БЕЗПЕКА ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

- ***П. Біленчук, А. Кофанов, О. Кобилянський, В. Міщенко***
  БЕЗПЕКА ІНФОРМАЦІЙНОЇ АНАЛІТИКИ: СТРАТЕГІЯ, ТАКТИКА, МИСТЕЦТВО, ТЕХНОЛОГІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський
  МІЖНАРОДНИЙ ТЕРОРИЗМ: КОНСОЛІДОВАНИЙ АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ
- П. Біленчук, А. Кофанов, О. Кобилянський
  ЗАПОБІГАННЯ, ПРОТИДІЯ, РОЗСЛІДУВАННЯ ТЕРОРИСТИЧНИХ АКТІВ: МІЖНАРОДНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ
- П. Біленчук, А. Кофанов, О. Кобилянський
  АНТИТЕРОРИСТИЧНІ СИЛИ, ЗАСОБИ, ТЕХНОЛОГІЇ БЕЗПЕКИ: КОНЦЕПТУАЛЬНІ ОСНОВИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ТЕРОРИЗМУ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Міщенко
  ІНФОРМАЦІЙНА АНАЛІТИКА В ЮРИСПРУДЕНЦІЇ: АВТОМАТИЗОВАНІ СИСТЕМИ І ТЕХНОЛОГІЇ
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Міщенко
  ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: УПРАВЛІННЯ, ПРАВО, ТЕХНОЛОГІЇ, БЕЗПЕКА
- П. Біленчук, А. Кофанов, О. Кобилянський, В. Міщенко, О. Самойленко
  ІНФОРМАЦІЙНІ ВІЙНИ: ІСТОРІЯ, СЬОГОДЕННЯ
- П. Біленчук, А. Кофанов, О. Кобилянський
  ВСЕСВІТНЄ ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ЄВРОПЕЙСЬКІ ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ, ТЕНДЕНЦІЇ, ТЕХНОЛОГІЇ

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

БЕЗПЕКА ІНФОРМАЦІЙНОЇ АНАЛІТИКИ:
СТРАТЕГІЯ, ТАКТИКА, МИСТЕЦТВО, ТЕХНОЛОГІЇ

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

- Серія „Людина, право, суспільство”
- Серія „Безпека людини, суспільства, держави”
- Серія „Міжнародна і вітчизняна злочинність”
- Серія „Міжнародне співробітництво”
- Серія „Криміналістична освіта XXI століття”
- Серія „Автоматизація, комп’ютеризація, інформатизація”
- Серія „Зброєзнавство і мисливствознавство”

Тел. 8 (067) 5738307
Тел./факс: (044) 468-31-21
E-mail: peregin@mail.ru

Навчальне видання

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

БЕЗПЕКА ІНФОРМАЦІЙНОЇ АНАЛІТИКИ:
СТРАТЕГІЯ, ТАКТИКА, МИСТЕЦТВО, ТЕХНОЛОГІЇ

Навчальний посібник

В авторській редакції

Підписано до друку 03.04.2009.
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 ІНСТИТУ ПІДГОТОВКИ
СЛІДЧИХ І КРИМІНАЛІСТІВ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ, БЕЗПЕКИ
ТА ІНФОРМАЦІЙНО-ПРАВОВИХ ТЕХНОЛОГІЙ

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

БЕЗПЕКА ІНФОРМАЦІЙНОЇ АНАЛІТИКИ:
СТРАТЕГІЯ, ТАКТИКА, МИСТЕЦТВО, ТЕХНОЛОГІЇ

Навчальний посібник

Серію засновано у 2000 році А.В. Кофановим

Київ 2009

УДК 007: [681.3+65.012.8]
ББК 73
Б 61

Схвалено і затвердженно та рекомендовано до друку кафедрою криміналістичної техніки ННІПСК КНУВС (протокол № 9 від 17.03.2009 року) та Вченою радою ННІПСК Київського національного університету внутрішніх справ (протокол № 7 від 03.04.2009 року).

Рецензенти:
Л.В. Борисова – кандидат юридичних наук, доцент
Л.О. Сидоренко – старший науковий співробітник НДЕКЦ УВС Черкаської області

Біленчук П.Д., Кофанов А.В., Кобилянський О.Л., Міщенко В.Б.
Б 61 Безпека інформаційної аналітики: стратегія, тактика, мистецтво, технології. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 68 с. – (Серія „Безпека людини, суспільства, держави").

У навчальному посібнику висвітлюються питання програмного і технічного забезпечення телекомунікаційного середовища, аналізуються потенційні ризики, загрози і небезпеки в кіберпросторі, дається характеристика злочинності в інформаційно-телекомунікаційній сфері.

Для студентів, викладачів, фахівців-практиків.

ББК 73

6.pdf.

163. Venture Impact 2004 Venture Capital Benefits to the US Economy // Report by National Venture Capital Association / www.nvca.org.

164. *WangM., PfleegerS., Adamson D., Bloom G, Butz W., FossumD., Gross M., KofnerA., Rippen H.* Technology Transfer of Federally Funded R&D: Perspectives from a Forum. – RAND Corporation, CF-187-OSTP, 2003.

165. *Wagner C, Brahmakulam /., Peterson D.J., Staheli L., Wong A.* U.S. Government Funding for Science and Technology Cooperation with Russia. – RAND Corporation, MR-1504-OSTP, 2002.

Waxman H. Politics and Science in the Bush Administration // US House of Representatives, August, 2003 / www.reform.house.gov/min.

Можливості аналізу та прогнозування розвитку ринків на основі патентної інформації // Стратегічна панорама. – 2002. – № 2. – С. 165-171.

148. *Цибульов П.М. Пирятинська С.Ф., Дмитрієва О.С.* Тенденції розвитку винахідницької діяльності за галузями економіки України // Науково-технічна інформація. – 2000. – № 1.

149. *Цибульов П.М., Пирятинська С.Ф., Дмитрієва О.С., Пархоменко О.В., Овчарик В.Е.* Можливості аналізу та прогнозування розвитку ринків на основі патентної інформації // Труди другої міжнар. наук.-практ. конф. „Виставкова діяльність України". – К., УкрІНТЕІ. 2001.

150. *Цибульов П.М., Пирятинсъка С.Ф., Дмитрієва О.С.* та інші. Тенденції розвитку винахідницької діяльності за галузями економіки України // Науково-технічна інформація. – 2000. – № 1. – С. 30-37.

151. *Цихан Т.В.* О концепции технологических укладов и приоритетах инновационного развития Украины // Теория и практика управления. – 2005. – №1. – С. 33-46.

68. *Шеннон К.* Работа по теории информации и кибернетики. – М: Изд-во иностранной литературы, 1963. – 19 с.

152. *Штарков СВ.* Методологические основы создания и функционирования системы информационной и аналитической поддержки органов власти и управления // Научно-техническая информация. – 1996. – № 3.

153. *Щекин Г.В.* Организация и психология управления персоналом: Учеб.-метод, пособие. – К.: МАУП, 2002. – 832 с.

154. *Юфрякова Н.К.* Тенденции изменения основных показателей патентной активности в капиталистических странах. – М.: ВИНИТИ, 1990. – 91 с.

155. *Янюк Б.И.* Организация и методика подготовки обзорно-аналитических документов. – М.: ИАКИР, 1983. – 63 с.

156. *Ядов В.А.* Стратегия социологического исследования. Описание, объяснение, понимание социальной реальности. – М: Добросвет. – 596 с.

157. Anton P.S., Silberglitt R., Schneider J. The Global Technology Revolution: Bio/ Nano/Materials Trends and Their Synergies with Information Technology by 2015.- RAND Corporation, MR-1307-NIC, 2001.

158. *Larson E., Brahmakulam I.* Building a New Foundation for Innovation: Results of a Workshop for the National Science. – RAND Corporation, MR-1534-NSF, 2002.

159. Patents and sectors economy. Connection between the international patent classification and systems of sectors of economy / S/Greif // WP 1, V; 14, № 4, 1992, p. 229-245.

160. *Popper S.W., Wagner C.S.* New Foundations for Growth: The US Innovation System Today and Tomorrow. – RAND Corporation, MR-1338.0-OSTP, 2002.

161. The Advanced Technology Program: Assessing Outcomes // Board on Science, Technology and Economic Policy, National Academies, 2002.

162. Towards a European Research Area // European Commission Report COM (2000) 6, January 18, 2000/ europa.en.int/com/research/era/pdf/com2000-

ЗМІСТ

ПЕРЕДМОВА

Захист 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. В нашому дослідженні – під безпекою інформації будемо розуміти всі заходи, спрямовані на збереження режиму таємності, протидію чужим розвідкам, збереження інформаційних ресурсів від знищення, спотворення, викрадення, перехоплення, несанкціонованого копіювання внаслідок умисних зловмисних дій, халатності, помилок персоналу, технічних несправностей і т.д. [1, с. 2-6].

Подібно до того, як будова складається з окремих цеглин, а живий організм – з клітин, так загальнодержавна безпека формується із багатьох складників, різних за своїм якісним і кількісним станом, об'єднаних єдиною формотворчою ідеєю – убезпечення держави від внутрішніх та зовнішніх загроз. 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.

Аналіз вітчизняної та зарубіжної літератури 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;

– 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

Доп. „Бизнес – пресса", 2000. – 326 с.

128. *Старіш О.Т.* Систематологія. Підручник. – К.: Центр навчальної літератури, 2005. – 232 с.

129. *Старбинский Э.Е.* Интеллектуальный капитал предпринимателя. – М.: 1996. – 301 с.

130. *Сухоруков А.І.* Пріоритети інвестування національного технологічного розвитку // Стратегічна панорама. – 2003. – № 1.

131. *Сухоруков А.І.* Трансфер економічних криз як причина недосконалих циклів // Стратегічна панорама. – 2004. – № 2.

132. *Сурми Ю.П.* Методология анализа ситуаций (Case study Metod) – К.: Центр-инновации и развития, 1999. – 99 с.

133. *Сурми Ю.П.* Проектировочная деятельность в области социальных технологий // Гуманитарный журнал. – 1999. – № 4. – С. 88-98.

134. *Сурмі Ю.П.* Аналітична діяльність у державному управлінні: технологічний аспект // Актуальні проблеми державного управління. – Дніпропетровськ: ДФ АУДУ. – 2000. С. 27-48.

135. *Сурмі Ю.П.* Аналітична діяльність. Посібник для аналітика неприбуткової організації. Центр інноваційного розвитку, 2002. – 95 с.

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

137. *Сколенко А.К.* Глобальные резервы роста. – К.: „Интеллект", 2002. – 427 с.

138. *Скурихин В.И., Гуриев М.А.* Темпометрическая модель для выбора решений в системах оперативного управления // Управляющие системы и машины. – 1983. – № 4. – С. 9-14.

139. *Танатар Н.* Информационно-аналитические системы оценки состояние науки // Наука та наукознавство. – 1996. – № 3-4. С. 124-132.

140. *Тити Б.* Пути к информационному обществу. Сценарий и почерки для экономики и для общества. – М.: Наука, 1993. – 182 с.

141. *Тимофеева Н.И.* Методы обработки патентной информации при изучении тенденций развития техники. – М.: ВНИИПИ, 1989. – 139 с.

142. Управление инновациями / Академия народного хозяйства при Правительстве Российской Федерации. – М.: Центр коммерческих технологий, 1999. – 246 с.

143. Управленческое консультирование: пер. с англ – М.: СП „Интерэкспорт", 1992. – 319 с.

144. Успехи Японии в развитии новых технологий // Экспресс-информация. Информатика. – М: ВИНИТИ, 1995. – 38 с.

145. *Ходаківськш Є.І., Богоявленська Ю.В.* Економіка та менеджмент праці (праксіологічний аспект): Навчальний посібник. – Житомир: ЖДТУ, 2004. – 378 с.

146. *Цибульов П.М., Пархоменко В.Д.* Правове регулювання у сфері науково-технічної інформації з позиції авторського права // Науково-технічна інформація. – 2002. – № 4. С. 3-6.

147. *Цибульов П.М., Пирятинська С.Ф., Дмитрієва О.С, Пархоменко О.В.*

107. *Пирятинська С.Ф., Дмитрієва О.С, Пархоменко О.В.* Винахідницька діяльність в Україні. – К.: УкрІНТЕІ, 2002. – 14 с.

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

109. Перспективи інноваційного розвитку України. – К.: Альтерпрес, 2002.

110. Послання Президента України. Про внутрішнє і зовнішнє становище України у 2002 році. – К.: Держкомстат України. – 2003. – 477 с.

111. Прогнозування розвитку технологій в Україні. – К.: Парламентське видавництво, 1998. – 134 с.

112. Проблемы организации, управления и доступности научной информации в Японии // Экспресс-информация. Информатика. М.: ВИНИТИ, 1995. – № 19. – 55 с.

113. *Райков А.Н.* Какая информация нужна руководителю? // Научно-техническая информация. – 2003. – №5. – 1-6.

114. *Рассадовский В.А.* Право в системе научно-технической информации // Правоведение. – 1984. – № 5. – С. 1-83.

115. Річний звіт Державного департаменту інтелектуальної власності за 2003 р. // Державний департамент інтелектуальної власності. – 2004.

116. *Рижих В.Н.* Стратегія і тактика науково-технічного і економічного розвитку України. – Харків: Прапор, 1998. – 384 с.

117. *Рокицкая Э.В.* Интеллектуальное преобразование информации в управлении деятельностью организации // Научно-техническая информация. – 2003. – №5. Сер.1. – С. 7-11.

118. *Романець В. А.* Психологія творчості: Навч. посібник. 3-тє вид. – К.: Либідь, 2004. – 288 с.

119. *Седов Е.А.* Информационные критерии упорядоченности и сложности организации структуры систем // Системная концепция информационных процессов. – М., 1998. – 222 с.

120. *Семиноженко В.П.,* Україна: Шлях до постіндустріальної цивілізації. – Харків: Константа, 2005. – 360 с.

121. *Семиноженко В.П.* Точка зору. – К.: УТТ „Гопак", 2005. – 304 с.

122. *Семенюк Э.П.* Глобализация и социальная роль информации // Научно-техническая информация. – 2003. – № 1. Сер.1. – С. 1-10.

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

124. *Семенюк Э.П.* Информатика и современные проблемы философии науки и техники / Научно-техническая информация. – 2005. – № 1. Сер. 1. – С. 1-10.

125. *Соснін О.* Політико-правові аспекти розвитку національної системи науково-технічної інформації // Держава і право. – 2000. – № 12. – С. 190-197.

126. *Соловьев. В.П.* Проблемы формирования организационно-правового механизма инновационного развития экономики. Под редакцией д.э.н. Б.А. Малицкого. – К.: Наука, 1996.– 69 с.

127. *Спицнадель В.Н.* Основы системного анализа: Учебное пособие. – М.:

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 оптимізації застосування сил і засобів забезпечення безпеки інформації має бути комплексним і включати в себе як адміністративно-організаційні, так і суто 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.

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 у будь-якому разі:

– аналіз загрози для інформації на даному об'єкту;

– оцінка ймовірності виникнення того чи іншого виду загрози та можливі втрати в разі "поразки";

– 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 окремого до загального) [2,3]:

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

– що саме з 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 володіти великою кількістю впорядкованої інформації з усіма наслідками. Основні шляхи надходження інформації і способи її впорядкування проаналізовано у [4].

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 [5].) Інакше кажучи, потрібен типовий алгоритм роботи посадових осіб та підрозділів при формуванні, експлуатації та супроводженні системи

забезпечення безпеки.

Необхідно зазначити, що, оскільки питання проблеми прийняття рішення, процесу збору, аналізу, обробки та зберігання інформації, збереження таємниці, захисту інформаційних ресурсів від ворожих посягань постали ще „на світанку цивілізації", то і знайшли вони свої наочні, вичерпні і дохідливі відображення у історичних, філософських та культурних пам'ятках минулого.

Наприклад, Сунь-Цзи, військовий теоретик Стародавнього Китаю, у своїх афоризмах досить дохідливо змалював основні закони, процеси та дії, які має обов'язково брати до уваги полководець будь-якого рівня [6]. Так, в основу війни та військових дій Сунь-Цзи кладе п'ять основних явищ: 1) *Шлях* (кажучи по-сучасному, *Події*), 2) *Небо*, або *Час,* 3) *Земля,* або *Простір*, 4) *Полководець*, або *Суб'єкт протиборства*, 5) *Закон* або *Аналіз* [6, с. 35-36, 75-85]. Кожен з цих елементів породжує наступний і, у свою чергу, сам народжується із попереднього. Звідси слідує така заповідь: „Керуй супротивником сам і не давай йому керувати собою" [6, с. 260]. Для цього необхідно дотримуватися іншої настанови: „…Якщо знаєш його (тобто супротивника) і знаєш себе, перемога недалека; якщо знаєш при цьому ще і Небо і знаєш Землю (тобто часові і просторові обмеження у даній ситуації), перемога забезпечена цілковито" [6, с. 60].

Сучасний дослідник прадавньої історії України Братко-Кутинський розповідає, зокрема, про багатий світ розмаїтих символів, якими наші предки зображували закони та процеси світобудови. І кожен із цих символів живе на рівні підсвідомості кожної освіченої людини, слугуючи при цьому своєрідним життєвим дороговказом [7]. На думку авторів, цими потужними набутками людства, адаптованими до сучасних умов, не можна не скористатися [8-16].

Тому в даному дослідженні автори аналізують новітні ідеї і концепції, які торкаються інформаційно-аналітичних систем і технологій, висвітлюють реальний стан потенційних загроз, що існують сьогодні у кіберпросторі, а також розкривають стан сучасної кіберзлочинності.

Література

1. *Термінологія в галузі захист*у інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 // К.: ДСТЗІ СБ України. – ст.ст. 4.1.2, 4.1.4-4.1.7, 4.3.7.

2. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты / К.: ООО «ТИД ДС», 2001. – 688 с.

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

4. *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.

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

6. *Сунь-Цзы* Трактаты о военном искусстве / Сунь-Цзы, У-Цзы; Пер. с

Труды IX Междунар. научно-практической конф. „Построение информационного общества: ресурсы и технологи". – К.: УкрІНТЕІ. – 2002. – С. 3-11.

95. *Пархоменко В.Д., Пархоменко О.В.* Науково-технічна інформація і суспільство // Науково-технічна інформація. – 2002. – № 3. – С. 62-64.

96. *Пархоменко В.Д., Гончаренко А.П, Пархоменко О.В.* Підходи до формування і використання національних інформаційних ресурсів науково-технічної діяльності // Науково-технічна інформація. – 2002. – № 3. – С. 40-44.

97. *Пархоменко В.Д., Пархоменко О.В.* Винахідницька діяльність за галузями економіки і науковий потенціал України // Науково-технічна інформація. – 2001. – №4. – С. 27-32.

98. *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.

99. *Пархоменко В.Д., Пархоменко О.В.* Научно-методологические основы
информационно-аналитического обеспечения принятия решения // Матеріали II Міжнар. науково-практичної конф. „Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління". – К.: УкрІНТЕІ. – 2001. – С. 26-35.

100. *Пархоменко В.Д., Калитич Г.И., Гончаренко А.П., Саверченко Е.А., Пархоменко А.В.* Подходы к управлению процессом создания и использования национальных ресурсов научно-технической деятельности // Тр. IX Меж-дунар. науч.-техн. конф. „Построение информационного общества: ресурсы и технологи". – К.: УкрИНТЭИ. – 2002. – С. 3-12.

101. *Пархоменко О.В.* Патентна результативність науково-технічного потенціалу в промисловості України // Статистика України. – 2002. – № 3. – С. 49-56.

102. *Пархоменко О.В.* Інформаційно-аналітична складова оцінки патентної результативності науково-технічного потенціалу в промисловості України // Труди III Міжнарод. наук.-практ. конф. „Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління". – К.: УкрШТЕІ. 2002. – С. 152-155.

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

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

105. *Пархоменко О.В., Гордієнко Я.Я., Лисенко М.Є.* Нові підходи до оцінювання ефективності результатів науково-дослідних та дослідно-конструкторських робіт // Науково-технічна інформація. – 2002. – № 1. – С. 21-23.

106. *Пуанкаре А.* О науке: Пер. с франц., 2-е изд. – М: Наука, 1990. – 736 с.

82. Науково-технічна політика Європейського Союзу: досягнення, проблеми, перспективи / І.Ю. Єгоров, В.І.Карпов, К.С. Степанкевич, К.А. Чекмарьов /Під заг. ред. А.О. Чекмарьова. – К.: Національна бібліотека України ім. В.І.Вернадського, 2004. – 147 с.

83. *Нельсон, Боб* и *Економи Пишер.* Умение управлять для „чайников": Пер. с англ. – К.: Диалектика, 1997. – 336 с.

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

85. Обґрунтування інноваційної моделі структурної перебудови економіки України / Манецький Б.А., Попович О.С., Соловйов В.П., Артемова В.Я., Єгоров І.Ю. – К: ЦДНТ потенціалу та історії науки ім. Г.М. Доброва НАНУ, 2005. – 64 с.

86. Обеспечение деловой информации малых и средних предприятий в Китае: применение маркетинговых моделей // Экспресс-информация. Информатика. М.: ВИНИТИ, 1995. – № 16. – 46 с.

87. *Партико З.П.* Образна концепція теорії інформації. – Львів: Видавничий центр ДНУ ім. Івана Франка, 2001. – 132 с.

88. *Пархоменко А.В.* Патентная статистика и научно-технический потенциал – индикаторы состояния инновационного курса развития // Труды IX Международной научно-технической конференции „Построение информационного общества: ресурсы и технологи". – К.: УкрІНТЕІ. 2002. – С. 99-105.

89. *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.

90. *Пархоменко А.В.* Патентная статистика и научно-технический потенциал // Тр. IX Междунар. науч.-практ. конф. „Построение информационного общества: ресурсы и технологи". – К.: УкрИНТЭИ. – 2002. – С. 99-105.

91. *Пархоменко В.Д., Гончаренко А.П., Пархоменко А.В.* Проблемы развития системы научно-технической информации на Украине. Материалы VI Международной конференции „Информационное общество, интенсивная обработка информации, информационные технологи". – М.: ВИНИТИ. 2002. – С. 272-274.

92. *Пархоменко В.Д., Пархоменко А.В.* Информационно-методическое обеспечение анализа научно-технической деятельности // Georgian Engineering News, 2001. – №4. – С. 34-38.

93. *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.

94. *Пархоменко В.Д., Калитич Г.И., Гончаренко А.П, Саверченко Е.А., Пархоменко А.В.* Подходы к управлению процессов создания и использования национальных информационных ресурсов научно-технической деятельности //

кит., предисл. и коммент. Н.И. Конрада.– М.: ООО "Издательство АСТ"; СПб.: Terra Fantastica, 2002. – 558 с.

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

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

9. Криміналістика. Підручник. / За ред. П.Д. Біленчук. – Київ: Атіка, 2001. – 544 с.

10. *Біленчук П.Д., Толочко О.Я., Кофанов А.В., Кобилянський О.Л.* Україна-Франція: договірні взаємовідносини у гуманітарній та правовій сферах. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 81 с. – (Серія „Міжнародне співробітництво").

11. Біленчук П.Д., Лютий І.О. Банківське право: українське та європейське. Навчальний посібник. – К., 1999. – 340 с.

12. *Биленчук П.Д., Кофанов А.В.* Транснациональная преступность: состояние и трансформация. Учебное пособие. – К., 1999. – 272 с.

13. *Биленчук П.Д., Биленчук Д.П.* Страхове право. Пыдручник. – К., 1999. – 368 с.

14. *Біленчук П.Д., Кофанов А.В., Сулява О.Ф.* Балістика: криміналістичне вогнестрільне зброєзнавство. Підручник. – К., 2003. – 384 с.

15. *Біленчук П.Д., Кофанов А.В., Сулява О.Ф.* Зброєзнавство: правові основи обігу зброї. Монографія. – К., 2004. – 464 с.

16. *Біленчук П.Д.* та ін. Комп'ютерна злочинність: суперхакери і кіберполіцейські. Навчальний посібник. – К., 2002. – 240 с.

Петро Біленчук

РОЗДІЛ 1.
ПРОГРАМНЕ І ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ТЕЛЕКОМУНІКАЦІЙ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

1.1. Телекомунікаційне середовище ІАС

Структура телекомунікаційного середовища передбачає наявність центрального телекомунікаційного середовища, що формує базову мережу, згідно з „Основними вимогами до Національної програми інформатизації".

Окремі інформаційні системи відрізняються за масштабом та структурою, та пов'язані між собою за допомогою телекомунікаційного середовища, що побудовано навколо центральної частини.

Телекомунікаційне середовище формується за допомогою ліній безпосереднього з'єднання, Frame Relay, ISDN та комутованих телефонних каналів.

Телекомунікаційне середовище в межах відомства (корпорації) передбачає наявність єдиного контрольованого шлюзу до мережі Інтернет.

Безвідмовне функціонування середовища забезпечується комплексними засобами підвищення надійності функціонування.

На канальному рівні безвідмовність функціонування забезпечується наявністю двох точок з'єднань кожного вузла з телекомунікаційним середовищем.

Окремі інформаційні системи використовують пару каналів доступу до телекомунікаційного середовища, один з яких виступає основним, а інший – резервним. Основний функціонує за допомогою ліній безпосереднього з'єднання (БЗ), а резервний використовує комутовані телефонні канали. Переключення між основним та резервним каналами виконується автоматично в разі виходу з ладу основного.

Безвідмовність у функціонуванні активного обладнання забезпечується використанням пристроїв безвідмовного електроживлення.

Інформаційне середовище, з точки зору системи маршрутизації, являє собою автономну систему, де на центральному рівні використовується OSPF протокол, в середині окремих зон – RIP-2, та на кордоні BGP-4.

Шлюз до глобальних інформаційних мереж виконується за допомогою мережі Інтернет. На кордоні між інформаційною мережею та мережею Інтернет використовується система захисту від несанкціонованого доступу Fire Wall.

Забезпечення захисту інформації в розгалуженому телекомунікаційному середовищі здійснюється за допомогою комплексних дій, що зорієнтовані на облік користувачів інформаційної системи, та регламентацію доступу до окремих ресурсів мережі.

В мережі використовується пул IP адрес, що не використовується в глобальних комп'ютерних мережах.

Всі випадки встановлення безпосередніх контактів між окремими абонентами в середині та ззовні мережі виконуються виключно за допомогою системи Network Address Translation (NAT).

Весь інший інформаційний обмін передбачає використання проміжних

2010 року. – Трудова Україна, К.: – 2005. – 60 с.

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

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

65. *Кринецкий И.И.* Основы научных исследований. – К. – Одесса: Вища школа, 1981. – 208 с.

66. *Керол Г.В.* Оцінювання. – К.: Видавництво Соломії Павличко „Основи", 2000. – 671 с.

67. *Кутель С.А., Зусъман О.М., Минкина В.А.* Информационное поведение ученых – представителей научной элиты Санкт-Петербурга // Научно-техническая информация. – 1995. – № 7. Сер.1. – С. 12-18.

68. *Кучерявий 1. Т., Клепіков 0.1.* Творчість – основа розвитку потенційних джерел особистості. – К.: Вища школа, 2000. – 288 с.

69. *Кузык В.Н., Яковец Ю.В.* Россия – 2050. Стратегия инновационного прорыва. – М.: Экономика, 2004. – 632 с.

70. *Кутель С.А., Зусъман О.М., Минкина В.А.* Информационное поведение ученых – представителей научной элиты Санкт-Петербурга // Научно-техническая информация. – 1995. – № 7. Сер.1. – С. 12-18.

71. *Кринецкий И.И.* Основы научных исследований. – К. – Одесса: Вища школа, 1981. – 208 с.

72. *Лобанов С.Г., Селиванов А.И.* Об информационно-аналитическом обеспечении управления в современной России // НТИ. Сер. 1.– 2005. – №5. – С. 1-6.

73. *Лобанов Е.Г., Селиванов А.И.* Об информационно-аналитическом обеспечении управления в современной России // НТИ. Сер.1. Орг. и методика информ. работы. – 2005.– № 5. – С. 1-6.

74. *Мартынов А.С., Артюхов В.В., Виноградов ВТ.* „Проект НЕФ. Сохранение биоразнообразия // Использование и охрана природных ресурсов в России". – 2000. – № 8. – С. 83-95.

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

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

77. *Марчук Є.К.* Стратегічна організація суспільства – рух на випередження // Стратегічна панорама. – 1999. № 4. – С. 13-17.

78. Методологические вопросы науковедения / Оноприенко В.И., Малицкий Б.А., Рыжкин Л.В. и др. – К.: УкрИНТЭИ, 2001. – 327 с.

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

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

81. *Монро М.Ю.* Как стать руководителем. – К.: Фарес, 2000. – 208 с.

Геєць В.М. // Кінах А.К., Семиноженко В.П. – К.: Знання України, 2002. – 336 с.

44. Интеллектуальная собственность в Украине: правовые основы и практика / Довгий С.А., Дробьязко В.С., Жаров В.А. и др.: ИнЮре, 1999. – 492 с.

45. Информационное пространство новых независимых государств / Арский Ю.М., Гиляровский С.С., Клещев Н.Г. и др. – М., 2000. – 200 с.

46. Информатика и культура / Отв. ред. И.С. Ладенко. – Новосибирск: Наука, – 1990. – 233 с.

47. Информационные ресурсы для обеспечения научной и учебной деятельности вуза. Сулименко СИ., Сиротина М.А., Мещерякова Т.В. и др. – // Информационные ресурсы России. – 2001. – № 2 (57). – С. 26-28.

48. *Камишин В.В., Пархоменко О.В., Одарич ОМ.* Формування системи критеріїв оцінки науково-технічних напрямів та програм методом „Дельфі" // Науково-технічна інформація. – 2001. – № 3. – С. 34-38.

49. *Каныгин Ю.М., Ермошенко КН., Калитич Г.И., Донченко Е.А.* Интеллект народа информатика и когнитивная этносоциология. – К.: УкрИНТЭИ, 1997. – 49 с.

50. *Каныгин Ю.М., Калитич Г.И.* Основы теоретической информатики. – К.: Наукова думка, 1990. – 229 с.

51. *Калитич Г.И., Джелали В.В., Андрогцук Г.А.* Идеи должны работать. – К.: УкрИНТЭИ, 1990. – 62 с.

52. *Корсунський С.В.* Досвід реформування системи державного управління науковими дослідженнями та їх організації в Ізраїлі. – У сб.: Розвиток науки та науково-технічного потенціалу в Україні та за кордоном, 1996, Вип. 3(11). – С. 28-32.

53. *Книга А.* Наука интернациональная // Наука о науке. – М.: Прогресс. – 1966. – С. 132-148.

54. *Корсунсъкий С.В.* Трансфер технологій у США. – К.: Укр.НТЕІ, 2005. – 148 с.

55. Концепція соціально-економічного розвитку України на період до 2010 року. – Трудова Україна. – К.: – 2005. – 60 с.

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

57. *Колесников А., Кузнецов Ю.* Анализ патентной статистики по фонду США // Интеллектуальная собственность. – 1997. – № 7. – С. 24-31.

58. *Козлов В.С., Щеглов В.П.* Справочно-информационное обеспечение / руководящих работников. – М.: ИПКИР, 1983. – 63 с.

59. *Корсунський С.В.* Покласти край атмосфері „похорон" науки // Дзеркало тижня. – 2002. – 22-28 червня.

60. *Корсунський СВ.* Науково-технологічна сфера як ключовий елемент розвитку економіки США // Науково-технічна інформація. – 2003. – №3. – С. 16-20.

61. *Корсунський С.В.* Економічна політика США на сучасному етапі // Науково-технічна інформація. – 2004. – № 2.– С. 11-14.

62. Концепція соціально-економічного розвитку України на період до

серверів, таких як SMTP, Proxy, Socks та ін.

Бази даних користувачів інформаційної системи підтримуються за допомогою X.500 та RADIUS сумісних систем.

Пасивні компоненти телекомунікаційного середовища.

Телекомунікаційне середовище ґрунтується на лінійних спорудах республіканської мережі передачі даних (РСПД), каналах КиївЕлектроЗв'язку та "УкрТелеком".

Активними компонентами телекомунікаційного середовища є модеми для виділених та комутованих ліній, сервери доступу та маршрутизатори виробництва RAD Data Comm., Bay Networks та інших всесвітньо відомих виробників.

Модеми виробництва RAD Data Comm. забезпечують високу швидкість з'єднання при використанні однією пари дротів. Система кодування 2B1Q дозволяє використовувати навіть канали з високим рівнем перешкод.

Сервери доступу родини MBE того самого виробника відомі своїми широкими функціональними можливостями. Серед найважливіших можна навести наявність системи захисту FireWall, підтримка протоколів аутентифікації PAP/CHAP, трансляція IP адрес, використання стандартних протоколів, використання системи аутентифікації RADIUS.

Наявність в сервері доступу двох каналів з'єднання з телекомунікаційним середовищем дозволяє в реальному часі виконувати переключення з основного каналу на резервний, в разі виходу з ладу основного.

Маршрутизатори виробництва BAY Networks являють собою оптимальне рішення з точки зору функціональність/вартість. Модульна конструкція цих пристроїв та можливість стикування дозволяють вважати їх найбільш придатними для послідуючого масштабування інформаційної системи.

Масштабування інформаційної системи виконується доукомплектацією маршрутизаторів додатковими модулями підтримки телекомунікаційного середовища та додатковими пристроями в стеках.

1.1.1. Загальна структура

Засоби інформатизації:
– електронні обчислювальні машини;
– програмне, забезпечення;
– математичне, забезпечення;
– лінгвістичне та інше забезпечення;
– інформаційні системи або їх окремі елементи;
– інформаційні мережі і мережі зв'язку.

1.1.2. Принципи створення технічного забезпечення ІАС

Вибір структури та побудова технічного забезпечення ІАС здійснюється згідно з такими принципами:

– забезпечення структурно-функціональної побудови ІАС, орієнтованої на створення територіально розгалуженої комп'ютерної мережі, що охоплює всіх користувачів ІАС. Виходячи з цього, комунікаційне обладнання повинно забезпечувати можливість віддаленого доступу в синхронному та

асинхронному режимах до інформаційних ресурсів ЛОМ;

– використання системного підходу при обранні технічних та технологічних рішень;

– впровадження тільки найбільш сучасних технічних та технологічних рішень в галузі створення інформаційних систем;

– найбільш повне використання наявного обладнання, що є в органах державної влади для створення технічної бази ІАС;

– відкритість та нарощуваність архітектури;

– дотримання вимог захисту інформації;

– переважна комплектація мережевого обладнання за принципом "від одного виробника" для усунення проблем взаємної сумісності;

– відповідальність виконавців проекту створення ІАС за довгострокове технічне обслуговування (гарантійне та післягарантійне), авторське супроводження та вдосконалення ІАС;

– безпека, нешкідливість та комфортність користування системою, дотримання встановлених ергономічних вимог та норм;

– достатня гнучкість та налагоджуваність елементів системи;

– забезпечення достатньої відмовостійкості найбільш важливих складових частин та системи в цілому.

1.1.3. Принципи створення програмного забезпечення ІАС

Вибір структури та побудова програмного забезпечення ІАС здійснюється згідно з такими принципами:

– реалізація переваг архітектури клієнт/сервер при побудові локальних комп'ютерних мереж ІАС;

– використання системного підходу при обранні технологічних рішень;

– впровадження тільки найбільш сучасних рішень при виборі програмного забезпечення;

– найбільш повне використання наявного ліцензійного програмного забезпечення, що є в органах державної влади для створення технічної бази ІАС;

– відкритість та нарощуваність архітектури;

– дотримання вимог захисту інформації;

– обґрунтований компроміс між універсальністю та спеціалізованістю рішень, покладених в основу побудови системи в частині вибору між використанням загального та прикладного програмного забезпечення;

– використання в системі "доброзичливого" інтерфейсу користувача для забезпечення можливості самостійного опанування знаннями та навичками використання системи;

– посилення ролі електронних носіїв інформації та поступовий перехід, де це можливо та доцільно, до безпаперової технології обміну інформацією в документообігу ІАС;

– достатньо низька вартість реалізації та експлуатації програмного забезпечення;

– можливість масштабування від локальної до корпоративної мереж;

– можливість централізованого оновлення, встановлення і

25. *Винер Н.* Кибернетика или управление и связь в животном и машине. – М.: Наука, 1983. – 343 с.

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

27. *Гальчинський А. С, Геєць В.М., Семиноженко В.П.* Україна: наука та технологічний розвиток. – К.: Оранта, 1987. – 67 с.

28. *Гаше-Сархане.* Проблеми розвитку-інформаційного ринку Латвії // Науково-технічна інформація. – 2000. – № 4.

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

30. *Гендина Н.И.* Повышение информационной культуры потребителей информации, как условие успеха информатизации рынка // Информационные ресурсы России. – 2001. – № 2. – С. 22-25.

31. *Григорьев Э.П., Комаров А.С.* Экспертный потенциал российского капитала: стратегическая роль, финансовая база, методология оценки // Научно-техническая информация. – 2001. – № 2. Сер.1. – С. 1-19.

32. *Григорьев Э.П., Жирков О.А. Орфеев Ю.В.* и др. Телевизионно-компьютерные средства проектирования и управления в строительстве. – М.: Стройиздат, 1993. – 360 с.

33. *Григорьев Э.П.* Концептуальная основа синтеза альтернативных решений // Информатика и вычислительная техника. – 1997. – № 1. – С. 78-82.

34. *Григорьев Э.П.* Теория и практика машинного проектирования объектов строительства. – М.: Стройиздат, 1974. – 208 с.

35. *Громов Г.Р.* Национальные информационные ресурсы: проблемы промышленной эксплуатации. – М: Наука, 1985. – 240 с.

36. *Ж. Чень.* Восьма стадія управління інформацією: управління інформаційними ресурсами і управління знаннями, адміністратор інформації і адміністратор знань // Міжнародний форум інформації і документації. – 1998. – № 3 (т. 23). – С 15-19.

37. Земля в лихорадке. Аргументы и факты в Украине, 2005, № 22.

38. *Зербіно Д.* Наукова школа: лідер і учні, Львів: „Євро світ", 2002. – 201 с.

39. *Дегтярев К.Ю., Ухин М.Ю., Колпаков Ю.А., Яблонский В.Б., Терещенко С.С.* Корпоративные системы управления: информационный аспект // НТИ, Сер.1. – 2005. – №5. – С. 7-12.

40. Державне управління: теорія і практика. НАН України, інститут держави і права ім. В.М. Корецького за загальною редакцією д.ю.н., проф. Авер'янова В.Б. – К.: Юрінком Інтер, 1998. – 432 с.

41. *Доброе Г.М., Задорожный Э.М., Щедрина Т.И.* Управление эффективностью научной деятельности. – К.: Наукова думка, 1978. – 237 с.

42. *Дротянко Л.Г.* Фундаментальне та прикладне знання як соціокультурна та праксеологічна проблема: Монографія. – К.: Четверта хвиля, 1998. – 180 с.

43. Інноваційна стратегія українських реформ / Гальчинський А.С.,

6. *Анохин П.К.* Избранные труды. Философские аспекты теории функциональных систем. – М: Наука, 1978. – 70 с.

7. *Анохин П.К.* Принципы системной организации функций. – М: Наука, 1973. – 190 с.

8. *Анохин П.К* Избранные труды. Кибернетика функциональных систем. Под общей редакцией академика РАМН Судакова К.В. – М: Медицина, 1998. – 247 с.

9. *Баранов О.А.* Інформаційне право України, стан, проблеми, перспективи. – К.: Видавничий дім „Софт Прес", 2005. – 316 с.

10. *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).

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

12. *Бегиелев С.Д., Гурвич Ф.Г.* Математико-статистические методы экспертных оценок. – М.; Статистика, 1980. – 320 с.

13. „Большая Советская Энциклопедия", главный редактор Прохоров А.М., 3-е изд. – М.: „Советская Энциклопедия", 1977, т. 21. – 624 с.

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

15. *Берна Дж.* Наука в истории общества. Пер. с англ. – М.: Изд-во иностр. литературы, 1956. – 735 с.

16. *Браун М.* Посібник з аналізу державної політики. Пер. з англ. – К.: Основи. – 2002. – 243 с.

17. *Брежнєва В.В.* Информационная культура специалиста и проблемы ее формирования // Современное библиотечно-информационное образование: учебные тетради – 1999. Вып.3. – С. 121-136.

18. *Брижков В.М., Базанов Ю.К., Харченко Л.С.* Ліцензування прав на інформаційні ресурси. – К.: Національне агентство з питань інформатизації при Президентові України, 1997. – 132 с.

19. *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.

20. Введение в теорию управления корпорацией / В.А. Панков, А.Л. Еськов, СВ. Ковалевский, С.Н. Петрусевич. – Краматорск. 1999. – 69 с.

21. *Веймер Д.Л., Вайтінг Е.Р.* Аналіз політики: концепція і практика: Пер. з англ. – К.: Основи, 1988. – 654 с.

22. *Венгеров А.Б.* Право и информационное обеспечение АСУ // „Сов.госуд. и право". – 1972. – № 8. – С. 36-38.

23. *Волькенштейн М.В.* Энтропия и информация. – М., 1986. – 46 с.

24. Вопросы информационного обеспечения научно-технического развития Республики Казахстан. Сб. науч. тр. – Алма-Аты: КазгосИНТИ, 2000. – 299 с.

відслідковування версійності;

– можливість створення і використання репозиторію типових програмних рішень.

Програмне забезпечення (ПЗ) ІАС призначається для забезпечення ефективного функціонування (та розробки) функціональних задач користувачів ІАС на принципах спільного використання (розподілу) ресурсів системи (апаратних, програмних та інформаційних).

У складі ПЗ ІАС виділено чотири класи компонентів:

– мережеві операційні системи, операційні системи клієнтів, засоби віддаленої та міжмережевої взаємодії;

– системи керування розподіленими базами даних, засоби аналізу даних та засоби розробки прикладних програм;

– географічні інформаційні системи;

– офісні та сервісні системи.

Головною мережевою операційною системою ІАС може бути, наприклад, Novell NetWare 4.11, що входить до складу групи мережевих засобів IntraNetWare і забезпечує функціонування ІАС на принципах інтрамереж.

Корпорація Novell пропонує нову прикладну програму для інтрамереж – GroupWise 5, що поєднує у собі розширену систему електронної пошти та засоби керування електронними документами для комунікацій та в інтрамережах та Internet.

Як операційну систему клієнтів пропонується використовувати Windows.

Як засіб доступу до ІАС віддалених користувачів пропонується використання продукту NetWare Connect 2.

Для забезпечення міжмережевого обміну можливе використання апаратно-програмних засобів 3ComNetbuilder 2, RemoutOffice та Extended WAN Software, або програмних продуктів з аналогічними функціями.

Другий клас компонентів ПЗ-системи управління розподіленими базами даних, засоби аналізу даних та засоби розробки прикладних програм може бути родиною продуктів фірми Oracle. Як головну серверну платформу баз даних доцільно використати СУБД Oracle 8, а як засоби проектування системи – Oracle Designer 2000 та Oracle Developer 2000. Для забезпечення аналітичної обробки даних в оперативному режимі пропонується використання серії програмних продуктів Oracle OLAP(On-Line Analitical Processing), що забезпечує аналітичну обробку даних з сховищ даних, в яких дані представлені у вигляді багатомірної моделі. Ці програмні продукти реалізовані у вигляді окремого серверу Oracle Express Server та засобів розробки Oracle Express Object. Для забезпечення доступу мобільних користувачів ІАС до баз даних з мобільних портативних комп'ютерів з використанням радіо-модемів, або комунікаційних систем пропонується використання програмного продукту Oracle Mobile Agent. Підтримку Web-сторінок забезпечує СУБД Oracle, що має в своєму складі Oracle Web Server, який підтримує CGI-інтерфейс і не потребує ніяких засобів програмування, крім серверного PL/SQL для створення динамічних HTML-сторінок по інформації з бази даних.

Третій клас компонентів ПЗ – географічні інформаційні системи,

наприклад, на серії програмних продуктів фірми ESPRI.

Четвертий клас компонентів ПЗ – офісні та сервісні системи, включає:

– систему управління документами GroupWise 5;

– засоби ведення та розпізнання графічних образів (FineReader та CuneiForm);

– графічний редактор Corel Draw; система розробки презентацій – Power Point);

– видавницьку систему Adobe Page Maker.

1.1.4. Математичне забезпечення ІАС

Математичне забезпечення ІАС включає математичні методи та моделі опису явищ та процесів, які будуть аналізуватися, моделюватися та вивчатися в органах влади, методи формулювання стандартних і нестандартних математичних задач; аналітичні та обчислювальні методи розв'язування цих задач; методи оцінки коректності побудованих розв'язків.

За характером розв'язуваних задач методи математичного забезпечення ІАС можна умовно поділити на три групи:

– методи аналізу індивідуальних експертних суджень, отримуваних при проведенні експертиз в органах державної влади, узагальнення цих суджень та обґрунтування відповідного їм підсумкового рішення експертованої проблеми;

– методи ідентифікації аналітичної моделі багатовимірних даних щодо діяльності органів державної влади на підставі відповідних спостережень та визначення і прогнозування проблемно-значущих характеристик цих моделей;

– методи всебічного аналізу, планування і прогнозування діяльності органів державної влади, міністерств та відомств, підприємств і установ різних рівнів і форм власності.

1.1.5. Лінгвістичне забезпечення ІАС

Лінгвістичне забезпечення повинне відображати багатоцільовий та багатофункціональний характер функціонування ІАС і являє собою комплекс засобів, які призначені для подання інформації та інтерфейсів користувачів програмно-інформаційних компонент системи у природно-мовному стилі. До складу лінгвістичного забезпечення входять:

– лінгвістичні (лексичні) засоби подання семантики даних: класифікатори та рубрикатори. Типи та зміст цих засобів визначається при описі структур систем баз даних, що розроблюються на стадії техноробочого проектування системи;

– інтерфейси користувачів (системи меню, діалогові вікна) програмно-інформаційних компонент, конкретний склад яких буде розроблений на стадії техноробочого проектування системи;

– спеціалізовані мови баз даних (мови, що призначені для описування та виконання операцій з базами даних різного типу), які орієнтовані на термінологію та семантику конкретної проблемної галузі, для якої спроектована конкретна програмно-інформаційна компонента. Призначення,

Наука, 1989.

19. *Біленчук Д.П., Біленчук П.Д., Залетов О.М, Клименко Н.І.* Страхове право України: Підручник. – К., 1999. – 368 с.

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

21. *Біленчук Д.П., Котляревський О.І.* Кібершахраї – хто вони? // Міліція України, 1999, № 7-8. – С. 32-34.

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

23. *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.

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

25. *Біленчук П.Д., Котляревський О.І.* Портрет комп'ютерного злочинця. – Київ, 1997. – 48 с.

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

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

28. *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.

29. *Корсунський С.В.* Трансфер технологій у США. – К.: УкрНТЕІ, 2005. – 148 с.

30. *Пархоменко В.Д., Пархоменко О.В.* Інформаційна аналітика у сфері науково-технічної діяльності. – К.: УкрНТЕІ, 2006. – 224 с.

31. *Югименко Н.И., Биленчук П.Д.* Логико-математические и кибернетические методы в криминалистике. – К.: УМК ВО. 1988. – 104 с.

ДОДАТКОВА ЛІТЕРАТУРА

1. *Авдеев Р.Ф.* Философия информационной цивилизации. – М., 1994. – 143 с.

2. *Александров С.А.* Роль патентной политики в конкурентной борьбе за рынки сбыта // Патенты и лицензии. – 1991. – № 6. – С. 33-36.

3. *Акаев Ш.М.* Информационно-аналитическое обеспечение принятия решений по обновлению продукции: дис. канд. экон. наук: Донецк. 1999. – 146 с.

4. Актуальні питання методології та практики науково-технічної політики / Малицький Б.А., Булкін І.О., Єгоров І.Ю. та ін. – К.: ДФФХ, 2001. – 201 с.

5. *Александров С.А.* Роль патентной политики в конкурентной борьбе за рынки сбыта // Патенты и лицензии. – 1991. – № 6. – С. 33-36.

ВИКОРИСТАНА І РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. *Агапов А.Ю.* Проблемы правовой регламентации информационных отношений в Российской Федерации // Гос. и право. – 1993. № 3.

2. *Агеев А.С.* Компьютерные вирусы и безопасность информации // Зарубежная радиоэлектроника. – 1989. – № 12.

3. *Александров В.Н., Соколовский Б.Е.* Системы защиты коммерческих объектов. Технические средства защиты. – М., 1992.

4. *Альбррехт У. ВенцДж., Уильяме Т.* Мошенничество: Луч света на темные стороны бизнеса / Пер. с англ. – СПб „Питер”, 1995.

5. *Андрианов В.И., Бородин В.А., Соколов А.В.* „Шпионские штучки” и устройства защиты объектов и информации / Под общей ред. *Золотарева С.А.* – СПб „Лань”, 1996 (1997).

6. *Андрушко П.* Проблеми кримінальної відповідальності за втручання в роботу автоматизованих систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в автоматизованих системах України. – К., 2000. – С. 50-53.

7. *Астапкин С, Максимов С.* Криминальные расчеты: уголовно-правовая охрана инвестиций. – ML: Юринформ, 1995.

8. *Балюк В.* Особенности развития Интернет в Украине // Правове, нормативне та метрологічне забезпечення системи захисту інформації в автоматизованих системах України. – К., 2000. – С. 21-24.

9. *Барсуков В.С.* Обеспечение информационной безопасности. – М.: „Технологии электронных коммуникаций”, 1996. – 94 с.

10. *Барсуков В.С, Водолазский В.В.* Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей. Ч. 1. – М.: „Технологии электронных коммуникаций”, 1993. – 146 с.

11. *Барсуков В.С, Марущенко В.В., Шигин В.А.* Интегральная безопасность. – М.: АО „Газпром”, 1994. – 170 с.

12. *Батурин Ю.М.* Новая информационная психология: правовое опосредствование // Влияние научно-технического прогресса на юридическую жизнь. – М., 1988. – С. 88.

13. *Батурин Ю.М., Жодзишский А.М.* Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991.

14. *Батурин Ю.М.* Проблемы компьютерного права. – М.: Юридическая литература, 1991.

15. *Бачило И.Л., Белов Г.Д.* О концепции правового обеспечения информатизации России. Законодательные проблемы информатизации общества // Труды Института законодательства и сравнительного правоведения при Верховном Совете РФ. – М, 1992.

16. *Бачило И.Л.* Правовое регулирование процессов информатизации // Гос. и право. – 1994. № 12. – С. 72.

17. *Бачило И.Л.* О собственности на информацию. Законодательные проблемы информатизации общества // Труды ИЗиСП. Вып. 52. – 1992. – С. 18.

18. *Белъсон Я.М.* Интерпол в борьбе с уголовной преступностью. – М.:

функції та склад мовних конструкцій для перелічених засобів буде визначений на стадії технороботочого проектування системи;

– мовні засоби СУБД різних типів, інструментальні засоби розробки програмно-інформаційних компонент, використання яких обумовлено проектом. Ці засоби призначені для опису даних та інтерфейсів користувачів, питання щодо їх використання повинні бути вирішені на стадії технороботочого проектування системи.

Проблемні питання:

– фінансування щодо забезпечення засобами інформатизації;

– забезпечення підготовки спеціалістів з питань інформатизації та інформаційних технологій;

– організація сертифікації програмних і технічних засобів інформатизації.

1.1.6. Шляхи вирішення проблемних питань

Для створення ефективної ІАС в межах України передбачається сприяння створенню і освоєнню виробів обчислювальної техніки та електроніки, сучасних приладів і обладнання, конкурентноздатних на світовому ринку, створенню замкнутого технологічного циклу вітчизняного виробництва сучасних компакт-дисків і перспективних DVD-дисків для забезпечення запису, збереження і розповсюдження аудіо- і відеоінформації та комп’ютерних баз даних великої ємності, створенню діючих зразків високоефективних ЕОМ різних класів, інтелектуальних робочих станцій, нейрокомп’ютерів, масових засобів інформатизації, таймерних комп’ютерних систем, систем комп’ютерного управління технологічними процесами, створенню вітчизняної елементної бази, налагодженню серійного виробництва електронних карток і впровадженню інформаційних систем з їх використанням. Виконання цих проектів сприятиме підвищенню рівня самозабезпечення засобами інформатизації і перетворенню України в рівноправного партнера у міжнародному розподілі праці з виробництва та використання засобів інформатизації.

Індустрія програмних засобів повинна стати базою для створення нових сучасних інформаційних технологій та систем, автоматизованих систем керування різноманітного призначення. Передбачається створення інструментально-технологічних комплексів підтримки розроблення високоякісного і конкурентноспроможного програмного забезпечення, відповідної державної системи оцінки якості, сертифікації програмної продукції. Виробництво програмних продуктів повинно стати самоокупною галуззю економіки, здатною експортувати свою продукцію.

На сьогоднішній день продемонстровано необхідність всеохоплюючого збору та аналізу інформації, потенційно важливої в інтересах фірми та відпрацьовано, як це слід робити на практиці [1-5]; існує низка придатних для комерційних структур варіантів методологій і математичних формалізацій аналізу і прогнозу ризиків [6-9].

Так, ведення інформаційно-аналітичної роботи доцільно розбити на два основних етапи [18].

Перший етап – вивчення і відбір потрібних першоджерел, формування

первинного інформаційного масиву. Розподіл інформації на заздалегідь визначені класи.

Другий етап – систематизація інформації за її змістом. Створення пошукових і довідкових систем, баз даних, каталогів і т.д., тобто вторинного інформаційного масиву.

Таким чином, організація інформаційно-аналітичного забезпечення здійснюватиметься за наступної схемою (рис. 1) [19]:

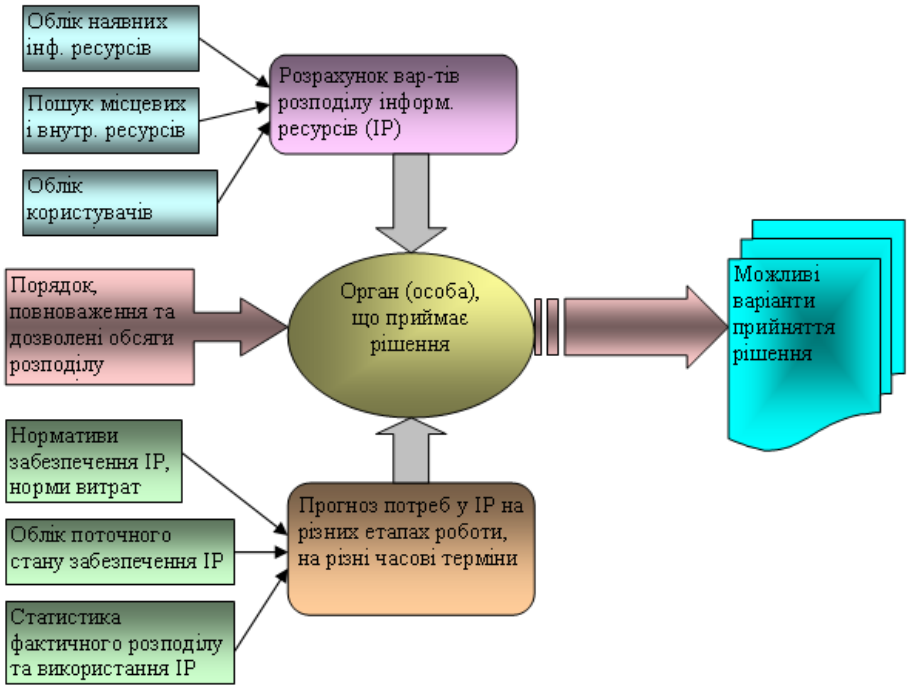

Рис. 1. Організація інформаційно-аналітичного забезпечення.

Проте відкритим залишається питання: як оптимізувати діяльність всіх задіяних у інформаційному процесі служб і посадових осіб? Інше, не менш важливе, питання: як найефективніше навчити основам організації і планування заходів інформаційного забезпечення (інформаційно-аналітичної діяльності, інформаційної безпеки) тих посадових осіб, кому це належить за посадою? Тобто, в наявності типова управлінська задача із необхідністю дотриматися стійкості, безперервності, гнучкості, оперативності і прихованості.

Після аналізу та опрацювання певної кількості першоджерел у попередніх авторських публікаціях запропоновано:

– порівняно простий (і наочний), що ґрунтується на теорії ймовірності математичний апарат для аналізу та прогнозування ризиків [10];

нашої країни у світове інформаційне суспільство та Указу Президента України № 928 від 31 липня 2000 року „Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні”.

Враховуючи важливість державного регулювання суспільних інформаційних відносин, Урядом України створена низка спеціальних організаційних структур щодо координації напрацювання державної політики у сфері організаційно-правового забезпечення входження нашої держави у світове інформаційне суспільство.

Серед них визначимо такі, як зазначена вище Урядова комісія, Міжвідомчий комітет з проблем захисту прав на об’єкти інтелектуальної власності, Міжвідомча робоча група з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з нелегальним їх використанням.

Зміст проекту Концепції реформування законодавства України у сфері суспільних інформаційних відносин та матеріали обґрунтування її положень розміщені в Інтернеті за адресою http://mndc. naiau. kiev/ua

Окремі питання в галузі інформаційної політики та розвитку інтернет-технологій в Україні розробляються та удосконалюються. Інформаційно-аналітичні матеріали з окремих галузей права розміщені в Інтернеті за адресою „INSURANCE ONLINE” – страхування майбутнього (www.uainsur.com).

Детальніший опис проблем комп’ютерної злочинності в Україні та у світі, зокрема, такої, що має ознаки організованої, подається в літературних джерелах, перелік яких додається.

Література

1. *Біленчук П.Д., Гавловський В.Д., Романюк Б.В. та ін.* Комп’ютерна злочинність: суперхакери і кіберполіцейські. – Київ: Атіка, 2002. – 240 с.

2. *Біленчук П.Д., Гуцалюк М.В., Кравчук О.В., Козир М.В.* Комп’ютерний тероризм: суперхакери та кібер-терористи, кібер-криміналісти. – Монографія / За заг. ред. П.Д. Біленчука. Київ: Наука і життя, 2008. – 291 с.

3. *Біленчук П.Д., Кравчук В.В., Кравчук О.В., Кулик В.М.* Комп’ютерний тероризм: практика запобігання, протидії, розслідування: Навчальний посібник / За заг. ред. П.Д. Біленчука. – Хмельницький. Хм. ЦНТЕІ, 2008. – 258 с.

законодавства України.

У відповідності з традиціями кодифікації України, на нашу думку, Кодекс має складатися з двох частин.

Частина І. Загальна частина. (Загальні положення);

Частина П. Особлива частина (Регулювання інформаційних відносин та інформатизації щодо галузей (сфер) суспільної діяльності).

Структура статті повинна складається з чіткого визначення диспозиції суспільних відносин. Окремі статті можуть містити прив'язки (посилання) до норм іншого законодавства України.

У статтях, в яких визначаються правопорушення, має бути обов'язкове посилання на вид відповідальності: відповідно до Цивільного кодексу, Кодексу Законів про працю, Кодексу про адміністративні правопорушення, кримінального кодексу.

Наприклад, „... покарання за дане правопорушення наступає у відповідності з Кодексом про адміністративні правопорушення України", чи „... відповідальність наступає у порядку, визначеному Кримінальним кодексом України", чи „... матеріальна відповідальність наступає у порядку, визначеному Цивільним кодексом України", „... дисциплінарна відповідальність наступає відповідно до Кодексу законів про працю".

У цивільному кодексі, Кодексі Законів про працю, Кодексі про адміністративні правопорушення, Кримінальному кодексі створюються відповідні розділи щодо питань регулювання та відповідальності за правопорушення суспільних інформаційних відносив з посиланням на норми Кодексу про інформацію.

У разі визначення нових сфер регулювання інформаційних відносин, в Кодекс (методом агрегації), вводяться нові розділи чи глави. Серед таких у перспективі можуть бути:

– захист персональних даних (інформації про особу, особистої інформації);

– забезпечення інформаційної безпеки суспільства і держави, регламентація основоположних організаційних заходів захисту інформації (організаційно-правових, організаційно-управлінських, організаційно-технічних, програмно-математичних) тощо.

Систематизація та удосконалення законодавства України в сфері суспільних інформаційних відносин розглядається нами як один з шляхів боротьби з комп'ютерною злочинністю, зокрема такою, що має ознаки організованої.

Подальше удосконалення чинного законодавства знайшло практичне впровадження їх результатів 6 жовтня 2000 року на засіданні Урядової комісії з питань інформаційно-аналітичного забезпечення органів виконавчої влади, де розглянуто проект Концепції реформування законодавства України у сфері суспільних інформаційних відносин (далі – Концепції) шляхом розробки Кодексу про інформацію.

За своїм змістом ця Концепція спрямована на системну, комплексну організаційно-правову реалізацію основних засад Програми інтеграції України до Європейського Союзу, зокрема її розділу 13, про входження

– стратегію безперервного забезпечення і вдосконалення безпеки (в першу чергу, інформаційної, а, отже, і загальної) підприємства [11].

У статті [11] запропоновані мнемосхеми для відображення суті стратегії, названі за своїми стародавніми прототипами "Сонцеворот" і "Хрещатий хрест". Чільне місце у кожній із цих схем займає своєрідне "ядро" – процес (і, відповідно, служба) аналізу.

Як організувати службу аналізу?

Для якісного управління необхідно з'ясувати [12, с. 14-16; 15, с. 124-155; 16, с. 47-57, 17]:

– чого необхідно досягти (мета);

– які задачі для цього потрібно виконати;

– яку інформацію для цього необхідно;

– які взаємозв'язки (взаємодії) варто налагодити між службами;

– яку ступінь компетенції і творчості допустити для виконавців того чи іншого рівня.

На сьогодні вже запропоновані і впроваджені у дослідну експлуатацію методики багатосторонньої кваліметричної оцінки праці фахівців різних рівнів і профілів [12, с. 46-53, 54-60, 66-71, 74-79, 132-142]. За допомогою кваліметричної оцінки є можливим формалізувати і взяти на облік такі показники:

– ефективність використання робочого часу;

– якість виконаної роботи;

– складність виконаної роботи;

– обсяги інформаційної складової;

– ступені самостійності (творчості) роботи і відповідальності за неї.

Подальший розвиток у працях вітчизняних фахівців питання теорії управління персоналом знайшли у посібнику В.М. Колпакова "Методы управления" [13].

Нижче ми адаптуємо ці методики для нашої проблематики. Так, у [14] зазначено, що важливим кроком є обчислення часу створення інформаційного масиву. Незважаючи на відносну простоту обчислень, це важливий етап, оскільки він відповідає на запитання: за який період особа, яка приймає рішення, володітиме щонайповнішою інформацією, потрібною для реагування на ту чи іншу кризову ситуацію? Звідси, інше запитання: наскільки ефективно витрачається наявний резерв часу?

Необхідно зазначити, що проблема раціонального розподілу часу як наукова проблема далеко не нова і досить ґрунтовно розкрита у [16]. Автори, зокрема, звертають увагу на важливість власних джерел і каналів надходження інформації для ефективного керівництва.

На підставі сказаного введемо такий показник:

$$\Phi = \frac{T_в}{T_в + T_з},\ 0 \le \Phi \le 1 \quad , \qquad (1)$$

де $Tв$ – час, витрачений на обробку інформації, що надійшла по власним каналам, $Tз$ – час на обробку інформації, отриманої ззовні.

Якщо $\Phi \in [0,5;1]$, то підрозділ (служба) є функціонально самодостатнім, у іншому ж випадку необхідно переглянути функції та завдання підрозділу.

Інший важливий показник має характеризувати, ступінь взаємопов'язаності служб при виконанні одного завдання.

$$Z = \frac{K_j^{(i)}}{M_j^{(i)}}, 0 \le Z \le 1, i, j = 1,2,.. \quad (2)$$

Тут $K_j^{(i)}$ – кількість зв'язків *j-го* підрозділу із іншими в межах виконання *i-ї* функції; $M_j^{(i)}$ – гранично можливий максимум таких зв'язків.

У тому разі, якщо $Z \le 0,5$, досліджуваний підрозділ необхідно тримати як окрему одиницю. В іншому випадку – або 1) підрозділи треба об'єднати принаймні в оперативному відношенні або 2) необхідно виділити невластиві або дубльовані функції.

Ще один аспект – готовність підрозділу до вирішення нових завдань, налагодження і підтримання нових зв'язків, виконання нових робіт. Цей аспект так само можна формально охарактеризувати. Формула обчислення показника за внутрішньою будовою аналогічна до формули (1) і має вигляд:

$$A = \frac{U_н}{U_н + U_c}, A < 1 \quad (3)$$

У цій формулі *Uн* – кількість нових зв'язків і робіт, *Uc* – кількість стабільно повторюваних зв'язків і робіт.

Для оцінки якості виконання завдань протягом звітного періоду застосуємо коефіцієнт

$$Q = \frac{X}{X_з}, 0 \le Q \le 1 \quad (4),$$

де *X* – кількість своєчасно та якісно виконаних завдань, *Xз* – загальна кількість завдань, покладених на підрозділ.

Висновок по формулам (3) і (4). Якщо A→1, Q=1, тоді підрозділ адаптований, тобто здатний адекватно реагувати на зміни в ситуації. Якщо A<1, Q<1 то підрозділ обмежено адаптований. У тому ж разі, якщо A→0, Q=0, підрозділ в цілому не адаптований.

Ще один важливий показник – показник розподілу прав, обов'язків та відповідальності (призначення відповідальних виконавців) при вирішенні рутинних завдань – допомагає виявити дефекти розподілу прав і повноважень.

$$P = \frac{1}{10n}\sum_{i=1}^{m} W_i \quad (5).$$

Тут *n* – загальне число вирішуваних завдань; *m* – число завдань, які вирішує керівництво; *Wi* – середня "вагова" оцінка важливості *i-ї* завдання із числа *m*, $W_i \in [0;10]$.

відповідності з теорією системи підцілей („дерева цілей"). Варіанти назви майбутнього Кодексу сьогодні дискутуються різними авторами і формуються по-різному. Наводимо деякі з них: Кодекс України про інформацію, Кодекс України про суспільні інформаційні відносини та інформаційну безпеку, Кодекс про інформаційний суверенітет України, Кодекс про захист інформації в Україні, Кодекс інформаційного права, Інформаційний кодекс України, Кодекс України про інформацію та інтелектуальну власність тощо.

На наш погляд найбільш змістовним є назва „Кодекс України про інформацію". У цій назві синтезуються всі перелічені вище положення сутності суспільних інформаційних відносин.

Мета Кодексу визначається у відповідності з теорією системи цілей. Метою Кодексу є правове регулювання суспільних відносин між їх суб'єктами щодо інформації за умов формування і розвитку інформаційного суспільства в Україні.

Інше визнається підцілями, функціями, напрямами, окремими завданнями регулювання нормами Кодексу.

Провідними функціями майбутнього Кодексу можна визначити такі, як:

– регулятивна функція – визначення прав та обов'язків, зобов'язань суб'єктів;

– нормативна функція – визначення норм, правил поведінки суб'єктів інформаційних відносин;

– охоронна функція – визначення гарантій та меж правомірної поведінки, за якими діяння утворюють правопорушення (делікти) та відповідальності за них у відповідності з нормами цивільного права, адміністративного права, трудового права, кримінального права;

– інтегративна функція – системне поєднання комплексу певних юридичних норм, які регулюють інформаційні відносини в Україні, поєднуюча ланка між провідними традиційними галузями права щодо застосування їх методів правового регулювання в сфері інформаційних відносин;

– комунікативна функція – зазначення в окремих статтях посилань на законодавчі акти, які є або необхідність в яких може виникнути, системоутворюючими різних міжгалузевих інститутів права.

Серед ключових завдань Кодексу можна визначити:

– визначення консенсусу (згоди) в суспільних стосунках, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників інформаційних відносин, відносин в інформаційній сфері;

– забезпечення інформаційного суверенітету, незалежності України у міжнародних стосунках;

– забезпечення інформаційної безпеки громадян, їх окремих спільнот, суспільства та держави, як складових національної безпеки України;

– визначення правомірної поведінки учасників інформаційних відносин в Україні;

– захист інформації від несанкціонованого доступу, знищення та модифікації, перекручення тощо.

Детальніше види завдань знаходять розвиток в нормах інформаційного

суспільства наслідків інформатизації, попередження поширенню комп'ютерної злочинності в Україні.

Новий підхід, щодо правового регулювання суспільних відносин, запропонований вітчизняною наукою інформатикою, її складовою – правовою інформатикою та міжгалузевою науковою дисципліною інформаційним правом. Це застосування принципів, підходів і методів інформатики до вирішення проблем права, зокрема правотворення.

При систематизації інформаційного законодавства на рівні створення Кодексу недопустимо необґрунтоване копіювання зарубіжного досвіду.

При розробці інформаційного законодавства необхідно враховувати такі принципи, як:

– повага та гуманне ставлення до людини, її честі, гідності, репутації;

– презумпція невинності громадянина, приватної особи перед державою.

Правотворення повинно ґрунтуватися на основі методології системного і комплексного підходів, зокрема теорії формування комплексних гіперсистем права.

Системоутворюючим інформаційного законодавства нашої країни має стати Кодекс. Він повинен об'єднувати і розвивати норми і принципи суспільних інформаційних відносин, що визначені в Конституції України; враховувати ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права; легалізувати позитивні звичаї в сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об'єднаних Націй в Декларації прав людини, та інших загальноприйнятих міждержавних нормативних актах.

Методологічною основою правотворення Кодексу є юридична доктрина щодо умовного поділу права України на галузі за принциповою моделлю:

– основа – конституційне право;

– його положення знаходять паралельний розвиток (у відповідності з методами правового регулювання і захисту прав) в адміністративному, цивільному, кримінальному праві та інших підсистемах національного права України, в яких інформація виступає як опосередкований, додатковий (факультативний) предмет регулювання.

Домінуючою методології є доктрина сучасного вітчизняного конституційного права (основа – Конституція України) та найкращих здобутків міжнародного права щодо верховенства прав людини у сфері суспільних відносин, об'єктом яких є інформація. Доктринально визнається багатооб'єктність юридичних норм, законодавства в правовій кваліфікації суспільних інформаційних відносин. Розробка проекту Кодексу повинна проводитися методом агрегації (приєднання):

– удосконалення окремих правових норм, чи створення нових і міжгалузевих правових інститутів не повинно порушувати цілісність та призначення Кодексу, а покращувати, удосконалювати і його дієвість в цілому;

– правотворення повинно створювати нову системну якість, яка не притаманна окремим його складовим.

Напрями, підцілі, завдання Кодексу повинні чітко формуватися у

Зрозуміло, що ідеальний розподіл повноважень спостерігається при $P=0$, тобто керівництво не виконує жодного з рутинних завдань. При $P=1$ структура вважається дезорганізованою, оскільки керівництво вирішує всі можливі рутинні завдання. Середній варіант – $P \in (0;1)$.

Загальний висновок: запропонована методика дозволяє: 1) визначити сильні і слабкі сторони в інформаційному забезпеченні, 2) з'ясувати готовність служб до нештатних ситуацій, 3) раціонально розподілити виконання завдань між посадовими особами різних щаблів ієрархії та групами виконавців. Сподіваємось, що практичне використання всіма зацікавленими особами наведеної методики виявить можливості її подальшого вдосконалення.

Література

1. *Біленчук П.Д.* та ін. Комп'ютерна злочинність: Навчальний посібник. – К.: Атіка, 2002. – 240 с.

2. *Давыдов И.* Тайна фирмы // К.: Фирма "Колир-2", 1993. – 174 с.

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

4. *Ронин Р.* Своя разведка: способы вербовки агентуры, методы проникновения в психику, форсированное воздействие на личность, технические средства наблюдения и съёма информации: Практическое пособие. – Минск: „Харвест", 1998. – 368 с.

5. *Землянов В.М.* Своя контрразведка: Практическое пособие / Под общ. ред А.Е. Тараса. – Мн.: Харвест, 2002. – 416 с.

6. *Браїловський М.* Захист економічної інформації. Навчальний посібник / М.М. Браїловський, В.О. Хорошко, Д.В. Чирков, М.Е. Шелест. За ред. проф. В.О. Хорошка. – К.: НАУ, 2002. – 78 с.

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

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

9. *Соколов А.В., Степанюк О.М*. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург; Арлит, 2002. – 496 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. – вып.13. – С. 127-135.

11. *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.

12. *Дмитренко Г.А.* Стратегічний менеджмент: цільове управління персоналом організацій: Навч. посібник. – К.: МАУП, 1998. – 188 с.

13. *Колпаков В.М*. Методы управления: Учебное пособие. – 2-е изд., испр. и доп. – К.: МАУП, 2003. – 368 с.

14. *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.

15. *Обэр-Крие Дж.* Управление предприятием.: Сокр. пер. с фр. – М.: Прогресс, 1973. – 304 с.

16. *Ниссинен Й., Воутилайнен Э.* Время руководителя: эффективность использования.: Сокр. пер с фин. – М.: Экономика, 1988. – 192 с.

17. *Твердохлеб Н.Г.* Безбумажная технология в управлении производством. – К.: Техника, 1991. – С. 6-8, 153-166.

18. *Пархоменко О.В.* Класифікація та ідентифікація джерел інформації і аналітичній роботі // Науково-технічна інформація. – 2001. – № 1-2. – С.29-31.

19. *Копійка О.В., Черепін Ю.Т.* Інформаційна підтримка управлінських рішень в системі органів виконавчої влади // Науково-технічна інформація. – 2000. – № 2. – С. 6-12.

1.2. Виявлення, збирання, оцінка подій, явищ і процесів

Захист безпеки інформації[1] та протидія розвідкам різних видів актуальний на всіх щаблях в усіх галузях життя держави – від окремої фізичної особи до державного відомства або крупної корпорації.

Подібно до того, як будова складається із окремих цеглин, а живий організм – з клітин, так загально державна безпека формується з багатьох складників, різних за своїм якісним і кількісним станом, об'єднаних єдиною формотворчою ідеєю – убезпечення держави від внутрішніх та зовнішніх загроз. 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 межах 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.

Аналіз вітчизняної та зарубіжної літератури 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;

[1] Під безпекою інформації будемо розуміти всі заходи, спрямовані на збереження режиму таємності, протидію чужим розвідкам, збереження інформаційних ресурсів від знищення, спотворення, викрадення, перехоплення, несанкціонованого копіювання внаслідок умисних зловмисних дій, халатності, помилок персоналу, технічних несправностей і т.д. [1, с. 2-6].

– правове регулювання щодо створення реальних умов для якісного і ефективного забезпечення необхідною інформацією громадян, органів державної влади, органів місцевого самоврядування, державних та приватних організацій, об'єднань на основі державних інформаційних ресурсів, сучасних інформаційних технологій;

– забезпечення співвідношення інтересів суб'єктів суспільних інформаційних відносин у сфері національної безпеки, її складової – інформаційної безпеки;

– забезпечення реалізації конституційних прав осіб (приватних немайнових) на режим доступу до персональних даних – інформації про громадян та їх спільноти, організацій за умов інформатизації державних органів управління;

– державно-правове сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, з пріоритетами для вітчизняних виробників інформаційної продукції, засобів, технологій;

– державне стимулювання вдосконалення механізму залучення інвестицій, розробки і реалізації проектів національної програми інформатизації та локальних програм інформатизації (установ, підприємств, організацій, всіх форм власності, міністерств та відомств, регіонів тощо);

– забезпечення правового режиму формування і використання національних інформаційних ресурсів, збору, обробки, накопичення, зберігання, пошуку, поширення та надання споживачам інформації; правове регулювання щодо стимулювання створення і використання в Україні новітніх інформаційних технологій;

– визначення і класифікація загроз безпеці суспільним інформаційним відносинам, регулювання захисту інформації, у тому числі в автоматизованих системах (в основу пропонується такий підхід класифікації загроз інформаційної безпеки: загрози першого порядку – стихійні (природні), соціогенні, техногенні. Серед найнебезпечніших соціогенних загроз є криміногенні та ентропія (міра невизначеності ситуації перших керівників органів управління щодо усвідомлення необхідності комплексного захисту інформації);

– створення реальних правових бар'єрів, недопущення свавілля державних та недержавних структур, посадових осіб щодо примушення подання їм громадянами інформації, яка існує в інших структурах. Повинен утвердитися принцип презумпції невинності громадянина, а не існуючий порочний принцип недовіри до документа, який був виданий іншою інстанцією („принеси довідку, тоді дамо тобі довідку"), в результаті чого громадяни змушені витрачати багато часу на ходіння по різних інстанціях, щоб підтверджувати правомірність виданих їм раніше документів. Перевірка достовірності документа, встановлення юридичного факту та його документування, повинно покладатися, бути функцією органу, уповноваженого видати відповідний документ.

Особливу увагу необхідно звертати на виявлення та дослідження недоліків, як вітчизняного, так і зарубіжного права для уникання їх у правотворчій та правозастосовчій діяльності в Україні, зокрема, запобігання негативних для

У зв'язку з тим, що різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без узгодження понятійного апарату, вони мають ряд термінів, які недостатньо коректні, не викликають відповідну інформаційну рефлексію, або взагалі не мають чіткого визначення свого змісту. Наприклад, „інформація", „таємна інформація" і „таємниця", „документ" і „документована інформація", „майно", „власність", „володіння", „автоматизована система" тощо. Термінологічні неточності та різне тлумачення однакових за назвою і формою понять та категорій призводить до їх неоднозначності розуміння і застосування на практиці, в тому числі щодо боротьби з так званою організованою комп'ютерною злочинністю.

Має місце розбіжність щодо розуміння структури і складу системи законодавства в сфері інформаційних відносин та підходи до їх формування. Нерідко в окремих законах у систему законодавства включають норми, що виражені в підзаконних нормативних актах. Це створює в практиці правозастосування деякими учасниками суспільних відносин колізію норм, ігнорування норм закону на користь норм підзаконного акта.

Велика кількість законів та підзаконних нормативних актів у сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування.

Нові правові акти в сфері суспільних інформаційних відносин, нерідко не узгоджені концептуально з раніше прийнятими, що призводить до правового хаосу.

Сукупність правових норм у сфері суспільних інформаційних відносин, визначених в законах і підзаконних актах, досягли за своєю кількістю критичного стану, що зумовлює необхідність виділення їх в окремий, автономний міжгалузевий інститут права – інформаційного права та систематизацію на рівні Кодексу.

На нашу думку, в основу такого Кодексу повинні покладатися відпрацьовані юридичною наукою і перевірені практикою інкорпоровані норми чинного інформаційного законодавства України.

Доктринально можна визначити низку основоположних методологічних принципів:

– інформаційне законодавство є міжгалузевий інститут національного права України;

– інформаційне законодавство має основний предмет регулювання – інформацію (відомості, дані, знання, таємниця тощо).

Ми вважаємо, що серед основних сфер правового регулювання Кодексу, визначаються такі:

– визначення та правове закріплення провідних напрямів державної політики інформатизації;

– забезпечення умов для розвитку і захисту всіх форм власності на інформацію та інформаційні ресурси;

– організація та управління створенням і розвитком державних регіональних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі України;

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

– відпрацьований порядок класифікації 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;

– 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 оптимізації 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 сферою, при цьому органічно інтегрованою до загальної системи управління цим об'єктом.

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:

– аналіз загрози для інформації на даному об'єкті;

– оцінка ймовірності виникнення того чи іншого виду загрози та можливі втрати в разі "поразки";

– 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 частинного до загального) [2, 3]:

– 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 володіти великою кількістю впорядкованої інформації з усіма наслідками. Основні шляхи надходження інформації і способи її впорядкування проаналізовано у [4].

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 [5]. Інакше кажучи, потрібен типовий алгоритм роботи посадових осіб та підрозділів при формуванні, експлуатації та супроводженні системи забезпечення безпеки.

Подамо один із можливих варіантів алгоритмізації. На початку зазначимо, що, оскільки питання проблеми прийняття рішення, процесу збору, аналізу, обробки та зберігання інформації, збереження таємниці, захисту інформаційних ресурсів від ворожих посягань постали ще "на світанку цивілізації", то і знайшли вони свої наочні, вичерпні і дохідливі відображення в історичних, філософських та культурних пам'ятках минулого.

Наприклад, Сунь-Цзи, військовий теоретик Стародавнього Китаю, у своїх афоризмах досить дохідливо змалював основні закони, процеси та дії, які має обов'язково брати до уваги полководець будь-якого рівня [6]. Так, в основу війни та військових дій Сунь-Цзи кладе п'ять основних явищ: 1) Шлях, 2) Небо, 3) Земля або Простір, 4) Полководець, або Суб'єкт протиборства, 5) Закон або Аналіз [6, с. 35-36, 75-85]. Кожен із цих елементів породжує наступний і, у свою чергу, сам народжується із попереднього. Звідси виходить така заповідь: "Керуй супротивником сам і не давай йому керувати собою" [6, с. 260]. Для цього необхідно дотримуватися іншої настанови: "…Якщо знаєш його (тобто супротивника) і знаєш себе, перемога недалека; якщо знаєш при цьому ще і Небо і знаєш Землю (тобто часові і просторові обмеження у даній ситуації), перемога забезпечена цілковито" [6, с. 60].

Сучасний дослідник прадавньої історії України Братко-Кутинський розповідає, зокрема, про багатий світ розмаїтих символів, якими наші предки зображували закони та процеси світобудови І кожен з цих символів живе на рівні підсвідомості кожної нормальної людини, слугуючи при цьому своєрідним життєвим дороговказом [7]. На думку автора, цими потужними набутками людства, адаптованими до сучасних умов, не можна не скористатися.

Таким чином, вимальовується така схема, де літерою "А" позначено місце аналізу (рис. 1).

Не принижуючи ролі організації інженерно-технічних засобів захисту інформації в автоматизованих (комп'ютерних) системах, необхідно зазначити, що зусилля ряду країн спрямовуються саме на розвиток організаційно-управлінських та організаційно-правових засобів забезпечення інформаційної безпеки в умовах інформатизації.

В Україні, на зразок інших країн, існує потреба формування і розвитку спеціальних підрозділів по боротьбі з комп'ютерною злочинністю: у МВС – у структурі підрозділів по боротьбі з організованою злочинністю, та у підрозділів державної служби по боротьбі з економічною злочинністю; у Державній податковій адміністрації, в складі податкової міліції; у Службі безпеки України, в підрозділах контррозвідки.

Щодо стратегії боротьби з комп'ютерною злочинністю, все більше фахівців в галузі боротьби з нею в нашій країні, як і дослідники в інших сферах боротьби зі злочинністю, стають прихильниками ідеї, вираженій у афоризмі: „Апелювати в позбавленні від злочинності до поліцейських засобів і пенітенційної (кримінально-правової) політики – це все одно, що за допомогою парасольки намагатися зупинити дощ"[1].

Важлива роль у міжнародній практиці боротьби з комп'ютерною злочинністю відводиться удосконаленню законодавчого регулювання суспільних інформаційних відносин, як на національному, так і на міжнародному рівні. Не залишилася поза цим процесом і Україна.

З часу проголошення 24 серпня 1991 року державної незалежності України створюється національна система законів та підзаконних нормативних актів щодо правового регулювання суспільних інформаційних відносин в умовах формування інформаційного суспільства, процесу інформатизації та комп'ютеризації.

Національне (державне, публічне) право України має значний масив нормативних (законів та підзаконних) актів, які прямо чи опосередковано регулюють інформаційні відносини в суспільстві. Це Закони України, Постанови Верховної Ради України (нормативного змісту), Укази Президента України, Розпорядження Президента України, Постанови Кабінету Міністрів України, Розпорядження Кабінету Міністрів України, нормативні акти міністерств і відомств.

У той самий час, для упорядкування та врегулювання цих відносин на державному рівні виникла потреба юридично визначитися у найважливіших правових нормах поведінки їх учасників, у тому числі запобігання та боротьбі з правопорушеннями в сфері суспільних інформаційних відносин.

Проблемою для України є те, що сучасне її інформаційне законодавство не має легальної чіткої, ієрархічної єдності, що викликає суперечливе тлумачення та застосування його норм на практиці. Через те, що нормотворення в Україні у сфері інформаційних відносин стало на шлях світової доктрини загального права, окремі проблеми вирішуються на рівні законодавства в окремих законах без узгодження їх з іншими нормативними актами.

[1] Див.: *BottomleyA.* Criminology in focus. N. Y. 1979. – P. 158.

РОЗДІЛ 3.
ЗЛОЧИННІСТЬ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СФЕРІ: ЗАПОБІГАННЯ, ПРОТИДІЯ, РОЗСЛІДУВАННЯ

Аналіз розвитку комп'ютерної злочинності дозволяє зробити декілька узагальнень.

Необхідно підкреслити, що проблематика комп'ютерної злочинності, особливо її складової – організованої комп'ютерної злочинності сьогодні вже має чітко визначений як національний, так і міжнародний, транснаціональний характер.

Факт економічної відмінності серед держав, який стає очевидний, повинен спонукати країни, які мають нижчий рівень економічного становища, докласти всіх зусиль, щоб наздогнати розвинені країни не тільки щодо технічного розвитку інфраструктури, засобів телекомунікації, але й у формах, методах, способах боротьби з комп'ютерною злочинністю. Це на сьогодні є актуальною парадигмою і для України.

Введення мережі електронних розрахунків веде до трансформації техніки виконання корисливих злочинів у сфері банківської та пов'язаної з нею кредитною, фінансово-економічною діяльністю, хоча в її основі є ті самі механізми документообігу, що ґрунтуються на системі звичайного бухгалтерського обліку. Тому діюча технологія вчинення злочинів автоматично переносяться в умови електронних розрахунків. У той самий час технології вчинення комп'ютерних злочинів у сфері економіки мають свої особливості.

Проблемою щодо нашої країни є відсутність кримінально-процесуальних та криміналістичних напрацювань методології, методики та тактики боротьби з комп'ютерною злочинністю, зокрема, у сфері економіки.

Комп'ютерна злочинність все більше й більше загрожує як економічним основам держави, так і світовій економічній системі, всій безпеці людства.

На погляд зарубіжних спеціалістів, незаконне використання комп'ютерів дає більші прибутки для злочинців з меншими ризиками, ніж вчинення традиційних злочинів шляхом викрадення грошей в банках, тому кількість таких злочинів з кожним роком буде зростати.

Деякі керівники господарських структур пов'язують надійність електронних (комп'ютерних) систем переважно із засобами їх технічного захисту, у тому числі введенням (системи паролів) для входження не тільки в саму комп'ютерну мережу, а й до різних рівнів інформації в автоматизованій системі, в залежності від допуску її користувачів. Коло працівників, які за технологією виконання господарських операцій мають доступ до широкого діапазону цієї інформації, досить значне. Тому система захисту електронних мереж, що спирається тільки на кодуванні входжень до різних видів інформації, є малоефективною. Практика потребує пошуку принципово нових підходів для розробки відносно надійної системи захисту комп'ютерних мереж. У зв'язку з цим зусилля в багатьох країнах концентруються на подоланні змін – невизначеності широкого кола громадськості щодо здобутків і загроз інформаційної безпеки.

Рис. 1. Взаємодія об'єкту з оточенням.

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

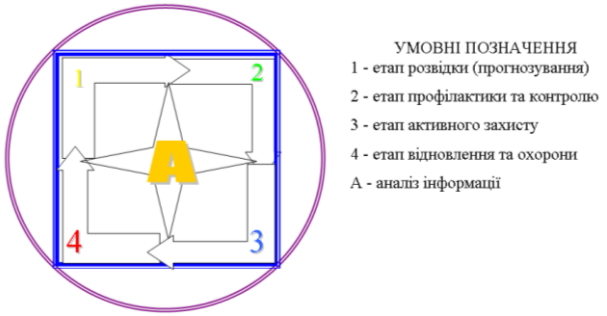

Рис. 2. Циркуляція потоків інформації

За основу при побудові даної схеми був взятий стародавній знак сонцевороту який символізує перехід від духу до матерії, тобто від задумів до конкретних дій, які, у свою чергу, породжують нові задуми.

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

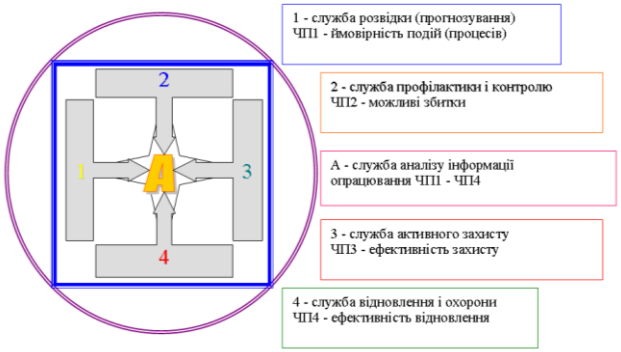

Рис. 3. Служби забезпечення безпеки

Результат роботи кожної служби повинен являти 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 необхідних захисних послуг, обмежень за ресурсами комплексується система захисту. У разі декількох варіантів комплексування необхідно вибрати з них оптимальний (на виході – ЧП3).

Після відбиття нападу визначається що саме, у якій послідовності і до якої міри підлягає відновленню; розбираються слабкі місця. 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.

Для повноцінного і ефективного використання названих вище ідей та навчання цим ідеям персоналу необхідно розробити спеціальний навчально-бойовий програмний комплекс.

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

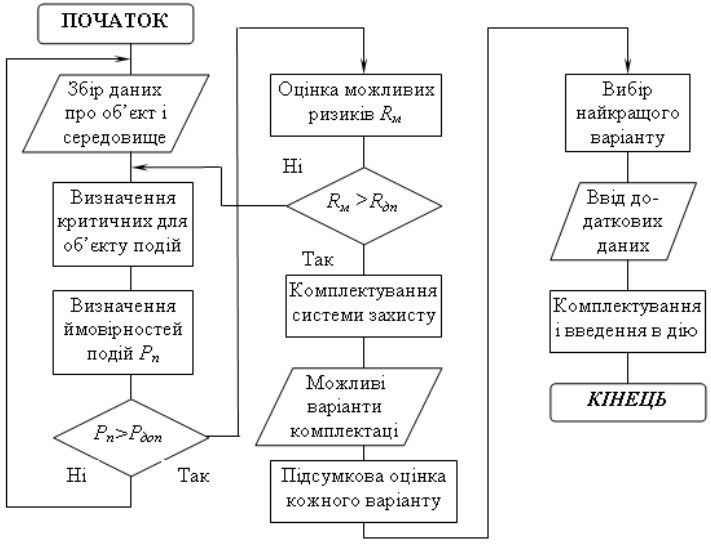

Рис. 4. Укрупнена блок схема алгоритму дії навчально-бойового програмного комплексу.

2.13. Створення багатства: знання проти капіталу

Прості ресурси типу капіталу усе менше і менше відповідають фактору обмеження у виробництві товарів і послуг, тому що покращення процесів виробництва дозволяє заміняти один компонент іншим. Щодня ми є свідками того, як цілі сектори економіки перебудовують себе до цього обмеження, що є результатом того, що універсальна автоматизація управляє функціонуванням економіки і заміщає традиційні структури виробництва. Ми зараз знаходимося у тій стадії розвитку, коли знання й інформація заміщають капітал. Старе прислів'я "знання – влада" не втрачає своєї актуальності. Дані, чи інформація стануть загальнодоступними в цифровому суспільстві. Відкриті джерела даних так само як і комерційно керовані конкурентно-інтелектуальні (Competitive Intelligence) дії зроблять дані й інформацію загальнодоступними. Однак подібне застосування інформації і знання мають принципову різницю.

Э.Фейгенбаум, що у 1977 році ввів поняття інженерії знань, відзначав у своїх працях: "По досвіду нам відомо, що велика частина знань у конкретній предметній галузі залишається особистою власністю експерта. І це відбувається не тому, що він не хоче розголошувати своїх секретів, а тому, що він не в змозі зробити цього – адже експерт знає набагато більше, ніж сам усвідомлює". Управління знанням призначено для підтримки і поширення чогось нового і більш зробленого. "Знати" важливіше ніж "мати" – стає основою нової соціальної, політичної й економічної моделі дій. І ця сила може бути багаторазово збільшена шляхом вкладення інформації і знання в реалізацію зроблених технологій.

2.14. Мережа як розповсюджувач і "підсилювач" інформації

Нова сторона технології мереж – специфічне "множення" чи "посилення". Електричні і механічні пристрої збільшують силу, мережі "підсилюють" інформацію. Для простої людини це означає те, що в мережі його можливості рівнозначні можливостям великих організацій у плані придбання, розподілу і збереження інформації. Таким чином, індивідуум може конкурувати за своїми можливостями у мережі нарівні з великими чи урядовими організаціями.

У багатьох відносинах, можливість доступу й обробки великої кількості інформації змінюється зі зміною суспільної політики. Фактор того, як визначена суспільна політика, характеризувався рівнем доступу до статистичної і демографічної інформації. Але тепер ця сама можливість використовується індивідуумами й організаціями "проти" уряду.

відносин при вирішенні величезного спектра проблем, що виникли в інформаційну еру. Але в цьому позитивному сценарії обов'язково повинні були з'явитися негативні елементи. Ріст організацій, що проповідують догматичний спосіб мислення, також намагається скористатися перевагами глобальних мереж для досягнення своїх цілей. Вже є ознаки, що напружені відносини між конфронтуючими групами закінчилися м'якими формами "мережної війни" (netwar), начебто псування телефонів, факсів, комп'ютерів. Більш того, вони переходять від приватного рівня до організованого. Ця тенденція буде продовжуватися, призводячи до руйнівних наслідків, коли одні групи будуть намагатися підкорити собі інші за допомогою глобальних інформаційних мереж. Вони можуть використовувати мережу для управління знанням і силою інших об'єднань, чи знищуючи, підкоряючи їх. Особливо якщо ці об'єднання залежні від Інтернету як частини його (Інтернету) інфраструктури.

Щоб зменшити цю можливість, необхідно відзначити, що збільшення потоку зв'язку між користувачами різних об'єднань, так само, як і офіційні співвідношення, на урядовому рівні, розглядається як можливість зменшення напруги між різними об'єднаннями. Існує навіть думка про створення повної загальнодоступності інформаційних інфраструктур, що значно знизить подібну небезпеку, тому що величезна кількість людей буде брати участь в обговоренні і вирішенні спірних питань.

2.12. Економіка координації і співробітництва

Для багатьох явне існування Інтернет – усе ще парадокс. Чому дозволяють безкоштовний доступ до такої великої інформації? Це розглядається як спроба знищення конкурентності, основного двигуна західної економіки. Зрозуміло, що руйнування старих типів організації і виникнення нових типів призведе до нових видів взаємин. Усе більше людей беруть участь у різних організаціях з нефактичною зайнятістю (наприклад, усі ми можемо брати участь у різних партіях, екологічних організаціях, приватних корпораціях, уряді). Проте, в умовах ринку об'єднана (загальна) стратегія більш вигідна і сприятлива (що й ілюструється останніми дослідженнями теорії гри). Також на сьогодні вартість приєднання до глобальних мереж типу Інтернету багаторазово перекривається наданими можливостями.

Оскільки кожен вузол мережі незалежний, має власне фінансування і технічні вимоги, приєднання до Інтернет практично нічого не коштує, якщо ваша організація вже є частиною цієї мережі. Як і телефонна лінія, комп'ютерна мережа стає більш коштовною зі збільшенням людей і ресурсів, які вона поєднує. Чим більше вона росте, тим більше користувачів і мереж прагнуть стати її частиною. Колись Інтернет був новинкою, але організація мереж сьогодні є необхідним компонентом усіх соціальних дій у всіх високорозвинених суспільствах. Крім того, це тепер передумова росту і розвитку, а в однаковій мірі і поліпшення умов людського життя.

Тут $Рп$, – ймовірність виникнення небезпечної події, $Рдоп$ – допустиме значення цієї ймовірності, $Rм$ – можливий ризик за такої ймовірності, $Rдп$– допустиме значення ризику.

Авторами вже проведена спроба формалізації одного із етапів – етапу оцінки ризиків [7]. Математичний апарат і алгоритми інших програм, які повинні входити до складу комплексу автори планують розглянути у подальших публікаціях та висловлюють своє сподівання на плідну співпрацю із усіма зацікавленими особами.

Література

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. – К.: ДСТЗІ СБ України. – ст.ст. 4.1.2, 4.1.4-4.1.7, 4.3.7.

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

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

4. *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.

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

6. *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.

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

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

1.3. Діагностика подій, явищ і процесів

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 сфер, а також за економією коштів на ведення інформаційної діяльності.

Весь процес збирання та обробки інформації можна розділити на такі етапи [1]:

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, можна розділити так (рис. 5) [1].

Наведена нижче схема є своєрідним шаблоном, який можна доповнювати або змінювати з урахуванням особливостей поточного моменту, досвіду, стану забезпеченості інформацією, вирішуваних поточних та перспективних завдань тощо.

Для формування і поповнення цього масиву можуть бути використані такі джерела інформації (рис. 6) [1].

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 факту ставимо у відповідність спеціальну літеро-цифрову оцінку, причому літерами позначають рівень надійності джерела, а цифрами – відкіля 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.

Ніколи не варто забувати, що надійне джерело (А) інколи здатне передати явну дезінформацію, а зовсім ненадійне (Г) – повідомити найцінніші дані. Тому цей 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 – не визначаємо.

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

Інтернеті виникає настільки динамічна ситуація росту Інтернету, що його, соціальний вплив практично неможливо вгадати. Крім того, з новими послугами типу відео конференц-зв'язку, цифрових грошей, відкритого ключового шифрування і віртуальних бібліотек, що є загальнодоступним у межах системи, існують труднощі в розумінні, і точній оцінці інформаційного суспільства. Поряд з легкою доступністю глобальних мереж, увага переноситься з їх технічних характеристик на соціальні наслідки від їх використання. Вплив мереж тепер замічений у змінах в економічній і соціальній динаміці. Усі комерційні організації змушені увійти у віртуальний глобальний ринок, і змушені діяти одночасно на віртуальному і фактичному рівнях.

2.10. Дослідницькі групи і віртуальні об'єднання

Йдуть суперечки щодо природи груп і об'єднань, які існують на основі Інтернету. Не вступаючи в подібні дебати, можливість через Інтернет поєднувати загальні інтереси і зусилля, змушує нас переглянути нашу концепцію спільності.

Традиційна інтерпретація об'єднання включає географічний аспект. Але Інтернет не має подібних обмежень, як державні кордони. З'являється новий тип об'єднань: глобальні суспільства – частини інших глобальних суспільств. Надалі це ще прискорить ріст Інтернету. Уже сьогодні неможливо уявити участь у будь-якій комп'ютерній діяльності без Інтернету. Однак ці глобальні суспільства не тільки обмежуються обговоренням різних технічних питань, але й утворили безліч неурядових організацій (Non Governmental Organizations NGO), різних рухів, наприклад, у захист навколишнього середовища тощо. Фактично ці групи стали серйозною силою в міжнародних відносинах, особливо в питаннях політики, прав людини і т. ін., у першу чергу тому, що Інтернет забезпечує волю і незалежність їх діяльності. Нарешті, Інтернет безпосередньо пропонує універсалізацію цінностей і відкрите суспільство.

2.11. Системи оцінки і політичні дії

Аналітичні групи, чи newsgroups, відображають різні думки, що виникають у різних об'єднаннях. Це – світ новин, суперечок та аргументів. Цей світ відомий за назвою USENET, насправді, зовсім відмінний від Web. USENET скоріше подібний об'єднанню різних думок по різних пекучих питаннях. USENET не стільки фізична мережа, як об'єднання різних соціальних зустрічей. В даний час на USENET є приблизно 3,500 окремих аналітичних груп, їх обговорення складають приблизно 7 мільйонів слів надрукованого коментарю щодня. Велика кількість обговорень стосується різних технологій, але обсяг обговорюваних тем величезний і росте з кожним днем. Крім цього, USENET вільно (безкоштовно) поширює різні наукові, соціальні і культурні електронні журнали і публікації.

Як наслідок, глобальні мережі можуть дозволити розподіл загальних завдань, цілей та ідеалів, забезпечувати обмін припустимою інформацією між користувачами. Це також сприяє колективному прийняттю рішень і взаємних

інформації, як в Інтернеті. Історично вже доведено, що зв'язок перетворює людство. Використання комп'ютерів для міжнародного зв'язку далі буде збільшуватися і розширюватися, тому що увесь час створюються все нові інформаційні громади. Усе це створює нові виміри у світових справах.

2.8. Виникнення мереж

Біля тридцяти років тому перед мозковим центром корпорації РЕНД (RAND Corporation) була поставлена проблема здійснення керівництвом США зв'язку після можливої ядерної війни. Ким будуть управлятися і контролюватися мережі зв'язку, оскільки будь-яке центральне управління буде під прицілом ворожих ракет?

Пропозиція РЕНД, обнародувана в 1964, запропонувала мережу без центрального контролю і управління, і яка буде працювати навіть зі зруйнованими вузлами. Корпорація повинна була створити мережу, побудовану з ненадійними елементами, але, яка, проте, могла гарантувати, що в цілому система буде надійна. Зв'язок вузлів здійснювався б за принципом "рівний рівному" (peer to peer), тобто кожен вузол міг окремо одержувати і передавати повідомлення. Повідомлення безпосередньо були б розділені на пакети, причому кожен пакет мав би окрему адресацію. Спочатку кожен пакет був би в якомусь конкретному початковому вузлі, у результаті він би виявлявся в деякому іншому вузлі призначення без дотримання вимог будь-якого конкретного маршруту. Таким чином, усі пакети будь-якої інформації прийшли б довільними маршрутами через усю мережу, відновлюючи все повідомлення, потрапляючи до місцевої адресації. Таким чином, якщо який-небудь вузол виходить з ладу, буде знайдений інший маршрут, що обгинає цей вузол. Ця структура стала основою системи Arpanet, яка через деякий час стала Інтернетом.

2.9. Розвиток Інтернету

Дивно звучить, але ніхто точно не знає дійсні масштаби Інтернету. Існують тільки приблизні оцінки його розміру і швидкості розвитку. Ще недавно, у квітні 1995, Інтернет поєднував близько 8 мільйонів адміністративних комп'ютерів і 10-50 мільйонів підключених до них користувачів. Але розвиток Інтернету можна порівняти лише з ростом геометричної прогресії. Відповідно до досліджень Масачусетського Технологічного Інституту, загальний обсяг даних, що проходять через Інтернет у 1992 році, складав 500 Mb. Для порівняння, із січня по березень 1993 року це значення вже складало близько 5 Gb. За 6 годин вересня 1994 – 13Gb.

Зараз багато хто оцінюють збільшення користувачів Інтернету в межах 10-15 відсотків кожен місяць, подвоюється кожні 53 дня; інші стверджують, що в 2000 році було більш 100 мільйонів серверів, підключених до мережі. Останні підрахунки показують, що обсяг ринку Інтернету (програмне забезпечення, апаратні засоби і послуги) приблизно оцінюється в $4.2 мільярдів.

З урахуванням поширення операційних систем з можливістю роботи в

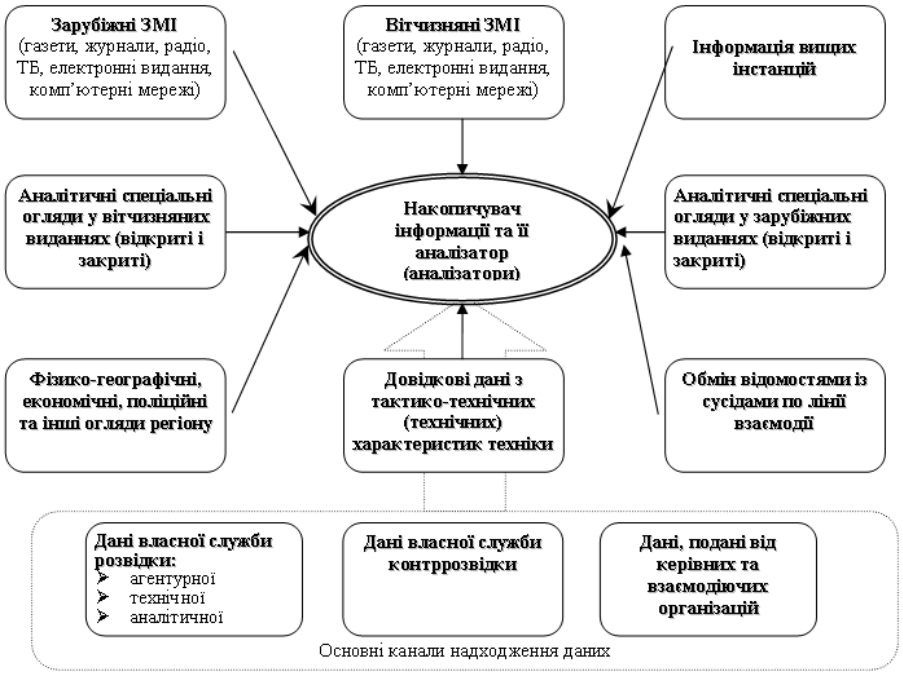

Рис. 6. Окремо виділені основні канали надходження інформації.

У таблиці показані основні взаємовідношення показників ймовірності та шансів [5, с. 274-275]:

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 необхідно 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 фоні відволікаючих увагу відомостей;

– 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.

Для успішної боротьби зі 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 їхні значення;

– істина звичайно 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:

даної інформації до іншої. Ці моделі, наприклад, ряд посібників з тактичних рішень, також повинні управлятися як єдиний критичний компонент повної інформаційної системи. Тому тепер існує ясна вимога до управління знанням.

Управління знанням припускає, що існує достатній рівень модульності в системі для того, щоб дані моделей і схем (процеси, структуровані знанням) могли управлятися незалежно від даних. Бази даних були б відділені від процесів пошуку. Це дало б можливість розвити дуже професійних "інтелектуальних" помічників. Необхідно розуміти, що ефективність роботи подібних моделей залежить від якості інформації, якою вони управляються.

Управління знанням відноситься проблем, пов'язаних зі створенням, перетворенням, збереженням, використанням і заміною складних моделей і обчислювальних структур, що функціонують організаційно формалізованим способом. Управління знанням виникає як ядро наступного покоління елементів програмного забезпечення.

2.6. Організація роботи зі знанням

Наявність доступу до великої кількості інформації ще не гарантує успіх. За всіма оцінками, найбільш важливе питання – "що це означає?" Для роботи зі знанням вимагаються експерти в конкретній галузі, вони повинні додавати інформації певне значення. Їх розуміння проблем і визначає ефективність дій. Знання стає силою тільки при роботі над ним. Обробка знань є однією з галузей обробки інформації. Однак фахівці обмежені в конкретних галузях, їх знання і здібності є нерівнозначні. Навички прийняття вірних рішень можуть бути збільшені систематичним застосуванням управління знанням. Для цього розглядаються такі три функції: формалізація, абстракція і поширення знання.

За допомогою кращих моделей можна збільшити загальну якість процесів прийняття рішень.

Системи міркування (Case Base Reasoning Systems) підтвердили свою цінність в галузі вирішення кризових ситуацій. З огляду на прецеденти, роблячи їх доступними для інших користувачів, ми збільшуємо можливості аналітиків і, таким чином, передбачаємо результат. Подібний підхід зручний навіть у тих випадках, коли фактична криза має лише загальні подібності з попередніми. У цьому випадку "вивчені уроки" запам'ятовуються і стають доступними користувачу при виникненні подібних умов. Роки досвіду, так само, як і сучасні принципи управління, засновані на схожостях між минулими і фактичними подіями, стають доступними користувачу.

2.7. IT-Інфраструктура - глобальні мережі

Існує безліч різних думок про походження глобальних комп'ютерних мереж. Деякі автори стверджують, що першою істинно глобальною мережею була міжнародна банкова справа. Деякі міжнародні компанії розвили дуже великий зв'язок і операційні системи. Світові ринки вважаються причиною подібної глобалізації. Однак, дивлячись на приклади подібних глобальних мереж, вони усі бліднуть у порівнянні зі злетом Інтернет. Немає жодної інформаційної системи, у якій би відбувалася така "демократизація"

коли користувач незареєстрований.

2.4. Робота, заснована на знанні

Інформація – стратегічний актив, однак інформація – тільки один рівень структури в представницькій епістемологічній (epistemological) ієрархії. Інформація – організовані дані, а бази даних – основні сховища даних. Набуття знань, що зберігаються в базах даних, здійснюється в процесі відновлення даних користувачем. Бази даних – це засіб для упорядкування взаємозалежної інформації та уніфікації управління її збереженням. Користувач баз даних може або одержувати інформацію, що задовольняє певним умовам, або додавати нову інформацію. Бази даних структуровані відповідно до онтологічної (ontological) моделі, яка є словником даних, що дозволяє користувачу одержати знання зі змісту. У великому японському тлумачному словнику знання визначають як "результат, отриманий пізнанням", чи, більш докладно, "система суджень з принциповою і єдиною організацією, що ґрунтується на об'єктивній закономірності". Не бажаючи створювати академічні дебати з даного предмету, відзначимо, що *знання – інформація, організована для конкретної мети. [Nagao]* Це і є спосіб співвідношення однієї інформації до іншої. Крім того, ці знання можуть бути повернуті в інформаційні бази даних, стаючи даними для іншої інформації. Важливо зрозуміти, що безпека інформації – частково проблема управління знанням. Сама по собі інформація не має ніякої реальної цінності.

2.5. Від управління інформацією до управління знанням

Оскільки йде безупинний розвиток мережних технологій, відбувається постійне диференціювання і спеціалізація їх компонентів. Збереження даних та їх архівація зараз є насущними проблемами. Великі організації починають зосереджуватися на проблемах збереження і відновлення великої кількості інформації. Ці великі бази даних мають різні найменування: загальні записи (Corporate Memories), тактичні бази даних (Tactical Databases) і військові бази даних (Military Datasets). Безпека збереження даних сьогодні є, мабуть, самим слабким місцем в архітектурі сучасних мережних систем. Ця проблема охоплює такі питання як вартість захоплення, збереження, відновлення і поширення даних та інформації.

Інформація відповідає "що сталося", знання перетворює у "що це означає" з точки зору єдиного спостерігача з його особистими суб'єктивними інтересами і підходами. Таким чином, та сама інформація в залежності від контексту може різними людьми сприйматися зовсім по-різному. Створення контексту до інформації і є основним завданням управління знанням (knowledge management). Управління знанням перевіряє "доречність" інформації в зв'язку з іншою інформацією. Та сама інформація, наприклад, щодо статусу персоналу, у залежності від контексту могла б мати організаційну, тактичну, експлуатаційну, чи стратегічну важливість. Для того, щоб велика кількість інформації мала конкретний сенс, для створення потрібного контексту для сприйняття її користувачем, необхідно використовувати схему-модель, що показувала б характер співвідношення

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

– виявлення, ґрунтуючись на інтуїції, ключових моментів;

– побудова припущень, що пояснюють основні факти;

– одержання, при необхідності, додаткових даних;

– 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 увагу відразу на багатьох, що здатні 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);

– 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, умовно 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 apriori не страждає суб'єктивністю і обмеженістю розуму людини [2-5].

Після проведеного таким чином аналізу фактів на виході маємо ймовірність виникнення загрози того чи іншого виду. Позначимо її як *P(A),*

де *А* – небезпечна подія. Це і є показники типу ЧП1.

Взагалі кажучи, за принципами [2-5] 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 показники ймовірності для небезпечних подій, необхідно обчислити обсяги можливих втрат від їх впливу та прогнози на майбутнє.

Література

1. *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.

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

3. *Ронин Р.* Своя разведка. – Минск. – “Харвест”. – 1997. – С.6-61.

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

5. *Плэтт В.* Стратегическая разведка. Основные принципы. – М.: Издательский дом “ФОРУМ”, 1997. – 376 с.

1.4. Дослідження подій, явищ і процесів

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 галузі та у визначений проміжок часу, що має нечіткі соціальні, економічні або інші наслідки [1].

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 являє 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 являє собою показник небезпеки, комбінована характеристика збитку і повторюваності, тобто середні за одиницю часу втрати (імовірнісний 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

можуть мобілізувати велику кількість ресурсів і синхронізувати дії набагато більш успішно, оскільки вони більше зосереджені на проблемі, ніж обслуговування через деякий час постійної організаційної структури.

Основні зусилля сфокусовані більше на централізацію управління, ніж на спроби інтеграції нових механізмів координації. Існуючий підхід до систем інформаційного контролю і управління (Command and Control Information Systems), що встановлює здатність до взаємодії систем через загальні стандарти вказує на те, що процес думки усе ще строго націлений на технологію керованого рішення. Також важливо і те, що необхідно реорганізувати структури управління, які дозволять більш швидко вирішувати і забезпечувати кращу інтеграцію всіх інформаційних елементів виробництва типу Ops, Plans, Intelligence and Logistic Support. Ця координаційна діяльність повинна включати організаційні елементи типу Personnel і Finance, відповідну зміну, необхідну для прийняття реальної моделі, а також забезпечувати управління і контроль обробки даних.

2.3. Віртуальні інформаційні середовища

Будь-які дії у сучасному обчислювальному середовищі мали б такі істотні елементи:

A. Ієрархія потужних обчислювальних можливостей, доступних усьому персоналу в будь-який час, включаючи портативні комп’ютери, домашні комп’ютери, офісні комп’ютери та різні організаційні та інформаційні послуги. Усі постійні комп’ютери були б фізично зв’язані через дуже високі широкополосні суспільні мережі. Це означає, що вони зв’язані, наприклад, через оптоволоконні кабелі, що дозволяють створювати і передавати велику кількість мультимедійної інформації практично в режимі реального часу окремим користувачам, і також інформація може бути загальнодоступною, якщо вона відповідає іншим типам питань. Переваги в технологіях віддаленого доступу телезв’язку дозволяють доступ до цих ресурсів без використання прямого зв’язку.

B. Використовуються вишукані інтерфейси, що поєднують удосконалені пізнавальні ергономічні проекти концепцій. Таким чином, комп’ютери надзвичайно соціальні. Вони (інтерфейси) були розроблені для задоволення різних способів роботи над конкретними завданнями, передбачені навіть зручності для роботи людей з різних культур. Розвиток Human Computer Interface дозволило розробити стандарт Social User Interface (SUI), що очікує інформаційні вимоги в залежності від типів проблем, над якими працюють, контексту і минулих запитів. Вони підтримують розмаїтість зборів і зв’язку, синтезу і візуалізації Knowbots. Knowbots та інші агенти програмного забезпечення дуже спрощують персональне використання інформаційної технології. Knowbots – програми, призначені для подорожей по мережах, оглядаючи і розуміючи подібні види інформації, незалежно від мови або форми, у якій вони виражені. Knowbots сприймають їх, зв’язуючи інформацію. Вони діють як шаблони, фільтруючи інформацію відповідно до заданих правил і критеріїв. Вони не тільки здійснюють текстовий пошук, але і фокусуються на концепціях. Більшість з цих Knowbots активні навіть тоді,

РОЗДІЛ 2.
ПОТЕНЦІЙНІ ЗАГРОЗИ В КІБЕРПРОСТОРІ І СТРАТЕГІЯ, ТАКТИКА, МИСТЕЦТВО БЕЗПЕКИ ІНФОРМАЦІЇ

2.1. Розвиток комп'ютерного управління

Обчислювальна техніка в даний час завоювала ключові позиції в багатьох сферах людської діяльності.

Комп'ютер існує більш 40 років. Першими машинами, що дозволили втілити в життя обробку інформації, були комп'ютери з архітектурою фон Неймана. Обчислювальна техніка пішла далеко вперед у першу чергу в таких напрямах, як мікроелектроніка, архітектура комп'ютерів, надійність, інформаційні мережі, програмне забезпечення. Він пройшов чотири головних стадії архітектурних перетворень. Тип управління, що здійснюється над процесами, також був результатом певного розвитку. Кожна стадія була більш складною, ніж попередня. Загальна тенденція була до поширення управління, оскільки інформаційні системи розвивалися. Відбувся перехід від особливого, центрального управління і монолітного підходу до більш демократичного "рівний до рівного (peer to peer)" універсального типу управління. Комп'ютерна архітектура пройшла через такі стадії: від "пакетного оброблювача" (Batch Processing) до "розділеного часу" (Time Sharing), потім "робочий стіл" (Desktop), і, нарешті, "мережі" (Network). Найбільш остання модель буде заснована, як найефективніша структура для управління обробкою інформації. Звичайно будуть подальші нововведення, оскільки мережі стануть усюдисущими, але мережна модель буде домінувати над обчислювальною парадигмою протягом наступних років. Зміни будуть мати скоріше кількісний характер, ніж радикальні зміни в самій структурі управління. Інтелектуальні і спільні (кооперативні) інформаційні системи, що використовують агентів програмного забезпечення, розглядаються, як спосіб вирішити існуючі проблеми обмежених баз даних і моделей інформаційної несумісності. Ці спільні зусилля зосереджені на досягненні "семантичної здатності до взаємодії". Але великі труднощі викликає забезпечення загальної інтерпретації даних – проблему "значення" – твердо встановленого структурного стандарту управління мереж. Поширення мереж – ознака успіху.

2.2. Перехід від управління до координації

Розвиток мереж також відрізняється структурою і комплексом завдань, що вирішуються. Інформаційні комп'ютерні мережі зламали строгі структури ієрархій та організаційні межі. Це допомагає створювати віртуальні організації, зосереджені більше на проектуванні і постачанні товарів та послуг. Усі дії подібного "процесу" здійснюються комп'ютерними інформаційними інфраструктурами безпосередньо через мережі. Віртуальні workgroups концентрують свої зусилля на ранніх стадіях планування і вирішенні проблеми. Результат їх праці може бути (або не бути) деяким дорученням організації, на яку вони працюють. У разі потреби (кризи, конфлікту) ці віртуальні workgroups поєднуються. Ці тимчасові організації

та доступності [1].

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 *Мвр.ел* – число вражених елементів, *Мзаг* – загальне число елементів ООТ (або загальне число елементів ООТ, які опинилися в сфері ураження).

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

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

де *Yn(A) – умовний повний збиток*, який чисельно рівний кількості або вартості всіх елементів ООТ (або кількості чи вартості тих елементів ООТ, які опинилися в сфері 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. Тоді ця формула набуває такого вигляду:

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

де *Rч(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. 8).

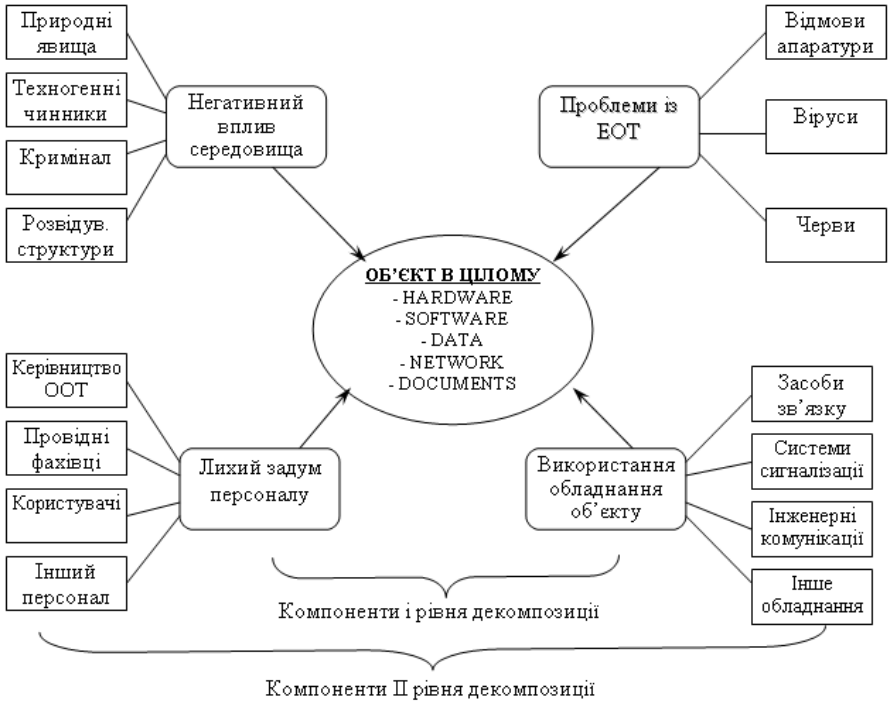

Рис. 8. Схема нарахування загального ризику.

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

Зазначимо, що кількість компонентів кожного з 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 іншим ознакам. Існують різні – відомчі (галузеві), національні та міжнародні системи класифікації таких подій, і вибір тієї чи іншої з-поміж них, на думку автора, залежить від конкретного частинного випадку.

а системи безпеки реагують на кожну з таких подій.

Тому подамо ще один, більш практичний варіант функції безпеки/ризику, що ґрунтується на застосуванні розподілу Ерланга.

Суть у такому. Системи безпеки реагують на можливу загрозу тільки в тому випадку, коли ймовірність виникнення небезпечної події *i*-го виду (наприклад, в певні дні тижня чи пору доби) перевищує гранично допустимий рівень. У такому разі середній інтервал між подіями, незалежно від значення їх ймовірності, дорівнює

$$\tau = \frac{1}{\lambda_i} \quad , \qquad (13)$$

де *λi* – інтенсивність потоку подій , обчислена за формулою (9).

Тоді часткова функція безпеки для загроз *i*-го виду дорівнює

$$F_i(t) = k\lambda_i \frac{(k\lambda_i t)^{k-1}}{(k-1)!} e^{-k\lambda_i t} \quad , \qquad (14)$$

де *k* – *порядок* потоку. Для обчислень можна за порядок приймати частоту повторення подій з ймовірністю вище допустимої (наприклад, кожна друга (*k*=2), кожна п'ята (*k*=5) і т.д. Сумарні ж функції обчислюються аналогічно до (11) і (12) як добутки відповідних часткових функцій.

Необхідно зазначити, що забезпечення безпеки може бути досягнуто 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 потрібно керуватися таким.

По-перше, до оцінки ризику необхідно вводити весь спектр небезпек, можливих для досліджуваного об'єкту при його роботі (див. рис. 2).

По-друге, заходи щодо зниження ризику приймаються на найбільш несприятливих напрямах (див. вище). При виборі заходів захисту перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

По-третє, як вже було сказано, для більш точного відтворення „потоку" небезпечних подій та їх впливу на роботу фірми, використовувати інші типи потоків подій, беручи за основу наведений вище матеріал.

Література

1. *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. – в. 13. – С.127-135.

1.5. Прогнозування подій, явищ і процесів

Розглянемо динаміку зміни небезпечних подій у часі. Якщо розуміти під безпекою відсутність неприпустимого ризику враження 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 у [1] "потік" небезпечних подій було запропоновано 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□□*i*□– інтенсивність небезпечних подій *i*-го виду; □*ij* – ймовірність враження подією *i*-го виду *j*-ї компоненти досліджуваного об'єкту.

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

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

Можна вважати, що

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

де *nij* – число "НП" *i*-го виду, які привели до враження *j*-ї компоненти; *ni* – загальне число "НП" *i*-го виду, *n* – число джерел небезпеки для даного об'єкту.

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 *Sj(t), Hj(t)* – функції безпеки і ризику для *j*-го компоненту об'єкта;

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

Але пуассонівський потік має серйозні обмеження щодо застосування на практиці, головне з яких – прийнято, що події відбуваються рівномірно у часі,

1.4.1. Комплектування системи захисту

Таким чином, нам відомі найбільш ймовірні загрози та орієнтовні обсяги втрат, які можуть бути ними завдані. Тепер співставимо отримані показники з 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 даного завдання в аспекті багатокритеріальної оптимізації. Природніше звести її до однокритеріальної. Проте при однокритеріальній постановці завдання без відповіді залишаються такі запитання: якою ціною досягається бажаний результат; в якій мірі погіршуються інші критерії якості; чому перевага віддана цьому, а не іншому критерію?

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

ДАНО:

1. 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 із результатів попереднього етапу необхідно надати системі *S* для забезпечення її безпеки;

– вектор значень $\vec{U} = < u_1, u_2, ...u_m, ...u_M >$, де *um* – значення потреби системи *S* в *m*-му вигляді обчислювального ресурсу для її нормального функціонування;

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

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 $a_{ir} \in h_i$ – безвихідність обраної підмножини *hi*;

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 *Сзад* – 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 *zk*, ($k = \overline{1,K}$), 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

дорівнюватиме:

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

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

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

де *L* – шуканий показник досліджуваної матриці, *m* – число елементів, які піддавалися оцінці, *n*- число можливих значень оцінок, *Wi*- „вага” *i*-го елементу, *Bj** – значення оцінки за бальною шкалою, *aij* – відповідний елемент матриці інцидентності, який, як вже було сказано, приймає значення 0 або 1.

Ми отримали показник ЧП4. Він дорівнює *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 об’єкту ззовні або протистояння цій загрозі.

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

1. Робити висновок про можливість чи неможливість обробки на даному об’єкту в даних умовах інформації певної важливості в певних обсягах.

2. Відпрацьовувати пропозиції і плани з покращення захищеності об’єкту 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.

Література

1. *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. – в. 13. – С. 127-135.

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

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 із 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:

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

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. [2].)

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

Таблиця 2

Елементи, що оцінюються	***Рівень* пріоритетності**	**"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 (найнижчий)	0	0	0	1
Елем. *m*		0	0	0	1

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

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

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

Враховуючи умову (7), маємо:

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

Звідси, коефіцієнт пропорційності γ для досліджуваної матриці

елемент $a_j \in h_i$ такий, що *qjk=1*. Мінімальність покриття інтерпретується як відсутність зайвого рядка у вибраній сукупності (умова б) у вимогах до підмножини *hi*).

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 *an*, $n = \overline{(1,N)}$. Модуль *an* є базовим, якщо існує стовпець *zj* такий, що *qnj =1* і *qij =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 з матриці інцидентності;

3. Зменшити розмірність матриці *Q*, отриманої у п. 2, шляхом послідовного викреслення лишніх стовпців, а потім – лишніх рядків. Стовпець *zk* є лишнім, якщо існує стовпець *zj* такий, що *qnk =qnj* для всіх залишившихся рядків *an*. Рядок *an* є зайвим, якщо *qnk =0* для всіх залишившихся стовпців *zk*;

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 *zk*, який залишився, диз'юнктивний терм утворюють тільки ті змінні *an*, для яких *qnk =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) з вище сформульованих вимог до рішення. В підмножині *H={hi}* залишити варіанти, які задовольняють згадані умови;

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

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

Приклад 1.

Нехай після виконання п. 4. отримана така матриця інцидентності

	z_1	z_2	z_3	z_4	z_5
a_1	1	0	0	0	0
a_2	0	1	0	0	1
$Q = a_3$	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

З матриці слідує, що потрібна послуга *z1* може бути забезпечена модулями *a1* або *a4*, тобто один з 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, *a1* або *a4*, покриє стовпець *z1*. Аналогічно, умова забезпечення послуги *z2* подається диз'юнктивним термом $a_2 \vee a_3 \vee a_5$. Покриття всіх стовпців матриці інцидентності подається таким булевим виразом:

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

Розкриваючи дужки в цьому виразі та використовуючи основні співвідношення алгебри логіки в 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:

h1 = { a2, a4, a5}; h2 = { a1, a3, a5};

h3 = { a3, a4, a5}; h4 = { a1 ,a2, a5 ,a6}.

Це набір ЧПЗ. Далі необхідно провести аналіз цих варіантів для визначення їх входження в зону 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 на досліджуваному об'єкті.

1.4.2. Оцінка системи захисту

Кожному із елементів множин *h1-h4* (див. приклад) 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 з 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 *Свст*;

– імовірність відмови захисного засобу або виникнення неконтрольованої небезпечної ситуації *Рвідм* зовні або всередині об'єкту;

– нанесені збитки в разі успішної реалізації загрози *Zmax.*, тобто в тому разі, коли *Рвідм =1*.

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

$$Zcep = Zmax * Рвідм. \qquad (13)$$

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

$$Рст = 1 - Рвідм. \qquad (14)$$

Тоді ефективність захисту становитиме:

$$Эзах = Рст * Zcep \qquad (15)$$

Звідси, значення абсолютної оцінки стійкості елементу:

$$B = \frac{\text{Эзах}}{\text{Свст}} \qquad (16)$$

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 з множин *h1-h4*: розставивши по колонкам можливі значення оцінок в порядку спадання зліва направо (*n*), а по рядкам – елементи множин *h1-h4* (*m*) в порядку зменшення їх важливості (пріоритетності).

За означенням, елемент матриці прийматиме значення:

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