припустимо, що в результаті всіх дій отримано такі вторинні матриці інцидентності, які ми обробимо у середовищі Excel, запрограмувавши формули (17-22) (Таблиця 3) та побудувавши порівняльну діаграму.

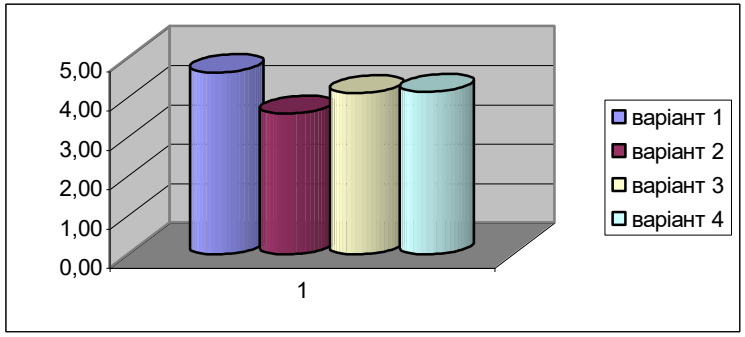


Рис. 8. Ілюстрація вибору найкращого варіанту.

Як було зазначено вище, кожен із запропонованих чотирьох варіантів задовольняє всім накладеним раніше обмеженням.

Зазначимо, що на практиці доцільно наперед визначити межі допустимих (можливих) значень коефіцієнту L в аналізованій ситуації (в конкретних умовах), тобто мінімальне і максимальне значення цього коефіцієнту, що покращуватиме наочність оцінки.

отже і рівень пріоритетності буде однаковий (див. Таблицю 2).

Таблиця 2

Елементи, що оцінюються	Рівень пріорітетності	"5"	"4"	"3"	"2"
Елем. 1	k-й (найвищий)	0	1	0	0
Елем. 2		1	0	0	0
...	….	..	..	..	..
Елем. *i*-1	j-й	1	0	0	0
Елем. *i*	j-й	0	0	1	0
Елем. *i*+1	j-й	0	0	1	0
.....	….	..	..	..	..
Елем. *m-1*	1-й	0	0	0	1
Елем. *m*	(найнижчий)	0	0	0	1

Наприклад, нехай визначено k рівнів пріоритетності . Тоді "вага" *i*-го елементу *Wi* дорівнюватиме:

$$W_i = \gamma\beta_{ij}, i = \overline{1,m}, j = \overline{1,k}, \quad (19)$$

де γ- коефіцієнт пропорційності, *βij*- рівень пріоритетності *i*-го елементу.

Враховуючи умову (7), маємо:

$$\sum_{i=1}^{m} \gamma\beta_{ij} = \gamma \sum_{i=1}^{m} \beta_{ij} = 1, j = \overline{1,k} \quad . (20)$$

Звідси, коефіцієнт пропорційності γ□ для досліджуваної матриці дорівнюватиме:

$$\gamma = \frac{1}{\sum_{i=1}^{m} \beta_{ij}}, j = \overline{1,k} \quad (21)$$

Для отримання показника, який однозначно характеризуватиме досліджувану матрицю, застосуємо формулу:

$$L = \sum_{i=1}^{m} \sum_{j=1}^{n} WiB_j^* a_{ij}, \quad (22)$$

де *L* – шуканий показник досліджуваної матриці, *m* – число елементів, які піддавалися оцінці, *n* – число можливих значень оцінок, *Wi* – «вага» *i*-го елементу, B_j^* – значення оцінки за бальною шкалою, a_{ij} – відповідний елемент матриці інцидентності, який, як вже було сказано, приймає значення 0 або 1.

Ми отримали показник ЧП4. Він рівний *L* і характеризуватиме (притаманно до заданого наперед рівня рентабельності):

1) *для досліджуваного об'єкту:* стійкість системи захисту об'єкту в комплексі до різних видів загроз.

2) *для чинників навколишнього середовища:* можливість відвернення загрози для ООТ ззовні об'єкту або протистояння цій загрозі.

На підставі отриманих чисельних значень (співставлення оцінки стійкості власних елементів ООТ і оцінки сприятливості середовища) є можливим (знову ж таки, виходячи з важливості даних, обмежень по вартості та критичним рівням втрат):

1) робити висновок про можливість чи неможливість обробки на даному

забезпечення витратними матеріалами тощо. Враховуючи вимоги до забезпечення захисту інформаційних фондів ОВС, особливу увагу необхідно приділити обладнанню у першу чергу таких приміщень: серверних залів комп'ютерного комплексу, оперативно-довідкових фондів, архівів, окремих оперативних груп та секретаріатів.

Виходячи з вимог інформаційного забезпечення в межах єдиної системи, всі інформаційні підрозділи підпорядковуються ДІТ МВС України. Адміністративно галузеві інформаційні підрозділи підпорядковуються безпосередньому керівництву.

Призначення керівників інформаційних підрозділів у галузевих службах МВС України погоджується з Департаментом інформаційних технологій МВС України, а в ГУМВС, УМВС, УМВСТ – відповідно з управлінням (відділом) оперативної інформації.

У галузевих підрозділах організаційно-кадрова структура визначається специфікою завдань, що виконуються, та узгоджується з ДІТ МВС України.

Ефективне використання можливостей інформаційних підсистем потребує організації відповідного рівня підготовки та перепідготовки кадрів системи ОВС, підвищення рівня спеціальної комп'ютерної підготовки працівників органів внутрішніх справ у вищих навчальних закладах МВС України.

Навчання та перепідготовка керівного складу передбачають:

– вивчення законодавства України та узгодження з ним вимог до функціонування інформаційних підсистем;

– аналіз тенденцій розвитку суспільства та визначення інформаційних фондів, комп'ютеризація яких доцільна для удосконалення інформаційного забезпечення ОВС;

– вивчення досвіду правоохоронних органів інших держав;

– підготовку керівників до самостійної роботи з комп'ютерними робочими місцями інформаційних підсистем.

Навчання фахівців у галузі інформаційного забезпечення має відбуватися за такими напрямами:

– супроводження операційних систем та систем керування базами даних (СКБД);

– технологія розробки програмних засобів інформаційних підсистем;

– адаптація та використання компонентів інформаційних підсистем;

– забезпечення функціонування телекомунікаційних засобів та електронної пошти;

– технічне обслуговування електронного обладнання;

– забезпечення адміністрування та захисту інформації.

Підготовка працівників ОВС (користувачів інформаційних підсистем) повинна забезпечити рівень їх кваліфікації, достатній для:

– виконання операцій, необхідних для інформаційної підтримки своєї службової діяльності;

– обізнаності з основними правилами поводження з комп'ютерним та комунікаційним обладнанням;

– виконання вимог щодо техніки безпеки та захисту інформації.

Навчання та перепідготовка кадрів може здійснюватися шляхом:

– обміну досвідом за принципом «вчитель – учень» на робочому місці;

– навчання на курсах, стажування в спеціальних закладах, участь у відповідних конференціях, семінарах, нарадах;

– використання навчальних пакетів програм, літератури, документації, посібників, інструкцій, довідників тощо;

– підготовки фахівців інформаційної служби у вищих навчальних закладах системи МВС України.

Враховуючи бурхливий розвиток інформаційних технологій, треба зазначити, що налагодження механізму підтримки професійного рівня персоналу, пов'язаного із забезпеченням функціонування інформаційних підсистем ОВС, є передумовою розвитку та удосконалення, якісного і своєчасного надання інформації, забезпечення її захисту та надійної роботи. Разом з цим, знання та навички щодо використання інформаційних підсистем співробітниками ОВС є складовою частиною загальних вимог до їх професійного та службового зростання.

2.2. Загальна характеристика електронної корпоративної мережі МВС України: поняття, структура

Корпоративна інформаційна мережа ОВС України – це комплекс програмних, технічних та організаційних засобів для забезпечення оперативного обміну даними оперативно-розшукового, довідкового та організаційно-управлінського змісту між підрозділами ОВС.

Основою корпоративної інформаційної мережі ОВС є комп'ютерна мережа, яка забезпечує поєднання всіх програмно-технічних комплексів інформаційних підсистем на всіх рівнях. Інформаційна мережа створюється в інтересах усіх галузевих служб ОВС і надає можливість оперативної інформаційної взаємодії як у системі ОВС, так і з правоохоронними органами, державними установами, міністерствами та відомствами України, а також з правоохоронними органами інших держав.

Комплекс технічних засобів системи інформаційного забезпечення ОВС передбачає підтримку всіх функцій сучасної архітектури «клієнт-сервер» та «термінал-сервер» з урахуванням специфіки завдань, що виконуються на кожному ієрархічному рівні системи. Усі рівні комплектуються серверами баз даних, комп'ютерними робочими місцями користувачів інформаційних підсистем.

Корпоративна інформаційна мережа ОВС України призначена для інформаційного забезпечення галузевих служб міністерства, підрозділів органів внутрішніх справ України.

У комплексі будівель центрального апарату МВС України створена структурована гетерогенна комп'ютерна мережа, інформаційною магістраллю якої є оптико-волоконне кільце, до якого через комутаційне обладнання підключені локальні мережі галузевих служб МВС України.

При побудові комп'ютерної мережі МВС України застосовано сучасне комутаційне обладнання, яке дозволяє об'єднувати інформаційні підсистеми.

Система зв'язку між інформаційними мережами ОВС України та ГУ-УМВС в областях передбачає створення корпоративної мережі передачі даних на базі некомутованих «виділених» 4-провідних каналів зв'язку з

Тоді ефективність захисту становитиме:

$Э_{зах} = P_{ст} * Z_{сер}$

Звідси, значення абсолютної оцінки стійкості елементу:

$$B = \frac{Эзах}{Свст}$$

Для спрощення подальших обчислень пропонуємо наперед встановити рівні рентабельності захисних засобів і відповідно до них поставити у відповідність абсолютним значенням, отриманим за формулою (4), оцінку за бальною шкалою (рангову оцінку). Наприклад, якщо $B<1$ – оцінка "2"; $B=1$ – оцінка "3"; $B>1$ – оцінка "4"; $B>>1$ – оцінка "5". Позначимо рангову оцінку через B^*.

Утворимо *вторинну матрицю інцидентності*: (0,1)-матрицю розмірності mxn (в загальному випадку m не рівне n) для кожної із множин h_1-h_4: розставивши по колонкам можливі значення оцінок в порядку спадання зліва направо (n), а по рядкам – елементи множин h_1-h_4 (m) в порядку зменшення їх важливості (пріоритетності).

За означенням, елемент матриці прийматиме значення:

$$a_{ij} = \begin{cases} 1, \text{якщо } i\text{-й елемент досліджуваної множини} \\ \text{отримує } j\text{-ту оцінку;} \\ 0, \text{в іншому випадку.} \end{cases} \quad (17)$$

Наприклад, при чотирьохбальній системі оцінок матриця матиме вигляд, показаний в Таблиці 1.

Зрозуміло, що в кожному рядку може бути лише одна одиниця (кожен елемент отримує лише одну оцінку), тоді як на колонки це правило не поширюється (дану оцінку може не отримати жоден з елементів, або її отримали всі елементи).

Кожен з елементів досліджуваної множини, який потрапляє до матриці інцидентності, отримує "вагу" W відповідно до своєї значимості в загальній системі. При цьому необхідно витримати умову:

$$\sum_{i=1}^{m} Wi = 1 \quad , (18)$$

де, як було вже сказано, m – число прийнятих до оцінювання параметрів.

(Примітка. Шкалу пріоритетності (порядок слідування) конкретних елементів в матриці інцидентності, створеній для тієї чи іншої множини потрібно визначати в кожному конкретному випадку. Пріоритети (порядок слідування) елементів і оцінки кожному елементу множини виставляють легітимні фахівці-експерти, виходячи з чинних нормативних вимог. Зараз це питання ми залишимо поза увагою Докладніше про проведення експертних оцінок див. [16].)

У загальному випадку, в досліджуваній системі кількість рівнів пріоритетності може не співпадати з кількістю її елементів ($i<>j$), інакше кажучи, декілька (або всі) елементи можуть мати однакову важливість, а

$(a_1 \vee a_4)(a_2 \vee a_3 \vee a_5)(a_3 \vee a_4 \vee a_6)(a_5)(a_2 \vee a_3)$

Розкриваючи дужки в цьому виразі та використовуючи основні співвідношення алгебри логіки у остаточному вигляді отримаємо:

$a_2a_4a_5 \vee a_1a_3a_5 \vee a_3a_4a_5 \vee a_1a_2a_5a_6$

Кожна кон'юнкція цього виразу визначає можливий варіант комплексування програмних модулів служб захисту, яке забезпечить задоволення потрібних послуг з боку підсистеми захисту, а саме:

h_1 = { a2, a4, a5}; h_2 = { a1, a3, a5};

h_3 = { a3, a4, a5}; h_4 = { a1 ,a2, a5 ,a6}.

Це набір ЧПЗ. Далі необхідно провести аналіз цих варіантів для визначення їх входження в область допустимих рішень і вибору найоптимальнішого з їх числа. Знаходження зазначеного варіанту дозволить відповідальним посадовим особам прийняти оптимальне рішення з розгортання захисних систем для збереження інформації, яка циркулює в засобах обчислювальної техніки.

Етап 4 Оцінка системи захисту

Кожному із елементів множин h_1-h_4 залежно від роду виконуваних ним функцій і його важливості на підставі керівних нормативних документів (накази, державні і галузеві стандарти, технічні умови, настанови, інструкції тощо) або експертних оцінок висуваються певні вимоги, які на практиці можуть мати чисельні (кількісні) значення. Цим значенням, у свою чергу, можна ставити у відповідність імовірність однієї із нижчеперелічених подій:

– подолання/неподолання власних захисних систем об'єкту;

– виникнення/невиникнення загрози для конфіденційності, цілісності та доступності оброблюваної інформації з боку персоналу об'єкту;

– виникнення/невиникнення ззовні загрозливих ситуацій (соціальних, природних, техногенних) та впливу їх тим чи іншим чином на оброблювану інформацію.

Наступний крок – отримані оцінки об'єднати і отримати узагальнене значення.

Найдоцільніше кожен з елементів оцінювати за такими показниками, аналогічно 2-му етапу:

– вартість встановлення захисного засобу або усунення потенційного джерела загрози $C_{вст}$;

– імовірність відмови захисного засобу або виникнення неконтрольованої небезпечної ситуації $P_{відм}$ зовні або всередині об'єкту;

– нанесені збитки в разі успішної реалізації загрози Z_{max}.,тобто в тому разі, коли $P_{відм} = 1$.

Як було вже показано, середнє значення втрат від загрози даного виду в такому разі дорівнюватиме

$Z_{сер} = Z_{max} * P_{відм}$.

Стійкість захисного засобу як імовірність його неподолання або ймовірність невиникнення неконтрольованої небезпечної ситуації дорівнюватиме:

$P_{ст} = 1-P_{відм}$.

інтеграцією послуг (дані, графічна інформація, мультимедіа та голос). *Інтеграція послуг* – це можливість мережі передавання даних надавати користувачу різноманітні види послуг незалежно від того, на базі якого протоколу працює сама мережа.

Мережа характеризується можливістю використання територіальних каналів зв'язку найрізноманітнішої природи і при обмеженій кількості каналів забезпечує задоволення потреб користувачів. Однак ця мережа потребує високої пропускної спроможності каналів зв'язку та спеціалізованого обладнання, яке підтримує різноманітні базові транспортні протоколи.

Підсистема обміну інформацією є складовою частиною мережевого сервісу корпоративної інформаційної мережі ОВС України і базується на діючій системі електронної пошти ОВС України (police.mail.ua).

В корпоративній інформаційній мережі МВС-ГУМВС України користувачам відповідно до їх повноважень Департаментом інформаційних технологій надається право доступу до центральних інформаційних підсистем, до локальних інформаційних мереж підрозділів МВС України та інформаційних підсистем ГУ-УМВС областей.

2.3. Принципи та етапи формування і комплексного використання електронної корпоративної мережі МВС України в діяльності органів досудового слідства.

Корпоративна інформаційна мережа будується за територіальним принципом та має трирівневу структуру:

– центральна інформаційна мережа;

– регіональні інформаційні мережі;

– територіальні інформаційні мережі.

Регіональні інформаційні мережі забезпечують інформаційну взаємодію між галузевими службами ГУМВС, УМВС, УМВСТ, територіальними і центральними інформаційними мережами ОВС та іншими правоохоронними органами.

Територіальні інформаційні мережі є складовими регіональних мереж і забезпечують інформаційну взаємодію між підрозділами міськрайлінорганів.

В окремих випадках створюються галузеві інформаційні мережі, що входять до складу інформаційної мережі ОВС і забезпечують інформаційний обмін відповідно до Концепції розвитку інформаційного забезпечення та з дотриманням протоколів обміну інформацією, що визначаються Департаментом інформаційних технологій (ДІТ) МВС України.

При побудові комп'ютерних мереж використовуються новітні інформаційні технології із застосуванням оптиковолоконних, провідних та радіоканалів передачі даних, сертифікованих програмно-апаратних засобів, які забезпечують надійність, достовірність та конфіденційність обміну інформацією.

Управління інформаційною мережею здійснюється центральною та регіональними системами адміністрування, які підпорядковані інформаційним підрозділам МВС, ГУМВС, УМВС, УМВСТ відповідно.

Адміністрування інформаційної мережі обумовлює:

– реєстрацію та авторизацію користувачів;

– ведення журналів доступу;

– забезпечення безпеки інформаційного обміну.

Інформаційна мережа повинна забезпечувати передачу текстової, графічної, аудіо-та відеоінформації.

Протоколи та формати інформаційного обміну ґрунтуються на світових стандартах у галузі телекомунікацій, визначаються ДІТ МВС України та регламентуються відомчими нормативними актами.

Враховуючи необхідність оперативності та безпеки інформаційного обміну, програмні і технічні засоби, що застосовуються в інформаційних мережах ОВС, сертифікуються та інсталюються централізовано через ДІТ та управління, відділи оперативної інформації ГУМВС, УМВС.

Інформаційні мережі всіх рівнів – це відомчі мережі закритого типу, що не допускають підключення до інформаційних мереж загального користування.

Розвиток корпоративної інформаційної мережі ОВС характеризується такими етапами.

Перший етап – це використання діючої комп'ютерної мережі на основі електронної пошти МВС України. На цьому етапі забезпечується розвиток системи електронної пошти всіх рівнів на основі комутованих каналів зв'язку, впроваджується доступ користувачів до інформаційних підсистем оперативно-розшукового призначення.

Другий етап – розвиток діючої електронної пошти на основі використання виділених каналів зв'язку між центральною та регіональними інформаційними мережами, застосування технології INTRANET. Впроваджується зв'язок з банками даних у режимі Off-Line та On-Line, забезпечується адміністрування на центральному та регіональному рівнях.

Третій етап – побудова корпоративної інформаційної мережі ОВС з обміном інформацією між територіальним, регіональним та центральним рівнями і забезпечення формування банків даних верхнього рівня з використанням телекомунікаційних технологій. На цьому етапі широко застосовуються швидкодіючі канали зв'язку між регіональними та центральним рівнями, основою яких мають бути супутникові та цифрові канали, реалізується доступ до комп'ютерної мережі з рухомих об'єктів та стаціонарних постів міліції.

Література

1. *Бірюков В.В.* Научные и практические основы использования компьютерных технологий для фиксации криминалистически значимой информации. – Луганск, 2002.
2. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. // Відомості Верховної Ради України. – 1998. – № 27-28. Ст. 181.
3. Програма інформатизації органів внутрішніх справ України на 2000-2010 роки. – К., Управління оперативної інформації МВС України, 1999.
4. Саницький *В.А., Карацюба А.М., Святобог В.В. та ін.* Система інформаційного забезпечення ОВС України: Навчально-практичний посібник / За ред. Л.В. Бородича. – К., 2000. – - 144 с: іл., табл.
5. 1С: Бухгалтерия. Версія 7.7. Руководство пользователя. – М., Фирма "1С", 2001.

залишившихся рядків a_n. Рядок an є лишнім, якщо $q_{nk} = 0$ для всіх залишившихся стовпців z_k;

4. Якщо матриця Q, отримана в п. 3, виявиться порожньою, то в якості множини H можливих варіантів рішення зафіксувати підмножину B базових модулів і перейти до п. 8. Якщо ж матриця Q не порожня, то перейти до пункту 5;

5. Знайти варіанти мінімальних покрить матриці інцидентності Q, отриманої в п. 3, для чого:

– побудувати диз'юнктивний терм по змінним $a_n \in A$, які відповідають рядкам у матриці Q. Для стовпця z_k, який залишився, диз'юнктивний терм утворюють тільки ті змінні an, для яких $q_{nk} = 1$;

– записати булевий вираз у вигляді кон'юнкції диз'юнктивних термів, отриманих вище;

– розкрити дужки і спростити отриманий булевий вираз, подавши кінцевий результат у вигляді диз'юнктивної нормальної форми;

6. Сформувати множину H можливих варіантів рішення. Для цього у відповідності із кожним кон'юнктивним термом отриманого кінцевого булевого виразу, отриманого у п. 5, створити окрему підмножину модулів захисту і доповнити його елементами базової підмножини B;

7. Перевірити виконання обмежувальних умов пунктів в) і г) із вище сформульованих вимог до рішення. В підмножині $H=\{h_i\}$ залишити варіанти, які задовольняють згадані умови;

8. Якщо множина H не порожня, то вона визначає область допустимих рішень, яка підлягає подальшому аналізу для вибору оптимального рішення.

Розглянемо приклад, який ілюструє процедуру виконання п. 6 наведеного алгоритму.

Приклад 3.

Нехай після виконання п. 4. отримана така матриця інцидентності

Q	z_1	z_2	z_3	z_4	z_5
a_1	1	0	0	0	0
a_2	0	1	0	0	1
a_3	0	1	1	0	1
a_4	1	0	1	0	0
a_5	0	1	0	1	0
a_6	0	0	1	0	0

Із матриці слідує, що потрібна послуга z_1 може бути забезпечена модулями a_1 або a_4, тобто один із цих модулів обов'язково повинен входити у склад формуємої захисної підсистеми. Ця умова подається диз'юнктивним термом $a_1 \vee a_4$, вона буде істинною, якщо хоча б один із рядків, a_1 або a_4, покриє стовпець z_1. Аналогічно, умова забезпечення послуги z_2 подається диз'юнктивним термом $a_2 \vee a_3 \vee a_5$. Покриття всіх стовпців матриці інцидентності подається таким булевим виразом:

Знайти підмножину hi={ai1, ai2,…,air,…,aiR } множини A, тобто $h_i \subseteq A$, яка екстремізує деякі критеріальні співвідношення і задовольняє умовам

$$Z \le G(h_i) = \bigcup_{a_{ir} \in h_i} G_i(a_{ir})$$

а) – повнота реалізації всіх потрібних послуг для захисту системи S;

б) $Z \not\subset G(h_i \setminus a_{ir})$ для будь-якого $a_{ir} \in h_i$ – тупиковість обраної підмножини h_i;

в) $\sum_{r=1}^{R} V_{(i,r)m} \le U_m$ для всіх $m = \overline{(1,M)}$;

г) $\sum_{r=1}^{R} C_{(i,r)} \le C_{зад}$, де пара (i,r) визначає індекс $n \in \{1,2,...,N\}$ модуля $a_{i,r} \in h_i$, а $C_{зад}$ – розумні обмеження за вартістю.

РІШЕННЯ.

Формуємо *первинну матрицю інцидентності* $Q = \|q_{nk}\|$, в котрій кожному рядку взаємно однозначно відповідає модуль an, ($n = \overline{1,N}$) захисту із множини A, а кожному стовпцю вид послуги z_k, ($k = \overline{1,K}$), який потрібний системі S для організації її захисту, і

$$q_{nk} = \begin{cases} 1, \text{якщо } z_k \in G_n, \\ 0 \text{ - в іншому випадку.} \end{cases}$$

По матриці інцидентності $Q = \|q_{nk}\|$ відшукуємо всі варіанти мінімального покриття сукупностями рядків (захисних модулів) всіх стовпців (захисних послуг, які використовує система S). Стовпець zk ($k = \overline{1,K}$), вважаємо покритим, якщо в обраній сукупності hi рядків air є хоч один елемент $a_j \in h_i$ такий, що $q_{jk}=1$. Мінімальність покриття інтерпретується як відсутність лишнього рядка у вибраній сукупності (умова б) у вимогах до підмножини h_i).

Наведемо алгоритм знаходження множини мінімальних покрить матриці інцидентності, базований на булевій алгебрі [19].

АЛГОРИТМ.

1. Сформувати матрицю інцидентності $Q = \|q_{nk}\|$;

2. Визначити підмножину B базових модулів a_n, $n = \overline{(1,N)}$. Модуль a_n є базовим, якщо існує стовпець z_j такий, що $q_{nj} = 1$ і $q_{ij} = 0$ для всіх i = 1,2,….,n-1,n+1,…,N. Модулі $a_n \in B$ повинні входити в усі варіанти мінімальних покрить, тому відповідні рядки можна викреслити із матриці інцидентності;

3. Зменшити розмірність матриці Q, отриманої у п. 2, шляхом послідовного викреслення лишніх стовпців, а потім – лишніх рядків. Стовпець z_k є лишнім, якщо існує стовпець z_j такий, що $q_{nk} = q_{nj}$ для всіх

РОЗДІЛ 3
ІНФОРМАЦІЙНО-АНАЛІТИЧНІ СИСТЕМИ І ПІДСИСТЕМИ ЕЛЕКТРОННОЇ КОРПОРАТИВНОЇ МЕРЕЖІ МВС УКРАЇНИ

3.1. Структурна побудова інформаційно-аналітичних загальновідомчих та галузевих систем і підсистем органів внутрішніх справ: вимоги, рівні, складові

Система інформаційного забезпечення правоохоронних органів (Рис. 1) утворюється сукупністю інформаційних підсистем, побудованих з урахуванням та дотриманням таких вимог:

– наявності нормативно-правової бази;

– організаційно-кадрового забезпечення інформаційних підрозділів;

– організації підготовки та перепідготовки кадрів;

– наявності відповідних технічних, програмних та телекомунікаційних технологій;

– матеріально-технічного та фінансового забезпечення.

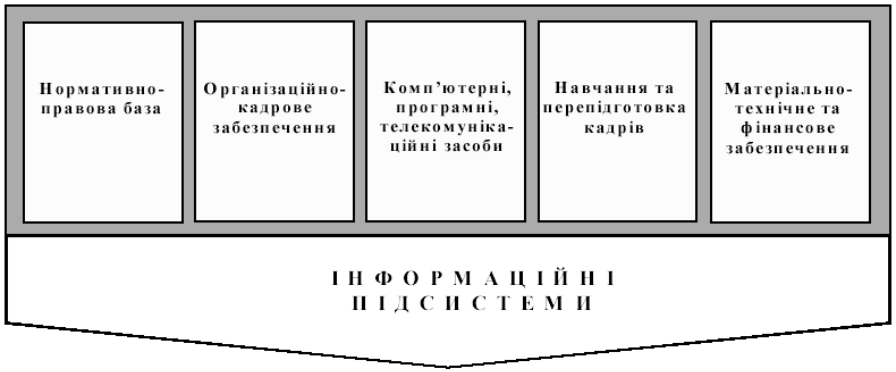


Рис. 1. Складові частини системи інформаційного забезпечення

Інформаційні підсистеми як основні складові системи інформаційного забезпечення призначені для збору, накопичення, зберігання та обробки інформації певних напрямів діяльності правоохоронних органів, орієнтовані на загальне використання галузевими службами мають загальновідомчий зміст і належать до міжвідомчих інформаційних підсистем.

Деякі спеціалізовані фонди інформації, що використовуються в діяльності підрозділів окремих галузей, належать до галузевих інформаційних підсистем. Структурна побудова інформаційних підсистем поєднує принципи територіально розподіленої та централізованої топології і організована у вигляді трирівневої ієрархічної моделі.

Належність інформаційної підсистеми до певного рівня визначається принципами територіальності, специфіки використання а також обсягом інформації, яка обробляється.

Перший рівень – центральний, інтегрує інформаційні підсистеми ОВС

міжвідомчого значення та галузевих служб МВС.

Другий рівень – регіональний, охоплює інформаційні обліки, які є складовими міжвідомчих інформаційних підсистем і використовуються як службами Головного управління МВС (ГУМВС), управлінь МВС (УМВС), УМВС територіальних (УМВСТ), так й іншими відповідними регіональними правоохоронними органами.

Третій рівень – територіальний, охоплює інформаційні обліки, що є складовими міжвідомчих інформаційних підсистем і використовуються в міських, районних та лінійних ОВС, спеціалізованих підрозділах міліції та відповідних рівнів інших правоохоронних органах.

Зазначений поділ стосується як міжвідомчих, так і галузевих інформаційних підсистем.

Основою системи збору, контролю та використання інформації є третій рівень. Саме на цьому рівні забезпечується первинне накопичення інформації, ведення територіальних банків даних, захист інформації, актуалізація інформаційних фондів та передача інформації до банків даних другого та першого рівнів.

На другому рівні здійснюється формування регіональних банків даних, обробка інформації, забезпечується доступ територіальних підрозділів для санкціонованого використання інформації, інформаційний зв'язок між регіонами та першим рівнем. Забезпечується зв'язок з територіальними правоохоронними органами та іншими установами держави. Здійснюються контрольні функції щодо виконання вимог повноти, достовірності, актуальності та збереження інформації відповідно до законів України та відомчих нормативних актів.

На першому рівні забезпечується інтеграція та обробка інформації для формування банків даних інформаційних підсистем, міжвідомчий та міжрегіональний інформаційний зв'язок, керування системою інформаційного забезпечення на базі ОВС та дотримання стратегії її розвитку, розробка нормативно-правової бази впровадження сучасних інформаційних технологій. Виконуються контрольні функції з дотримання вимог повноти, достовірності, актуальності та захисту інформації у системі інформаційного забезпечення відповідно до законів України та відомчих нормативних актів, визначається інформація міждержавного обміну (Рис. 2).

погіршуються інші критерії якості; чому перевага віддана цьому, а не іншому критерію?

В постановці та вирішенні даної задачі в аспекті багатокритеріальної оптимізації основним етапом є побудова допустимої, а потім оптимальної множини рішень. Тому перейдемо до формалізації постановки задачі в даному аспекті і розглянемо один із можливих варіантів пошуку сфери допустимих рішень в рамках нижче структурованої моделі.

ДАНО:

1. *Програмно-апаратна система S,* яка підлягає захисту. До розгляду беруться такі формалізовані об'єкти опису:

множина $Z = \{z_1, z_2, ...z_k, ...z_K\}$ – клас захисних послуг, які, виходячи з результатів попереднього етапу необхідно надати системі S для забезпечення її безпеки;

вектор значень $\vec{U} = < u_1, u_2, ...u_m, ...u_M >$,

де u_m – значення потреби системи S в m-му виді обчислювального ресурсу для її нормального функціонування;

вектор значень $\vec{W} = < w_1, w_2, ...w_m, ...w_M >$, де w_m – величина обсягу потреби m-го виду обчислювального ресурсу, який виділяється системі S з урахуванням огранізації її підсистеми захисту.

2. *Комплекс модульних програмних засобів*, з яких комплектуються підсистеми забезпечення безпеки інформації програмно-апаратних систем класу S. Розглядаються такі об'єкти формалізованого опису цього комплексу:

програмні модулі різних служб захисту і функціональних процесів у вигляді множини A={a1, a2,…,an,…,aN }, в котрій кожний модуль an служби захисту реалізує деякі підмножини послуг Gn={gn1, gn2,…,gnl,…,gnk } і виконуються умови:

а) $G_i \neq G_j$ для будь-яких пар (i,j) при $i \neq j$,

б) $G = \bigcup_{n=1}^{N} G_n$ – множина всіх видів послуг, які можуть бути надані для виконання захисних функцій в системі S,

в) $Z \subseteq G$;

обчислювальні ресурси, необхідні для забезпечення нормального функціонування кожного модуля an, $n = \overline{(1, N)}$, який буде введений до складу підсистеми захисту, у вигляді матриці значень $V = \|v_{nm}\|, n = \overline{1, N}, m = \overline{1, M}$, де змінна n визначає модуль an, а змінна m – вид споживаного обчислювального ресурсу; вектор значень $\vec{C} = < c_1, c_2, ..., c_n, ...c_N >$ – показники вартості придбання, установки і супроводу служб захисту.

ПОТРІБНО:

Функція ризику для програмного забезпечення:

$$H^{((SOFT)}(t) = 1 - S^{(SOFT)}(t) = 1 - \exp\left\{-t\sum_{i=1}^{4}\lambda_i \rho_i^{(SOFT)}\right\} = 1 - \exp\{-2{,}42t\}$$

3. Сумарні функції безпеки та ризику за формулами(9'), (11),(12):

$$S_{\Sigma}(t) = S^{(HARD)}(t) * S^{(SOFT)}(t) =$$

$$= \exp\left\{-t\left(\sum_{i=1}^{4}\lambda_i \rho_i^{(HARD)} + \sum_{i=1}^{4}\lambda_i \rho_i^{(SOFT)}\right)\right\} = \exp\{-4{,}063t\};$$

$$H_{\Sigma}(t) = H^{(HARD)}(t) * H^{(SOFT)}(t) =$$

$$= 1 - \exp\left\{-t\left(\sum_{i=1}^{4}\lambda_i \rho_i^{(HARD)} + \sum_{i=1}^{4}\lambda_i \rho_i^{(SOFT)}\right)\right\} = 1 - \exp\{-4{,}063t\}$$

.

Висновок: навіть без побудов графіків функцій (для економії місця) можна побачити, що з плином часу ймовірність нештатних ситуацій зростає по експоненті, а стан безпеки ООТ так само по експоненті спадає. Тобто необхідно передбачати комплекс відповідних профілактичних заходів.

Варто зазначити, що забезпечення безпеки може бути досягнуте двома шляхами: по-перше, вжиттям всіх практично можливих заходів, по-друге, зниженням ризиків до прийнятного рівня. Проте досягнення абсолютної безпеки від одного фактора є економічно недоцільним, оскільки викликає неефективну витрату коштів.

Тому при управлінні безпекою ООТ необхідно керуватися таким.

По-перше, в оцінку ризику необхідно вводити *весь спектр небезпек*, можливих для досліджуваного об'єкту обчислювальної техніки при його роботі.

По-друге, в першу чергу заходи щодо зниження ризику приймаються *на найбільш несприятливих напрямах*. При виборі заходів захисту перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

По-третє, для більш точного відтворення «потоку» небезпечних подій та їх впливу на роботу ООТ і його компонентів, використовувати інші, окрім пуассонівського, типи потоків подій, беручи за основу наведений вище матеріал.

Етап 3 Комплектування системи захисту

Таким чином, нам відомі найбільш ймовірні загрози та орієнтовні обсяги втрат, які можуть бути ними завдані. Тепер співставимо отримані показники із обмеженнями за вартістю засобів захисту та спектрами наявних та потрібних послуг.

Отже, на цьому етапі ставиться завдання розглянути одну з можливих моделей і алгоритм комплексування складу підсистеми захисту інформації, орієнтуючись на модульність наданих засобів і систем захисту.

Виконаємо постановку і вирішення даної задачі в аспекті багатокритеріальної оптимізації. Природніше звести її до однокритеріальної. Проте при однокритеріальній постановці задачі без відповіді залишаються такі запитання: якою ціною досягається бажаний результат; в якій мірі

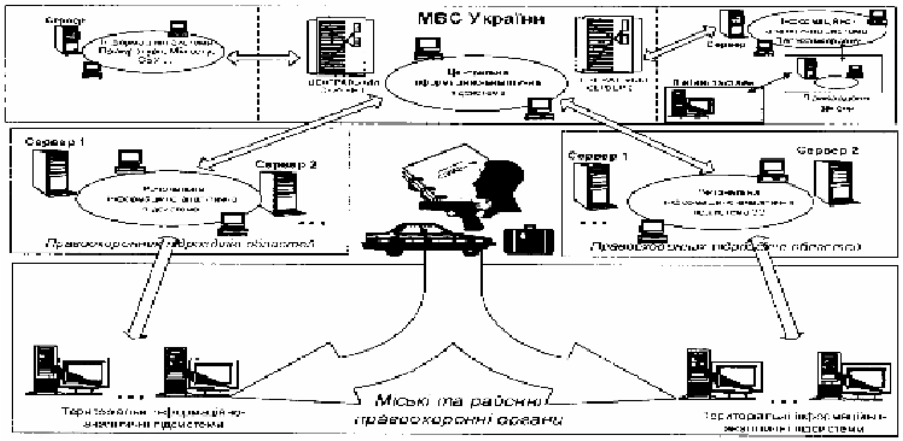


Рис. 2. Схема взаємозв'язків структурних рівнів системи інформаційного забезпечення

3.2. Автоматизовані банки даних оперативно-розшукового, оперативно-довідкового, адміністративного та статистичного призначення: відомості, колекції, картотеки, фонди

Інформаційні обліки в системі органів внутрішніх справ створюються для оперативного інформаційного забезпечення службової діяльності всіх підрозділів правоохоронних органів: від міських, районних, лінійних органів (далі – міськрайлінорганів) до республіканських.

На територіальному рівні управління в міськрайлінорганах на основі документів первинного обліку формуються банки даних оперативно-розшукового, оперативно-довідкового, адміністративного та статистичного призначення, які містять відомості про:

– події та факти кримінального змісту;

– адміністративні правопорушення;

– підприємства, організації та установи, що становлять оперативний інтерес;

– об'єкти дозвільної системи;

– зареєстрований автомототранспорт;

– зареєстровану вогнепальну та газову зброю;

– викрадені, загублені та вилучені предмети злочинного посягання, у тому числі:

- номерні та безномерні речі;
- антикваріат;
- автомототранспорт;
- вогнепальну та газову зброю;
- документи;
- знаряддя вчинення злочинів та правопорушень, речові докази;
- повідомлення спецапарату та іншу оперативну інформацію;

– фото- та відеотеки:

- місць вчинення злочинів та пригод;

- осіб криміногенних категорій;

– осіб:

- власників посвідчень водія;
- які скоїли злочини;
- які відбули покарання у місцях позбавлення волі;
- які скоїли адміністративні правопорушення;
- наркоманів;
- злочинців, які перебувають у розшуку;
- які зникли безвісти;
- невпізнаних трупів та невідомих хворих;
- які становлять оперативний інтерес;

– паспортну реєстрацію громадян та інші.

У межах міжвідомчих інформаційних підсистем галузевими службами міськрайлінорганів формуються такі основні первинні фонди інформації:

– підрозділами Департаменту інформаційних технологій МВС України:

- заяви та повідомлення про вчинені злочини та пригоди;
- затримані та зареєстровані особи;
- невідкладні дії чергового при отриманні повідомлень про правопорушення та пригоди, ведення оперативних планів тощо;
- табельна зброя, спеціальні засоби, засоби індивідуального захисту та активної оборони;
- оперативна інформація щодо осіб, які підозрюються в вчиненні злочинів, осіб певних категорій, членів злочинних угруповань;
- криміногенні об’єкти;
- вилучені та викрадені речі та інше;

– карним розшуком:

- особи криміногенних категорій, члени злочинних угруповань та інші, які становлять оперативний інтерес;
- особи, які оголошені в розшук;
- невпізнані трупи та невідомі хворі;
- викрадені та вилучені номерні речі, автомототранспорт, зброя;
- криміногенні об’єкти;
- оперативна інформація та інше;

– державною службою боротьби з економічними злочинами (далі – ДБЕЗ):

- оперативна інформація щодо осіб, підозрюваних у вчиненні злочинів, які займаються незаконними валютними операціями, виготовленням фальшивих монет тощо;
- способи вчинення розкрадань, злочинів у валютній та кредитно-фінансовій сферах;
- об’єкти господарської діяльності, які потребують оперативного нагляду;
- вилучений та викрадений автомототранспорт та інше;

– слідчими органами:

- особи, що притягуються до кримінальної відповідальності;
- кримінальні справи та їх рух;

III. ймовірність злого задуму $\lambda_{III}=0,8$;

IV. ймовірність виникнення реальної загрози ззовні $\lambda_{IV}=0,5$.

Протягом певного періоду спостережень мали місце:

50 подій I виду, з них 15 привели до ураження апаратури, 20 – до ураження програмного забезпечення;

10 подій II виду, з них 3 привели до ураження апаратури, 2 – до ураження програмного забезпечення;

5 подій III виду, з них 1 привела до ураження апаратури, 5 – до ураження програмного забезпечення;

2 події IV виду, з них 1 привели до ураження апаратури, 1 – до ураження програмного забезпечення.

ПОТРІБНО.

Побудувати часткові та сумарні функції безпеки та ризику.

Для спрощення будемо вважати, що:

– інтенсивності відповідних подій вже обчислені за формулою (9) на підставі даних правоохоронних, ремонтно-відновлювальних та інших органів;

– повний умовний збиток дорівнює кількості всіх комплектів ЕОТ $Y(A)=10$;

– всі події вважаємо незалежними одна від одної;

– компонент вважається враженим тоді, коли вражено хоча б один із комплектів ЕОТ або ПЗ.

Рішення

1. За формулою (10) розрахуємо ймовірності ураження компонент досліджуваного об’єкту:

Для апаратури:

$$\rho_I^{(HARD)}=\frac{15}{50}=0,3;\ \rho_{II}^{(HARD)}=\frac{3}{10}=0,3;\ \rho_{III}^{(HARD)}=\frac{1}{5}=0,2;\ \rho_{IV}^{(HARD)}=\frac{1}{2}=0,5$$

Для програмного забезпечення:

$$\rho_I^{(SOFT)}=\frac{20}{50}=0,4;\ \rho_{II}^{(SOFT)}=\frac{2}{10}=0,2;\ \rho_{III}^{(SOFT)}=\frac{5}{5}=1,0;\ \rho_{IV}^{(SOFT)}=\frac{1}{2}=0,5$$

2. Користуючись формулами (7) і (8) виведемо функції безпеки і ризику для апаратури і програмного забезпечення по кожному із потоку подій:

Функція безпеки для апаратного забезпечення:

$$S^{(HARD)}(t)=\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{(HARD)}\right\}=$$

$$\exp\{-t(2,74*0,3+1,37*0,3+0,8*0,2+0,5*0,5)\}=\exp\{-1,643t\}$$

Функція ризику для апаратного забезпечення:

$$H^{(HARD)}(t)=1-S^{(HARD)}(t)=1-\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{(HARD)}\right\}=1-\exp\{-1,643t\}$$

Функція безпеки для програмного забезпечення:

$$S^{(SOFT)}(t)=\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{(SOFT)}\right\}=$$

$$\exp\{-t(2,74*0,4+1,37*0,2+0,8*1,0+0,5*0,5)\}=\exp\{-2,42t\}$$

подій будемо наближено вважати пуассонівським. Тоді для *j*-ї компоненти досліджуваного об'єкту можна записати:

$$S_j(t) = \exp\left\{-t\sum_{i=1}^{N}\lambda_i\rho_{ij}\right\}, \quad (7)$$

$$H_j(t) = 1-\exp\left\{-t\sum_{i=1}^{N}\lambda_i\rho_{ij}\right\}, \quad (8)$$

де λ_i – інтенсивність небезпечних подій *i*-го виду ($i=\overline{1,N}$);

ρ_{ij} – ймовірність ураження подією *i*-го виду *j*-ї компоненти досліджуваного об'єкту($j=\overline{1,K}$).

$$\lambda_i = \frac{a_i(t)}{T}, \quad (9)$$

де $a_i(t)$ – математичне сподівання числа подій *i*-го типу за період спостереження *T*.

Наближено можна вважати, що

$$\rho_{ij} = \frac{n_{ij}}{n_i}, \quad (10)$$

де n_{ij} – число "НП" *i*-го виду, які привели до ураження *j*-ї компоненти; *ni*– загальне число "НП" *i*-го виду, *N* – число джерел небезпеки для даного об'єкту обчислювальної техніки .

Тоді сумарні функції безпеки та ризику матимуть, відповідно, такі вигляди:

$$S_\Sigma(t) = \prod_{j=1}^{K} S_j(t) = \exp\left\{-t\sum_{j=1}^{K}\Lambda_j\right\}, \quad (11)$$

$$H_\Sigma(t) = \prod_{j=1}^{K} H_k(t) = 1-\exp\left\{-t\sum_{j=1}^{K}\Lambda_j\right\}, \quad (12)$$

де *Si(t), Hi(t)* – функції безпеки і ризику для *j*-го компоненту об'єкта($j=\overline{1,K}$);

$$\Lambda_j = \sum_{i=1}^{K}\lambda_i\rho_{ij}. \quad (9')$$

Значення функцій безпеки і ризику, "пропущені" через формули (1)-(6) дають значення показників типу ЧП2 у майбутньому.

Розглянемо застосування на практиці наведених вище формул (7)-(12).

Приклад 2

ДАНО.

Для того самого об'єкта обчислювальної техніки за результатами спостережень обраховані такі інтенсивності небезпечних подій:

I. виникнення проблеми із технікою $\lambda_I=2,74$;

II. перехоплення інформації або НСД через допоміжне обладнання $\lambda_{II}=1,37$;

- речові докази та інше;

– експертно-криміналістичною службою:

- сліди, вилучені з місць подій, та знаряддя вчинення злочинів;
- фотороботи підозрюваних осіб;
- дактилоскопія;
- фото- та відеотеки;
- вилучена фальшива валюта;
- кулегільзотека та інше;

– службою громадської безпеки:

- розташовування сил та засобів;
- індивідуальна та відомча зброя;
- об'єкти дозвільної системи;
- адмінправопорушення;
- паспортні дані громадян;
- особи, які відбули покарання в місцях позбавлення волі згідно з чинним законодавством та інше;

– службою ДАІ:

- зареєстрований автомототранспорт;
- викрадений та вилучений автомототранспорт;
- власники посвідчень водія;
- дорожньо-транспортні пригоди;
- адмінправопорушення тощо;

– державною службою охорони:

- стан та характеристики об'єктів, що охороняються;

– службою виконання покарань:

- спецконтингент;
- оперативна інформація;
- порушення режиму утримання;
- результати перевірок явок з повинною та інше.

Порядок формування інформаційних фондів галузевими службами, відповідальність за їх актуальність, достовірність та використання регламентуються відповідними нормативно-правовими документами.

У складі банків даних регіонального рівня накопичується інформація, яка надходить з міськрайлінорганів та установ виконання покарань, має регіональний зміст та містить дані про:

– надзвичайні події;

– злочини та адміністративні правопорушення;

– підприємства, організації та установи, що становлять оперативний інтерес;

– зареєстрований автомототранспорт;

– зареєстровану вогнепальну та газову зброю;

– викрадені, загублені та вилучені предмети злочинного посягання, у тому числі:

- номерні та безномерні речі;
- антикваріат;
- автомототранспорт;

- вогнепальну та газову зброю;
- документи;

– криміналістичні обліки (кулегільзотеки, слідотеки, відбитки пальців рук тощо);

– осіб таких категорій:
- які вчинили злочини та оголошених у розшук;
- які вчинили адміністративні правопорушення;
- наркоманів;
- які зникли безвісти, невпізнаних трупів та невідомих хворих;
- які становлять оперативний інтерес;

– обліки адресних бюро;

– обліки оперативно-довідкових та дактилоскопічних картотек;

– обліки адміністративно-управлінського призначення (законодавчо-нормативні акти, розпорядчі документи, накази);

– обліки спеціалізованого призначення галузевих служб (кадрові, господарчі, бухгалтерські тощо), архівів та спецфондів.

На центральному рівні управління накопичується інформація, що використовується при аналізі, плануванні, прийнятті рішень та проведенні в межах України оперативно-розшукових, слідчих та інших спеціальних заходів по боротьбі зі злочинністю. До складу інформаційних фондів першого рівня входять:

– банки кримінологічної інформації, що містять відомості про:
- надзвичайні події;
- нерозкриті тяжкі та резонансні злочини;
- викрадені, загублені та вилучені предмети, знаряддя вчинення злочинів, речові докази, у тому числі:
  - номерні речі;
  - антикваріат;
  - автомототранспорт;
  - вогнепальну зброю;
  - документи;
- криміналістичні обліки;
- викрадені та вилучені наркотичні речовини;
- об’єкти виготовлення, переробки, зберігання та використання наркотичних речовин;
- осіб таких категорій:
  - особливо небезпечних рецидивістів;
  - злочинців-«гастролерів»;
  - злочинців, оголошених у міждержавний розшук;
  - організаторів і членів злочинних угруповань, кілерів;
  - які були засуджені за злочини, пов’язані з наркотиками, торговців та розповсюджувачів наркотичних речовин з міжрегіональними та міжнародними зв’язками;
  - схильних до вчинення злочинів, пов’язаних з посяганнями на інтереси держави;
  - що зникли безвісти;

$$C_{чII}^{(SOFT)}(A) = \frac{0,6 * 25}{50} = 0,3$$

– для програмного забезпечення.

Тоді часткові ризики від події II виду за формулою (6) становитимуть відповідно

$$R_{II}^{(HARD)}(A) = 0,6 * 0,5 * 10 * 0,3 = 0,9$$

– для апаратури;

$$R_{II}^{(SOFT)}(A) = 0,6 * 0,5 * 0,3 * 50 = 4,5$$

– для програмного забезпечення.

В разі виникнення події III і IV виду у сфері ураження опиняться всі наявні ЕОМ із своїм програмним забезпеченням.

Звідси,

$$C_{чIII}^{(HARD)}(A) = \frac{0,25 * 10}{10} = 0,25,$$

$$C_{чIV}^{(HARD)}(A) = \frac{0,06 * 10}{10} = 0,06$$

– для апаратури;

$$C_{чIII}^{(SOFT)}(A) = \frac{0,25 * 50}{50} = 0,25,$$

$$C_{чIV}^{(SOFT)}(A) = \frac{0,06 * 50}{50} = 0,06$$

– для програмного забезпечення.

Тоді часткові ризики від події III виду за формулою (6) становитимуть відповідно

$$R_{III}^{(HARD)}(A) = 0,25 * 1,0 * 10 * 0,25 = 0,625$$

– для апаратури;

$$R_{III}^{(SOFT)}(A) = 0,25 * 1,0 * 0,25 * 50 = 3,125$$

– для програмного забезпечення.

Відповідно, часткові ризики від події IV виду становитимуть

$$R_{IV}^{(HARD)}(A) = 0,06 * 1,0 * 10 * 0,06 = 0,036$$

– для апаратури;

$$R_{IV}^{(SOFT)}(A) = 0,06 * 1,0 * 0,06 * 50 = 0,18$$

– для програмного забезпечення.

7. Повний ризик для даного об’єкта:

$R_{пов}(A)$=0,31+1,53+0,9+4,5+0,625+3,125+0,036+0,18=8,206.

Висновок: без введення в дію систем захисту повноцінна робота даного об’єкта обчислювальної техніки практично неможлива.

Тепер розглянемо динаміку зміни небезпечних подій у часі.

Якщо розуміти під безпекою ООТ відсутність неприпустимого ризику ураження об’єкта при виникненні небезпечних ситуацій, для оцінки вводиться *функція безпеки S(t).* Сукупність характеристик небезпечних подій, «зважених» за ймовірностями їх виникнення подамо як *функцію ризику H(t)*.

Для спрощення подальшого викладення матеріалу, «потік» небезпечних

$$C_{IV}(A) = \frac{0,6}{10} = \frac{6}{100}.$$

3. Тоді можливі одномоментні збитки від тих же подій відповідно до (5) становитимуть

$$R_{Iодн}(A) = 0,7 * \frac{7}{10} * 10 = 4,9$$

$$R_{IIодн}(A) = 0,6 * \frac{6}{10} * 10 = 3,6;$$

$$R_{IIIодн}(A) = 0,25 * 0,25 * 10 = 0,625;$$

$$R_{IVодн}(A) = 0,06 * \frac{6}{100} * 10 = 0,036$$

4. Комбінований одномоментний ризик дорівнює

$$R_{Кодн} = 4,9 + 3,6 + 0,625 + 0,036 = 9,16;$$

5. Комбінований середній ризик дорівнює

$$R_{Ксер} = 7 + 6 + 2,5 + 0,6 = 16,1.$$

Припустимо тепер, що на кожному із 10-ти комплектів ЕОМ встановлено 5 комплектів програмного забезпечення. В разі виникнення події I виду у сфері ураження може опинитися приблизно чверть наявних ЕОМ із своїм програмним забезпеченням, тобто 2,5 комплекти апаратури і 12,5 комплектів програмного забезпечення відповідно.

6. Часткові ступені уражаємості дорівнюють

$$C_{чI}^{(HARD)}(A) = \frac{0,7 * 2,5}{10} = 0,175$$

– для апаратури;

$$C_{чI}^{(SOFT)}(A) = \frac{0,7 * 12,5}{50} = 0,175$$

– для програмного забезпечення.

Тоді часткові ризики від події I виду за формулою (6) становитимуть відповідно

$$R_I^{(HARD)}(A) = 0,7 * 0,25 * 10 * 0,175 = 0,31$$

– для апаратури;

$$R_I^{(SOFT)}(A) = 0,7 * 0,25 * 0,175 * 50 = 1,53$$

– для програмного забезпечення.

В разі виникнення події II виду у сфері ураження може опинитися приблизно половина наявних ЕОМ із своїм програмним забезпеченням, тобто 5 комплектів апаратури і 25 комплектів програмного забезпечення відповідно.

Звідси,

$$C_{чII}^{(HARD)}(A) = \frac{0,6 * 5}{10} = 0,3$$

– для апаратури;

• невпізнаних трупів та невідомих хворих;

– банк оперативно-довідкової інформації, що містить дані алфавітного та дактилоскопічного фондів раніше засуджених осіб;

– банк статистичної інформації про стан злочинності та результати боротьби з нею;

– банк спеціальної інформації, що містить повідомлення спецапарату та іншу оперативну інформацію загальновідомчого значення;

– банк паспортних даних громадян;

– банк з інформацією про зареєстрований автотранспорт;

– банк з інформацією про зареєстровану вогнепальну зброю;

– банки даних адміністративно-управлінського призначення;

– банки даних спеціалізованого призначення галузевих служб;

– банки даних архівів, спеціальних фондів та інші.

Повнота даних на кожному рівні за категоріями обліку визначається відповідними нормативними документами.

Література

1. *Бірюков В.В.* Научные и практические основы использования компьютерных технологий для фиксации криминалистически значимой информации. – Луганск, 2002.

2. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. // Відомості Верховної Ради України. – 1998. – № 27-28. Ст. 181.

3. Програма інформатизації органів внутрішніх справ України на 2000-2010 роки. – К., Управління оперативної інформації МВС України, 1999.

4. Саницький *В.А., Карацюба А.М., Святобог В.В. та ін.* Система інформаційного забезпечення ОВС України: Навчально-практичний посібник / За ред. Л.В. Бородича. – К., 2000. – - 144 с: іл., табл.

5. 1С: Бухгалтерия. Версія 7.7. Руководство пользователя. – М., Фирма "1С", 2001.

РОЗДІЛ 4
БЕЗПЕКА МЕРЕЖ, СИСТЕМ І БАНКІВ ДАНИХ ОРГАНІВ ДІЗНАННЯ ТА ДОСУДОВОГО СЛІДСТВА

4.1. Концепція забезпечення безпеки інформації на об'єкті в умовах необхідної ситуації

Доктринальні засади

Забезпечення безпеки інформації та протидія розвідкам різних видів актуальний на всіх щаблях в усіх галузях життя держави – від окремої фізичної особи до державного відомства або крупної корпорації. (*Примітка. Під забезпеченням безпеки інформації будемо розуміти всі заходи, передбачені НД ТЗІ 1.1-003-99 ст.ст. 4.1.2, 4.1.4-4.1.7, 4.3.7)

Подібно до того, як будівля складається з окремих цеглин, а живий організм – з клітин, так загальнодержавна безпека формується з багатьох складників, різних за своїм якісним і кількісним станом, об'єднаних єдиною формотворчою ідеєю – убезпечення держави від внутрішніх та зовнішніх загроз. Як відомо з біології та медицини здоров'я однієї клітини часто визначає стан здоров'я всього організму. Тому основу, серцевину, забезпечення безпеки інформації та протидії ворожій розвідувальній діяльності, становить саме захист фізичної особи та безпосередньо того середовища, де ця особа проводить свою життєдіяльність. Як правило, таким середовищем є квартира, цех, офіс, штаб тощо, словом, такий об'єкт, геометричними розмірами якого при розгляді його в рамках населеного пункту (місцевості) можна знехтувати, причому цілеспрямована дія на цей об'єкт, як правило, не зачіпає сусідні (принаймні це не ставиться за мету). Надалі такий об'єкт називатимемо ТОЧКОВИМ.

Детальний огляд вітчизняної та зарубіжної літератури як з питань комп'ютеризації, так і з питань забезпечення збереження таємниці та безпеки інформації показав, що на сьогоднішній день:

– показано важливість інформації у сучасному світі;

– дані визначення найголовнішим властивостям інформації, які визначають її практичну цінність;

– визначені та класифіковані основні джерела загроз для інформації у її традиційній і машинній формі;

– створено методичну базу з питань добування та опрацювання інформації, визначення її достовірності і точності та організації діяльності відповідних служб;

– відпрацьований порядок класифікування інформації відповідно до її цінності;

– фундаментально розроблена нормативна і науково-методична база для проведення організаційно-адміністративних, нормативно-правових та інженерно-технічних заходів, спрямованих на забезпечення конфіденційності, цілісності і доступності підзвітних інформаційних ресурсів;

конкретного часткового випадку.

Розберемо застосування цих теоретичних викладень на практиці та отримаємо числові показники другої групи (ЧП2).

Приклад 1

ДАНО.

Нехай внаслідок декомпозиції до І рівня досліджуваного гіпотетичного об'єкту обчислювальної техніки із 10 комплектами ЕОТ та відпрацювання першого етапу досліджень для цього об'єкту , виділено такі небезпечні події із наступними ймовірносними показниками:

І. ймовірність виникнення проблеми із технікою *PI(A)=0,7*;

ІІ. ймовірність перехоплення інформації або НСД через допоміжне обладнання *PII(A)=0,6*;

ІІІ. ймовірність злого задуму *PIII(A)=0,25*;

IV. ймовірність виникнення реальної техногенної чи стихійної загрози ззовні *PIV(A)=0,06*;

Для спрощення будемо вважати, що:

– імовірності виникнення відповідних подій вже обчислені за формулою (2) на підставі даних правоохоронних, ремонтно-відновлювальних та інших органів;

– повний умовний збиток дорівнює кількості всіх комплектів ЕОТ *Y(A)=10*;

– всі події вважаємо незалежними одна від одної.

ПОТРІБНО.

1. Обчислити часткові ризики від подій кожного виду.
2. Обчислити комбінований ризик.

РІШЕННЯ.

1. За формулою (1) середні ризики становлять:

– від подій І виду (відмови в ЕОТ)

$$R_I(A) = 0{,}7 * 10 = 7;$$

– від подій ІІ виду (перехоплення через допоміжне обладнання):

$$R_{II}(A) = 0{,}6 * 10 = 6;$$

– від подій ІІІ виду (злий задум персоналу):

$$R_{III}(A) = 0{,}25 * 10 = 2{,}5;$$

– від подій IV виду (негативний вплив середовища):

$$R_{IV}(A) = 0{,}06 * 10 = 0{,}6.$$

2. Тепер обчислимо відповідні ступені ураженості елементів об'єкту за формулою (3), пам'ятаючи фізичний зміст формули (1):

$$C_I(A) = \frac{7}{10};$$

$$C_{II}(A) = \frac{6}{10};$$

$$C_{III}(A) = \frac{2{,}5}{10} = 0{,}25;$$

Тоді ця формула набуває такого вигляду:

$$R_ч(A) = \frac{\nu(t)}{T}\Big|_A P(H)C_{уч}(A)H \quad , (6)$$

де $R_ч(A)$ – частковий ризик, $P(H)$ – ймовірність перебування елементів певного типу у сфері ураження, H – їх кількість (відповідає $Yn(A)$ у виразі (5)), $Суч(A)$ – ступінь вражаємості цієї групи елементів.

Як наслідок, повний ризик для всього об'єкта обчислювальної техніки буде рівним сумі часткових ризиків для груп елементів кожного типу, які складають досліджуваний ООТ. *Тобто, ми отримали набір показників групи ЧП2.*

Для ілюстрації наведемо схему обчислення ризиків (рис. 6).

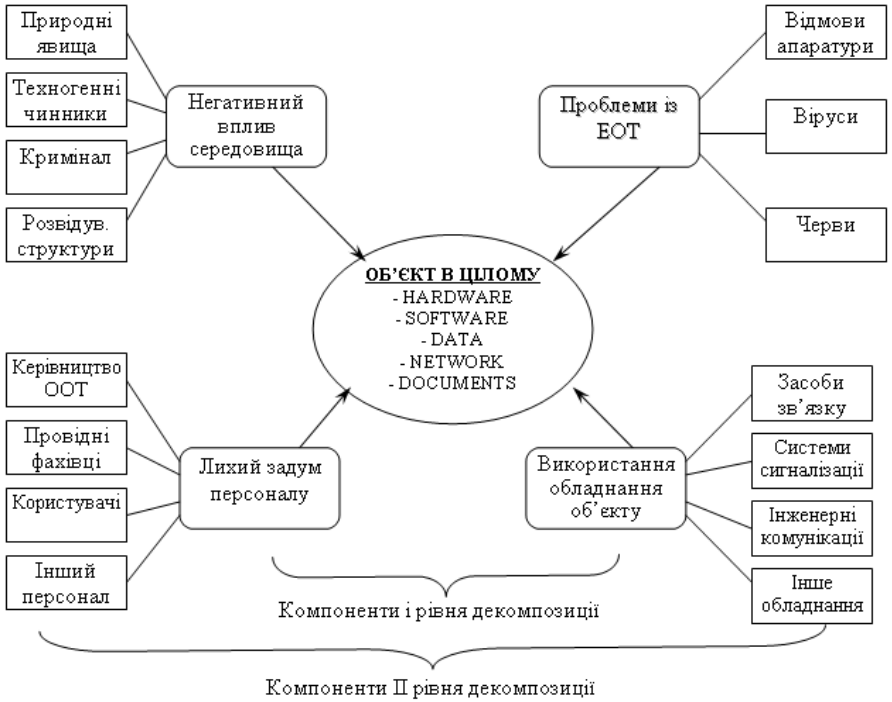


Рис. 6. Схема нарахування загального ризику.

Іншими словами отримано набір числових показників другої групи (ЧП2).

Зазначимо, що кількість компонент кожного із рівнів може варіюватися відповідно до часткових випадків, як і число рівнів декомпозиції.

Необхідно завжди брати до уваги, що небезпечні події можуть класифікуватися за масштабом, тяжкості наслідків та іншими ознаками. Існують різні – відомчі (галузеві), національні та міжнародні системи класифікації таких подій, і вибір тієї чи іншої з-поміж них залежить від

– розроблений розгалужений методичний апарат для втілення вищезазначених заходів у життя;

– існує широкий асортимент спеціальних засобів фізичного, апаратного, програмного, криптографічного захисту об'єктів та інформації, яка циркулює всередині цих об'єктів та між ними.

Основні завдання, які виникають в ході забезпечення безпеки інформації, такі:

– захист об'єктів, де розміщені фізичні носії та засоби обробки інформації;

– забезпечення нормального і безперебійного функціонування баз і банків даних;

– збереження якості інформації.

З точки зору застосування сил і засобів забезпечення безпеки інформації має бути комплексним і включати в себе як адміністративно-організаційні, так і чисто технічні заходи.

В умовах несталої постійно мінливої політичної, економічної, кримінальної ситуації в державі (населеному пункті) система безпеки точкового об'єкту має бути спеціальною областю, при цьому органічно інтегрованою до загальної системи управління цим об'єктом. Всі ці положення авторами вперше були систематизовані і подані в комплексі у проведених досліджень і опублікованих раніше праць.

Як показує багаторічна практика побудови математичних моделей і алгоритмів різного призначення, одним із слабких місць подібних розробок є наявність в них складних (а реально – майже незастосовних) для практичного застосування формул. Тому автори у даному матеріалі здійснюють спробу уникнути подібного.

Система безпеки точкового об'єкту є, як правило, унікальною в кожному конкретному випадку і залежить від багатьох суб'єктивних і об'єктивних чинників. Але три процедури є обов'язковими в будь-якому разі:

1) аналіз загрози для інформації на даному об'єктові;

2) оцінка ймовірності виникнення того чи іншого виду загрози та можливі втрати в разі «поразки»;

3) випрацювання альтернативних засобів і способів захисту.

Наступне, що необхідно відпрацювати при розробці концепції захисту інформації (для конкретного об'єкту в конкретних умовах), це (як правило, шляхом послідовних ітерацій, переходячи від часткового до загального):

– якого плану і з якою імовірністю може виникнути загроза для інформації;

– що саме із інформаційних ресурсів підлягає захисту, в якій мірі і на який термін;

– в яких умовах (розташування об'єкта на місцевості, архітектурні та будівельні особливості, місцеве населення тощо) за допомогою яких технічних засобів проводиться обробка і передача інформації (засоби зв'язку, ЕОТ і т.д.);

– індивідуальні та загальні особливості персоналу.

Іншими словами, *для того, щоб ефективно захистити свої інформаційні*

ресурси, засоби їх зберігання, обробки та передачі, необхідно, у свою чергу мати велику кількість впорядкованої інформації з усіма наслідками.

Після того, як відповідь на згадані запитання (їх може бути і більше) отримана, можна розробляти власні організаційні і технічні заходи, спрямовані на захист інформації, або використовувати вже існуючі пристрої, засоби та методики. І саме тут починаються найбільші складнощі, оскільки загальна теорія захищеності об'єкту до кінця ще далеко не побудована, а рівень автоматизації, як правило випереджує рівень забезпечення безпеки. Інакше кажучи, *потрібен типовий та наочний алгоритм* роботи посадових осіб та підрозділів при формуванні, експлуатації та супроводженні системи забезпечення безпеки.

Нижче ми розглянемо один із можливих варіантів алгоритмізації.

Рис. 1. Взаємодія об'єкту з оточенням.

Всі зображені вище компоненти перебувають у стані безперервного інформаційного кругообміну. Сильно спрощена схем циркуляції інформаційних потоків показана на рис. 2.

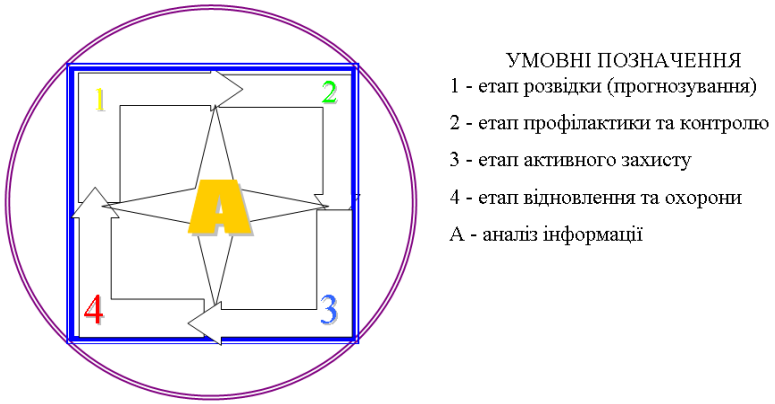


Рис. 2. Циркуляція потоків інформації

показник небезпеки, комбінована характеристика збитку і повторюваності, тобто середні за одиницю часу втрати (ймовірносний збиток).

За основу пропонуємо взяти раніше розроблений нами апарат аналізу ризиків для обґрунтування рішень і дій посадових осіб, відповідальних за збереження всіх основних якостей інформації – конфіденційності, цілісності та доступності.

У загальному випадку середній за певний проміжок часу комбінований ризик від небезпечної події *A* може бути обчислений за формулою

$$R(A)=P(A)Y(A) \qquad (1)$$

де $P(A)$ – статистична ймовірність події A (або *подієвий ризик*),

$Y(A)$ – можливий одномоментний збиток (або, якщо $P(A)=1$, *вартісний ризик*).

У свою чергу, подієвий ризик дорівнює

$$P(A)=\frac{\nu(t)}{T} \qquad (2)$$

де $\nu(t)$ – кількість проявів події A за час t;

T – період спостереження.

Тоді формула (1) набуде вигляду:

$$R(A)=\left.\frac{\nu(t)}{T}\right|_A Y(A) \qquad (1')$$

Тобто, фізичний зміст показника $R(A)$ – кількість або вартість підданих ризику протягом періоду дослідження елементів.

Введемо нову характеристику ООТ – *ступінь уражаємості* від впливу події A

$$C_y(A)=\frac{M_{вр.ел}}{M_{заг}}. \qquad (3)$$

Тут $M_{вр.ел}$ – число вражених елементів, $M_{заг}$ – загальне число елементів ООТ (або загальне число елементів ООТ, які опинилися в зоні ураження).

Тоді можливий одномоментний збиток $Y(A)$ може бути визначений за такою формулою:

$$Y(A)=Cy(A)Yn(A) \qquad (4)$$

де $Y_n(A)$ – *умовний повний збиток*, який чисельно рівний кількості або вартості всіх елементів ООТ (або кількості чи вартості тих елементів ООТ, які опинилися в зоні ураження).

Таким чином, з урахуванням виразу (2) і (4), формула (1) набуде такого вигляду:

$$R(A)=\left.\frac{\nu(t)}{T}\right|_A C_y(A)Y_n(A) \qquad (5)$$

Це загальна формула вирахування ризику. При *розгляді часткових ризиків*, притаманних саме для певного типу елементів ООТ, які підпадають під вплив «НП», до формули (5) необхідно вводити необхідні модифікації.

– є чи деяка система в його діях;
– чого в них більше: логіки, емоцій, традицій чи випадків;
– чи існує такий союзник, з який супротивник не порве;
– явні границі допустимості в його діяннях;
– уразливі місця супротивника;
– те, як він оцінює ситуацію;
– ймовірні реакції на дії з кожної сторони.

У деяких випадках перспективно йти не від фактів до побудови гіпотези, а від висунутої гіпотези до наявних фактів. Так, відмінно знаючи ключову особу супротивника, думкою поставте себе на його місце. Виходячи з цього, виведіть ряд припущень про його наміри і визначите дії, притаманні кожному з тих намірів. Зіставивши уявні ситуації і наявні реалії, відберіть ту гіпотезу, яка відповідає більшості наявних фактів.

Оптимальну допомогу в обробці всієї подібної інформації може зробити будь-яка, ЕОМ, яка аргіогі не страждає суб'єктивністю і обмеженістю розуму людини.

Після проведеного таким чином аналізу фактів на виході маємо ймовірність виникнення загрози того чи іншого виду. Позначимо її як P(A), де A – небезпечна подія. Це і є показники типу ЧП1.

Взагалі кажучи, за принципами має бути збудована база знань або експертна система. Проте питання її побудови ми не будемо розглядати у даному матеріалі, а обмежимося для спрощення припущенням, що набуті дані обробляються вручну.

Після того, як будуть отримані ймовірносні показники для небезпечних подій, нехобхідно обчислити обсяги можливих втрат від їх впливу та прогнози на майбутнє.

Етап 2. Аналіз та прогнозування ризиків.

Візьмемо за основу визначення: *небезпека* – це властивість матеріальних об'єктів та систем природи і суспільства завдати при їх взаємодії яку-небудь шкоду. Небезпека проявляє себе у вигляді передбачуваної, але не контрольованої загрози настання негативного явища з певними параметрами у певній сфері і у визначений проміжок часу, що має нечіткі соціальні, економічні або інші наслідки.

Основними показниками (мірами) небезпеки є *інтенсивність* та *ризик*. *Інтенсивність* характеризується обсягом та швидкістю явищ, які можуть викликати негативні наслідки, масштабом дії таких явищ та імовірністю подій з певними параметрами, незалежно від можливих втрат враженого при цьому ООТ або одного чи декількох його складових частин.

Ризик можна оцінити тільки для об'єкту, та (або) системи, які підпадають під небезпеку. Тому ризик становить собою усвідомлену небезпеку (загрозу) настання в будь-якій системі негативної події з окресленими у часі та просторі наслідками або, іншими словами, існування чи можливість виникнення ситуації при якій формуються передумови протидії реалізації завдань і функції ООТ і забезпеченню його безпеки. *Показниками* ризику можуть виступати соціальний, економічний, інший збитки та (або) змішаний збиток, повторюваність (ймовірність) негативної події, яка становить собою

Тепер покажемо, які ж служби мають брати участь у загальній справі (рис. 3.).

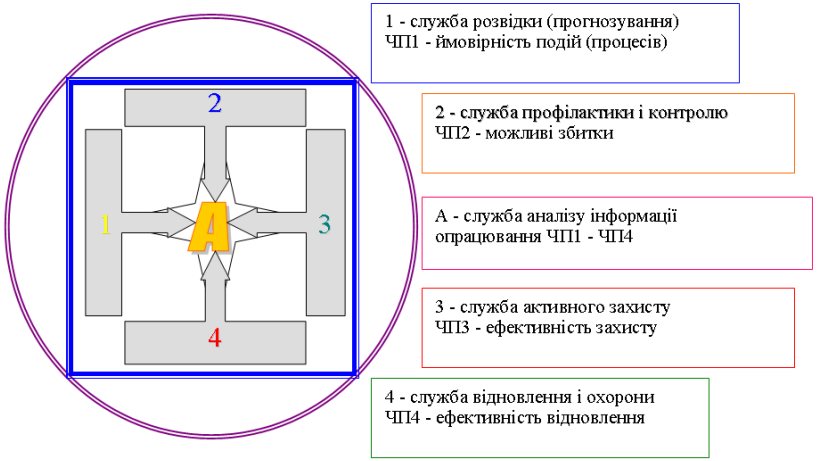


Рис. 3. Служби забезпечення безпеки

У цьому матеріалі «служба» є поняття умовне і не обов'язково означає «структурний підрозділ». Функції кожної із служб може виконувати одна особа, одночасно одна особа може виконувати функції декількох, а то і всіх служб.

Результат роботи кожної служби мусить становити собою числовий показник (ЧП) або їх впорядкований набір.

Отже, відправною точкою в процесі забезпечення безпеки є аналіз відповідних потреб і проблем, які виникли або можуть виникнути із плином часу.

Далі настає черга зовнішньої розвідки із подальшим аналізом достовірності добутих даних. Також працює служба внутрішньої безпеки і подає аналогічні відомості (на виході – ЧП1).

Потім ці дані розглядаються під кутом зору можливої загрози. Аналізуються втрати, які може завдати та чи інша загроза в разі її успішної реалізації. Проводиться вся можлива профілактика (на виході – ЧП2).

На підставі вартісних оцінок втрат, аналізу множин потрібних захисних послуг, обмежень за ресурсами комплексується система захисту. У разі декількох варіантів комплексування необхідно вибрати оптимальний з них (на виході – ЧП3).

Відповідно до отриманих результатів службою аналізу вносяться відповідні корективи до роботи служб зовнішньої розвідки, внутрішньої безпеки, активного захисту, відновлення і охорони (на виході – ЧП4).

Головне при цьому – гарантувати повноцінний обіг інформації між названими службами.

Укрупнена блок схема алгоритму цього комплексу зображена на рис. 4.

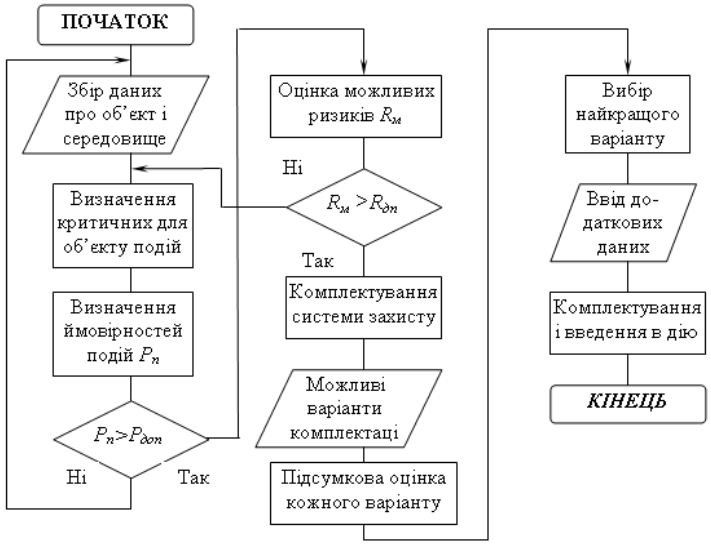


Рис. 4. Укрупнена блок схема алгоритму дії навчально-бойового програмного комплексу.

Тут P_n – ймовірність виникнення небезпечної події, $P_{доп}$ – допустиме значення цієї ймовірності, $R_м$ – можливий ризик за такої ймовірності, $R_{дп}$ – допустиме значення ризику.

Для повноцінного і ефективного використання названих вище ідей та навчання цим ідеям персоналу необхідно розробити спеціальний навчально-бойовий програмний комплекс, який би на підставі введених даних наочно показував основні джерела загроз та способи їх запобігання або захисту від них.

Тепер перейдемо до розгляду формального апарату, покладеного в основу кожного із названих етапів алгоритму.

Етап 1. Пошук, систематизація та аналіз інформації.

Враховуючи те, що на сьогодні найбільше значення має інформація саме у електронній формі, пошук, систематизацію та аналіз даних розглянемо на прикладі мережі Internet.

Кількість інформації, розміщеної в Internet, зростає з кожним днем, однак рівень її структуризації низький, а частота оновлення дуже висока. Вже в 1998 році, згідно з дослідженнями Лі Джилса і Стіва Лоуренса із NEC Research, Internet налічував більш ніж 320 млн. сторінок, в той час як індексні бази найбільш потужних пошукових вузлів містять відомості приблизно про 140 млн. документів. Проблема наповнення, що стояла раніше, трансформувалась у проблему пошуку відкритих та безкоштовних, але занурених в надрах колосального заплутаного гіпертекстового середовища джерел. Традиційні пошукові механізми не виконують завдання індексування і навіть не в змозі надати в упорядкованому вигляді наявні данні. При створенні в інформаційній установі проблемно-орієнтованого каталогу

Для успішної боротьби з ймовірною дезінформацією необхідно:

– розрізняти факти і думки;

– усвідомлювати, чи здатний інформатор за своїм статусом мати доступ до фактів, що ним повідомляються;

– враховувати суб'єктивні (зарозумілість, фантазійність...) характеристики джерела і його можливе відношення та/або ставлення до виданого повідомлення;

– застосовувати дублюючі канали інформації;

– виключати всі зайві проміжні ланки;

– пам'ятати, що особливо легко сприймається та дезінформація, яку ви припускаєте, чи бажаєте почути.

Користь від наявних матеріалів, , різко зростає, якщо:

– прояснено їх значення;

– істина розкривається не у вихідних даних, а в їх точному тлумаченні, тому що конкретний факт можна усвідомити лише в сполученні з іншими фактами.

Переробка інформації після попереднього збирання фактури і конкретної постановки проблеми має на увазі:

а) систематизацію фактів, що сортують за ступенем їх відношення до того чи іншого питання;

б) виявлення, ґрунтуючись на інтуїції, ключових моментів;

в) побудова припущень, що пояснюють основні факти;

г) одержання, при необхідності, додаткових даних;

д) оформлення висновків та їх перевірка на відповідність іншим беззаперечним фактам.

На окремі питання часто вдається одержати пряму і цілком визначену відповідь, а у відношенні інших вимушено обмежуються одними припущеннями.

Треба інтуїтивно розуміти, які саме з моментів є найважливішими, а не концентрувати увага відразу на багатьох, що здатне заблокувати роботу людського мозку (або ЕОМ).

Інколи корисно прокрутити отриману інформацію серед осіб, що мають до неї деяке відношення, з того міркування що вони допоможуть виявити які-небудь зв'язки з деякою побічною інформацією.

Висловивши певне припущення, його ретельно перевіряють на узгодженість із усіма даними і коли тут виявиться значна непогодженість, а факти явно правдиві, – потрібно змінити судження.

Помилкова інтерпретація фактури ймовірна, якщо:

– представлені не всі матеріали,

– деякі з наявних під рукою фактів сумнівні,

– вся увага зосереджується лише на тих повідомленнях, які підтверджують чекання і припущення аналітика.

Щоб виявити можливі шляхи розвитку початкової ситуації, треба дуже чітко уявляти:

– ключових персон супротивника;

– те, до чого він у сутності прагне (як по максимуму, так і по мінімуму);

Таблиця 1

ДОСТОВІРНІСТЬ				
Шанси "за"	**Шанси "проти"**	**Ступінь достовірності, виражена у шансах**	**Ступінь достовірності, виражена через ймовірність**	**Значення імовірності**
99-85	1-15	Майже напевно, інформація достовірна (шанси: 9 проти 1)	Майже напевно, інформація достовірна (майже напевне - "так")	0,99-0,85
84-60	16-40	Багато шансів, що інформація достовірна (шанси: 3 проти 1)	Певно що, інформація достовірна (певно - "так")	0,84-0,51
59-40	41-60	Шанси приблизно рівні (шанси: 1 проти 1)		0,50
39-15	61-85	Багато шансів, що інформація недостовірна (шанси: 1 проти 3)	Певно що, інформація недостовірна (певно - "ні")	0,49-0,15
14-1	86-99	Майже напевно, інформація недостовірна (шанси: 1 проти 9)	Майже напевно, інформація недостовірна (майже напевне - "ні")	0,14-0,01
НЕДОСТОВІРНІСТЬ				

Обов'язково варто враховувати, що інформація, що надходить до вас, може бути:

– підсунута джерелу як дезінформація;

– перекручена їм навмисно;

– змінена – довільно чи мимоволі – у ході її передачі.

Усні повідомлення циркулюючі по горизонтальним і неформальним каналам, менш піддані перекручуванням, а от інформація що йде «нагору», частіше спотворюється (через явне бажання догодити, одержати винагороду, уникнути покарання...), ніж навпаки.

При навмисній дезінформації застосовують як відому неправду, так і витончену напівправду, що поволі підштовхує сприймаючих до помилкових суджень. Найбільш розповсюдженими прийомами тут є:

– пряме приховання фактів;

– тенденційний підбір даних;

– порушення логічних і хронологічних зв'язків між подіями;

– подавання правди в такому контексті (додаванням помилкового факту чи натяку...), щоб вона сприймалася як неправда;

– виклад найважливіших даних на яскравому тлі відволікаючих увагу зведень;

– змішування різнорідних думок і фактів;

– повідомлення інформації такими словами, які можна витлумачувати по-різному;

– не згадування ключових деталей факту.

Перекручування, що виникають у процесі ретрансляції початкових даних, найчастіше відбуваються через такі причини:

– передачі тільки частини повідомлення;

– переказу почутого своїми словами («зіпсований телефон»);

– пропуску фактури через призму суб'єктивно-особистісних відносин.

ресурсів Internet доцільно звертатися до пошукових служб.

Пошукові служби розрізняються за кількісними (обсяг, глибина пошуку) і за якісними (можливість використання формальних логічних запитів, фільтрація результату) характеристиками. Умовно їх можна поділити на *«пошуковими»* (пошукові машини) і *каталоги* (директорії, рубрикатори).

Перші – *«пошуковими»* «прочісують» простір IP-адрес за допомогою спеціальних програм під назвою «павуки» (spider) або роботів, і індексують найдені сторінки. До самих потужних і популярних звичайно відносять AltaVista, HotBot, Northem Life, російськомовні – Яndex, Rambler.

Каталоги працюють зовсім інакше: нові Web-вузли вивчаються експертами і відносяться до відповідних тематичних категорій. Багато каталогів також забезпечують пошук у своїй базі даних. Як приклад можна навести Yahoo! та російськомовний «Ау!».

Для пошуку різнорідних документів у глобальній мережі використовуються описи документів, або «метадані» – «дані даних», термін, що є нестандартизованим але часто використовується останнім часом.

Система метаданих являє собою центральний логічний компонент будь-якої електронної бібліотеки, вона організовує сукупність її електронних інформаційних ресурсів (або цифрових об'єктів).

Якщо поняття «метаданих» розглядати в аспекті історії інформатики, то це поняття є інтегральним по відношенню до таких традиційних понять, як формати надання даних, мови опису даних, лінгвістичне забезпечення АІС. Головна відмінність поняття метаданих від вище перелічених понять полягає в більш загальному характері метаданих, подібно до того, як «цифровий об'єкт» (інформаційний ресурс) є більш широким поняттям порівняно з поняттям «документ» або «одиниця зберігання».

Але створюються метадані по-різному, все залежить від того, в якій пошуковій системі власник даних хоче їх надати:

– в системі з ручною індексаціїю необхідно вручну вводити метадані в поля, перелік яких пропонується системою; дані при цьому зберігаються поза цією системою, на сервері власника або створювача;

– системи з автоматичною індексацією передбачають наявність метаданих у самому документі, практично дані і метадані мають форму єдиного документа.

До того ж різні люди по-різному підходять до набору метаданих (найчастіше це Content-Type, Content, Generator, Autor, Keywords, Description), їх перелік не є визначеним і обов'язковим, не розроблено також чітких правил порядку подання метаданих. А також Internet постійно поповнюється великою кількістю ресурсів, яка не завжди подається у форматі HTML.

Завдяки всьому цьому пошук в Internet часто не дає очікуваних результатів.

Маючи за мету виправити існуючий стан в березні 1995 року в місті Дубліні (штат Огайо) 52 вчених і спеціалістів в галузі бібліотечної справи, інформатики і суміжних дисциплін прийняли модель опису електронних ресурсів, яка отримала назву Дублінського ядра елементів метаданих (Dublin Metadata Core Elements). Dublin Core об'єднує у собі формат метаданих та

правила його складання. Еволюція документа, що описує цю модель, а точніше вже формат, відбувалась і відбувається під егідою Dublin Core Metadata Initiative (DCMI). В 1999 році DCMI рекомендувала набір з 15 елементів.

На погляд фахівців на сьогоднішній день Dublin Core являє собою найбільш розроблену і перспективну концепцію, що описує методи обробки електронних документів і може бути реально застосована для будь-яких цілей і типів документів.

Як показує накопичений досвід ведення інформаційної роботи, ведення винятково легального збору та опрацювання потрібної інформації дає добрі результати як в плані ваги добутих відомостей, так і в плані масштабності охоплення потрібних предметних галузей, а також за економією коштів на ведення інформаційної діяльності.

Весь процес збирання і обробки інформації можна поділити на такі етапи:

1. Етап *завчасної* обробки. Набір статистичних і довідкових даних про середовище, об'єкт, його першочергові та другорядні завдання.

2. Етап *попередньої* обробки. Ті самі дії, але прив'язані до конкретної дати та/або завдання. Саме на цьому етапі найдоцільніше використовувати зворотне планування.

3. Етап *безпосередньої* обробки. Є найважливішим і водночас найскладнішим, оскільки жорстко прив'язаний до часу, місця, умов та ресурсів.

4. Етап *перспективної* обробки. Робота з прогнозування змін у середовищі, завданнях та відповідне планування роботи об'єкту.

Всі обсяги інформації, які можуть бути використані для формування інформаційного масиву. Для формування і поповнення масиву можуть бути використані такі джерела інформації (див. мал. 5) [8]:

Подамо основні прийоми обробки інформації. Будь-яка інформація, що надходить, характеризується певним ступенем вірогідності, який, зокрема залежить від ступеня надійності джерела і того, відкіля те джерело її одержало.

Щоб висвітити такі показники, кожному зареєстрованому факт ставимо у відповідність спеціальну букво-цифрову оцінку, причому буквами позначають рівень надійності джерела, а цифрами – звідки взяті відомості.

Рівень надійності джерела прийнято кодувати так:

А – абсолютно надійний і компетентний;

Б – звичайно надійний;

В – не занадто надійний;

Г – ненадійний;

Д – невизначений.

Те, як це джерело одержало дані, що представляються, відзначають у такий спосіб:

1 – сам бачив;

2 – через посилання на інше надійне джерело;

3 – чутки тощо.

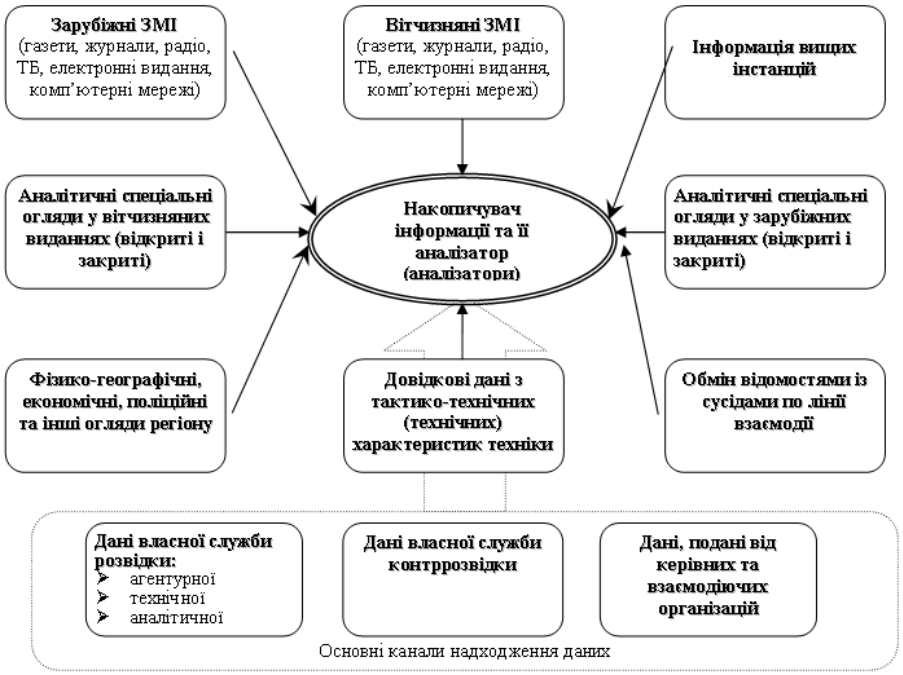


Рис. 5. Окремо виділені основні канали надходження інформації.

Ніколи не варто забувати, що надійне джерело (А) інколи здатне передати явну дезінформацію, а зовсім ненадійне (Г) – повідомити найцінніші дані. Тому двохзначковий індекс доцільно доповнити римською цифрою, що вказує на передбачувану вірогідність факту:

I – підтверджується іншими фактами;

II – ймовірно правдивий (3 до 1);

III – можливо правдивий (1 до 1);

IV – сумнівний (3 проти 1);

V – неправдоподібний;

VI – невизначаємо.

Маркірування ІІІ-Б2, приміром, означає, що фактура надана досить надійним інформатором (Б) зі слів знаючого людини (2) і можливо – «50 на 50» – правдива (ІІІ). За наявності яких-небудь сумнівів у вірогідності отриманих даних, їх корисно відкласти про запас (впорядковане архівування) у чеканні інших підтверджень чи спростувань.

Наступна таблиця показує основні взаємовідношення показників ймовірності та шансів: