УДК 354.31(477)(004.7+65.012.8)

В.А. Кудінов,
кандидат фізико-математичних наук, доцент

ОЦІНКА КОЕФІЦІЄНТА ОПЕРАТИВНОЇ ГОТОВНОСТІ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ДО ЗАХИСТУ ТИПОВОГО ВУЗЛА ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ З ОБРОБКИ ІНФОРМАЦІЇ

У статті розглянуто шість послідовних зон захисту апаратно-технічних засобів та програмного забезпечення з обробки інформації для типового вузла інтегрованої інформаційно-пошукової системи органів внутрішніх справ України. Отримана формула для підрахунку коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла інтегрованої інформаційно-пошукової системи органів внутрішніх справ України з обробки інформації.

Ключові слова: *апаратно-технічні засоби, інформація, захист інформації, обробка інформації, організаційні заходи захисту інформації.*

В статье рассмотрены шесть последовательных зон защиты аппаратно-технических средств и программного обеспечения обработки информации для типового узла ИИПС ОВД Украины. Получена формула для подсчета коэффициента оперативной готовности организационных мероприятий для защиты типового узла интегрированной информационной поисковой системы органов внутренних дел Украины при обработке информации.

Ключевые слова: *аппаратно-технические средства, информация, защита информации, обработка информации, организационные мероприятия по защите информации.*

Six successive zones of the defence of vehicle, technical facilities and treatment of information software for the model knot of the integrated IRS of organs of internal affairs of Ukraine are considered. A formula is got for the count of a coefficient of operative readiness of organizational measures on the defence of a model knot of the integrated IRS of the organs of internal affairs of Ukraine at treatment of information.

Keywords: *vehicle and technical facilities, information, priv, treatment of information, organizational measures on a priv.*

Серед основних напрямів державної інформаційної політики в Україні, відповідно до оновленого Закону України “Про інформацію” [1], є створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України. Не залишається осторонь цих завдань і Міністерство внутрішніх справ (МВС) України [2].

Від початку процесу інформатизації органів та підрозділів внутрішніх справ (ОВС) України минуло вже 40 років. За цей час накопичений чималий досвід використання різноманітних інформаційних систем оперативно-розшукового та інформаційно-довідкового призначення [3, 4]. Так, зокрема, на виконання Указу Президента України від 20 жовтня 2005 року № 1497 [5] наказом МВС України від 07 червня 2006 року № 571 була затверджена Програма створення Інтегрованої інформаційно-пошукової системи (ІІПС) ОВС України [6, 7], якою передбачено створення та впровадження типового програмного забезпечення системи, єдина технологія оброблення даних, інтеграція всіх інформаційних обліків до системи та єдина технологія обміну інформацією між центральним та локальними вузлами системи, побудова єдиної цифрової відомчої телекомунікаційної мережі МВС України до рівня міськрайлінорганів, створення комплексної системи захисту інформації (КСЗІ).

Протягом останніх років Департамент інформаційно-аналітичного забезпечення (ДІАЗ) МВС України [8] створив та впровадив в діяльність ОВС України зазначену ІІПС [9, 10]. Для ефективного її функціонування важливе значення має створення та постійне вдосконалення КСЗІ. Тобто, працівникам ДІАЗ МВС України необхідно постійно вживати комплекс відповідних заходів щодо вирішення проблеми забезпечення належного захисту апаратно-технічних засобів та програмного забезпечення з обробки інформації типового вузла ІІПС ОВС України. Зазначена проблема є актуальною не тільки для системи МВС України. В органах державної влади є майже 40 інформаційних ресурсів баз даних, які становлять найбільший інтерес для правоохоронних органів і в подальшому повинні бути об'єднані в Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю [11].

В літературі існують різні визначення поняття КСЗІ. Це, зокрема:

1) сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в системі [12]; 2) сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [13]; 3) сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Таким чином, забезпечення безпечного функціонування типового вузла ІІПС ОВС України повинно вирішуватися в трьох аспектах: правовому, організаційному та технічному. При цьому однією з важливих характеристик КСЗІ є коефіцієнт оперативної готовності організаційних заходів до захисту типового вузла ІІПС ОВС України з обробки інформації, дослідження якого в літературі відсутнє, що і було метою даної статті.

Інтегрована інформаційно-пошукова система ОВС України – це сукупність організаційно-розпорядчих заходів, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІІПС [6, 9, 10].

Метою створення ІІПС є об'єднання існуючих в ОВС України інформаційних ресурсів в єдиний інформаційно-аналітичний комплекс із використанням сучасних інформаційних технологій, комп'ютерного та телекомунікаційного обладнання для підтримки оперативно-службової діяльності органів і підрозділів внутрішніх справ, суттєвого зміцнення їх спроможності протидії та профілактики злочинності [6]. *Призначення ІІПС* – це інформаційно-аналітичне та організаційно-технологічне забезпечення службової діяльності структурних підрозділів районних, міських, лінійних управлінь (відділів) Головних управлінь, управлінь МВС України в Автономній Республіці Крим, областях, містах Києві та Севастополі, на залізницях (далі – ГУМВС, УМВС), центрального апарату МВС України.

Структура ІПС побудована за трирівневою ієрархічною моделлю, що відповідає організаційній побудові МВС України [2, 10]: 1) перший рівень – це центральний вузол (банк даних) ІПС, який розташований в спеціально виділених службових приміщеннях ДІАЗ МВС України; 2) другий рівень – це регіональні (обласні) вузли (банки даних) ІПС, які розташовано в спеціально виділених службових приміщеннях Управлінь або відділів інформаційно-аналітичного забезпечення ГУМВС, УМВС; 3) третій рівень – це територіальні вузли ІПС, які розміщені і функціонують безпосередньо в районних, міських, лінійних управліннях (відділах) ГУМВС, УМВС. На територіальному рівні експлуатація ІПС забезпечується відділами (секторами) інформаційно-аналітичного забезпечення цих підрозділів.

До складу зазначених вузлів ІПС входить низка відповідних серверів та автоматизованих робочих місць (АРМ) працівників [10]. Так, наприклад, до територіального вузла ІПС входять: 1) АРМ, які забезпечують авторизований доступ користувачів ІПС міськрайлінорганів ГУМВС, УМВС до формування та використання інформаційних ресурсів (баз даних) регіонального вузла ІПС; 2) територіальний сервер, що складається з технологічного сервера, спеціального програмного забезпечення, призначеного для виконання технологічних операцій, що забезпечують функціонування, відновлення, архівне збереження АРМ територіального вузла ІПС. Обмін інформацією між вузлами та доступ користувачів до ІПС забезпечується засобами єдиної цифрової телекомунікаційної мережі МВС та локальними обчислювальними мережами центрального апарату МВС, апаратів і районних, міських, лінійних управлінь (відділів) ГУМВС, УМВС.

Для спрощення дослідження розглянемо узагальнений типовий вузол ІПС ОВС України, який містить деякі апаратно-технічні засоби та програмне забезпечення з обробки інформації (далі – об'єкти захисту). Організаційні заходи для їх захисту передбачають побудову низки зон захисту, в яких функціонують відповідні засоби охорони. В загальному випадку можна виділити шість послідовних зон захисту об'єктів захисту типового вузла ІПС ОВС України, які зображені на рис. 1, а саме:

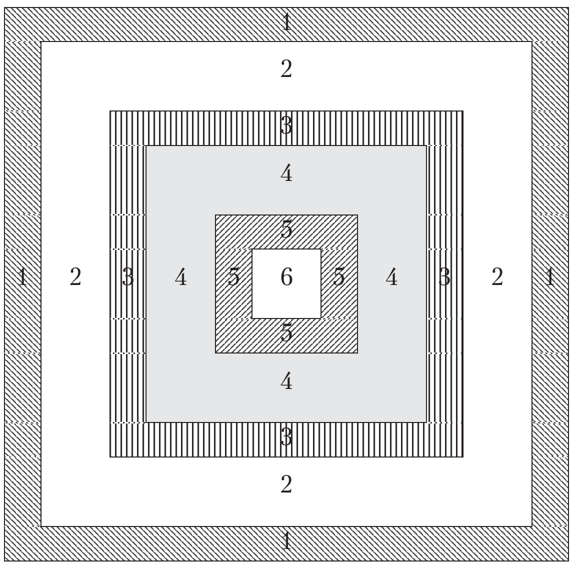

Рис. 1. Зони захисту апаратно-технічних та програмних засобів типового вузла ІПС ОВС України, де: 1 – периметр території; 2 – територія; 3 – периметр будинку; 4 – внутрішній об'єм будинку; 5 – периметр приміщення; 6 – приміщення з програмно-апаратними засобами.

Надамо характеристику цим зонам захисту, а саме: 1 – це периметр території, де знаходяться об'єкти захисту (використовуються засоби інженерного захисту, зокрема, огорожі, засоби телеспостереження по периметру, засоби охорони периметру, а також фізична охорона); 2 – це територія, де знаходяться об'єкти захисту (використовуються технічні засоби охоронної сигналізації, засоби телеспостереження тощо); 3 – це периметр будинку, де знаходяться об'єкти захисту (використовуються засоби телеспостереження, замки, домофони, різні методи автентифікації, фізична охорона тощо); 4 – це внутрішній об'єм будинку, де знаходяться об'єкти захисту, в якій, як правило, є зони вільного та обмеженого доступу для працівників (використовуються засоби телеспостереження тощо); 5 – це периметр приміщення, де знаходяться об'єкти захисту (використовуються засоби, які аналогічні п. 3); 6 – це приміщення, де знаходяться об'єкти захисту (використовуються засоби телеспостереження, апаратні та програмні засоби захисту тощо).

Для оцінки коефіцієнта оперативної готовності організаційних заходів до захисту апаратно-технічних засобів та програмного забезпечення типового вузла ІПС ОВС України проаналізуємо послідовність подій при проникненні порушника на об'єкт захисту, що зображена на рис. 2, та реагування на це системи охорони. Даний коефіцієнт буде визначатися достовірністю того, що група охорони об'єкту захисту своєчасно прибуде на місце виникнення загрози згідно заданого часу.

Достовірність виявлення групою охорони порушника, який намагається проникнути на об'єкт захисту, визначається як $P\{T_{пер}>T_з\}$, де $T_{пер}$ – час перебування порушника в зоні, що охороняється; $T_з$ – заданий час прибуття групи охорони.

Нехай P_i – достовірність виявлення порушника в i-й зоні ($i=\overline{1{,}6}$), причому $\sum_i P_i = 1$. Час прибуття групи охорони в i-у зону $t_{пi}$ є випадковою величиною.

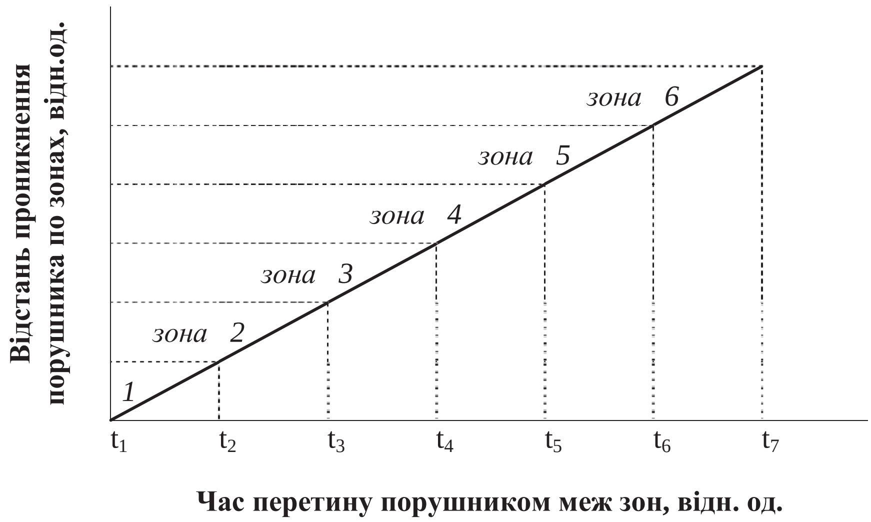

Рис. 2. Послідовність подій під час проникнення порушника на об'єкт захисту.

Середньозважений час прибуття групи охорони після сигналу спрацьовування засобів сигналізації можна визначити за формулою

$$t_п = P_1 t_{п1} + P_2 t_{п2} + ... + P_6 t_{п6} .$$

Функція розподілу середньозваженого часу прибуття групи охорони $t_п$ розрахуємо за формулою

$$F_n(t) = P\{t_n<t\} = P_1F_{n1}(t) + P_2F_{n2}(t) + \dots + P_6F_{n6}(t),$$

де $F_{ni}(t) = P\{t_{ni}<t\}$ − функція розподілу випадкової величини t_{ni} .

Якщо випадкова величина t_{ni} розподілена за експоненціальним законом $F_{ni}(t) = 1 - exp(-_i t)$, , де l_i − інтенсивність прибуття групи охорони на місце виникнення загрози, то

$$F_n(t) = \frac{\sum_{i=1}^{6} \lambda_i F_{ni}(t)}{\Lambda},$$

$$\Lambda = \sum_{i=1}^{6} \lambda_i .$$

Тоді коефіцієнт оперативної готовності організаційних заходів до захисту апаратно-технічних засобів та програмного забезпечення з обробки інформації типового вузла ІПС ОВС України визначається формулою

$$K_{оз}(T_з) = F_П(T_з) = P\{t_п \rangle T_з\} = \frac{\sum_{i=1}^{6} \lambda_i F_{ni}(T_з)}{\Lambda}.$$

Таким чином, можна розрахувати достовірність того, що група охорони своєчасно з’явиться на місці виникнення загрози відповідно до заданого часу.

У загальному випадку можна розглядати шість послідовних зон захисту апаратно-технічних засобів та програмного забезпечення з обробки інформації типового вузла ІПС ОВС України. Отримана формула для підрахунку коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла ІПС ОВС України з обробки інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про внесення змін до Закону України “Про інформацію” : Закон України від 13 січня 2011 року // Офіційний вісник України від 18.02.2011. − 2011. − № 10. − Стор. 21. − Ст. 445.

2. Про затвердження Положення про Міністерство внутрішніх справ України : Указ Президента України від 6 квітня 2011 року № 383.

3. Системна інформатизація правоохоронної діяльності / [М. Швець, С. Антоненко, В. Буржинський та ін.] ; за ред. В. Дурдинця, В. Євдокимова, М. Швеця. − К. : НДЦПІ АПрН України, 2006. − 287 с.

4. Від арифмометра до високих технологій / [С.П. Черних, О.М. Іщенко, І.А. Аршинов та ін.]. − К. : Преса України, 2012. − 1112 с.

5. Про першочергові завдання щодо впровадження новітніх інформаційних технологій : Указ Президента України від 20 жовтня 2005 року № 1497.

6. Про створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Наказ МВС України від 18 липня 2003 року № 786.

7. Про затвердження Програми створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Наказ МВС України від 7 червня 2006 року № 571.

8. Про затвердження Положення про Департамент інформаційно-аналітичного забезпечення МВС України : Наказ МВС України від 29 квітня 2011 року № 174.

9. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : Наказ МВС України від 12 жовтня 2009 року № 436.

10. Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Наказ МВС України від 10 березня 2010 року № 75.

11. Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю : Указ Президента України від 31 січня 2006 року № 80.

12. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

13. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року (в редакції Закону № 2594-IV від 31 травня 2005 року) // Відомості Верховної Ради України (ВВР). – 2005. – № 26. – Ст. 347.

Отримано 11.06.2013