Список литературы

1. State of the Practice of Intrusion Detection Technologies. J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. CMU/SEI Technical Report (CMU/SEI-99-TR-028), 2000. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/ids-state.pdf>.
2. Sobirey, Michael. Michael Sobirey's ID Systems Page, 2000. <URL: http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html>.
3. Becky Base and Peter Mell, Intrusion Detection Systems, National Institute of Standards and Technology Special Publication 800-31, 2001. <URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
4. Research in Intrusion Detection Systems: A Survey. S. Axelsson. Technical Report, 1999. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/ids_research_survey.ps.gz>.
5. A Revised Taxonomy for Intrusion-Detection Systems. H. Debar, M. Dacier, and A. Wepsi. IBM Research Report, 1999. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/IDS_taxonomy.ps>.
6. Balasubramaniyan, Jai, et al. (Purdue University). An Architecture for Intrusion Detection Using Autonomous Agents (Coast TR 98-05). West Lafayette, IN: COAST Laboratory, Purdue University, 1998. <URL: http:/ /www.cs.purdue.edu/coast/projects/autonomous-agents.html>.

Поступила 17.05.2004

УДК 65.012.8:354.31(477)

В.О. Хорошко, В.А. Кудінов

МЕТОДИЧНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ ЗАДАЧІ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОВС УКРАЇНИ

Вступ

Інформаційну систему (ІС) органів внутрішніх справ (ОВС) України розглядають як систему інформаційного забезпечення ОВС – це сукупність інформаційних автоматизованих підсистем певних обліків, призначених для збирання, накопичення, зберігання, обробки та використання інформації в діяльності підрозділів та служб ОВС України [1]. Вона здійснює всебічну інформаційну підтримку їх практичної діяльності у розкритті, розслідуванні та попередженні злочинів, встановленні і розшуку злочинців, надає багатоцільову статистичну, аналітичну та довідкову інформацію.

Подальший розвиток системи інформаційного забезпечення ОВС передбачений Програмою інформатизації органів внутрішніх справ України на 2000-2005 роки [2], яка містить розділ "Розробка та впровадження стратегії захисту інформації в інформаційній мережі ОВС України". У пункті 1 цього розділу передбачено: "Розробити концепцію комплексного захисту інформаційної системи ОВС України з метою забезпечення обробки конфіденційної інформації в інформаційних підсистемах ОВС України". У зв'язку з необхідністю виконання цього завдання дослідження проблеми оцінювання ефективності системи захисту інформаційної системи ОВС України є дуже актуальною проблемою.

Крім цього, робота відповідає тематиці приоритетних напрямів фундаментальних та прикладних досліджень вищих навчальних закладів та науково-дослідних установ МВС України на період 2002-2005 роки, яка затверджена наказом МВС України від 30 червня 2002 року № 635 [3]. Зокрема, у додатку 2 до наказу визначений такий напрям наукового дослідження: "Проблеми захисту інформації обмеженого користування в діяльності ОВС" (розділ 2, п.2.4).

Загальне дослідження стійкості багаторубіжної комплексної системи технічного захисту інформації проти дій зловмисника й ефективності розподілу її ресурсів між

рубежами захисту при спрямованому і сконцентрованому подоланні визначеного рубежу наведено в роботі [4]. Аналізу проблем створення захисту конфіденційної інформації, що обробляється в системі оперативного інформування МВС України, присвячена робота [5].

Ціль даної статті – розробити методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України.

Постановка задачі та шляхи її вирішення

Інформаційна система ОВС України будується за територіальним рівнем та має три рівня у своїй структурі, а саме: 1.) центральний (рівень Міністерства внутрішніх справ України) – призначений для інформаційного забезпечення галузевих служб міністерства, підрозділів ОВС України, а також для інформаційної взаємодії з правоохоронними органами; 2.) регіональний або обласний (рівень Головних Управлінь (Управлінь) МВС України в областях та на транспорті) – забезпечує інформаційну взаємодію між обласними галузевими службами, територіальними і центральною інформаційними мережами ОВС та правоохоронними органами; 3.) територіальний (рівень міськрайлінорганів Головних Управлінь (Управлінь) МВС України в областях) – є складовим регіональних мереж і забезпечує інформаційну взаємодію між підрозділами міськрайлінорганів.

При формалізації задачі оцінювання ефективності системи захисту ІС ОВС України будемо вважати, що система будується у вигляді багаторівневої ієрархії I_p, де p – кількість рівнів ієрархії (у нашому випадку p=3).

Для інформаційних підсистем на кожному р-му рівні ієрархії вибирається множина об'єктів захисту $M_{кр}$, де к – номер об'єкта на р-му рівні ієрархії. За допомогою експертного оцінювання для кожного $M_{кр}$ об'єкта формується вектор загроз V_{skp}, де s – номер загрози для к-го об'єкта на р-му рівні ієрархії.

Зниження ефективності функціонування інформаційної системи на кожному р-му рівні ΔE_p визначається складним впливом реально діючих загроз на об'єкти р-го рівня, тобто:

$$\Delta E_p(t) = F\{ M_{кр}, V_{skp}, t\}, \qquad (1.1)$$

де F {*} – функціонал, що описує вплив реально діючих загроз V_{skp} на множину об'єктів $M_{кр}$ в підсистемі р-го рівня; t – часова характеристика.

Будемо вважати, що відновлення ефективності підсистеми р-го рівня (тобто, автоматизованої інформаційної системи – АІС) можливо лише за рахунок проведення адекватного рівню інтегральної загрози комплексу заходів безпеки Z_{jkp}, де j – номер заходу безпеки Z стосовно к-го об'єкта підсистеми р-го рівня. Для ідеального випадку цей постулат можна записати у вигляді:

$$\Sigma Z_{jkp}(t): \Delta E_p(t) = 0, \text{ де } j = 1,2,\ldots J;\ k = 1,2,\ldots K;\ t > 0, \qquad (1.2)$$

що читається так: "комплекс J заходів безпеки стосовно К об'єктів підсистеми р-го рівня нейтралізує дію інтегральної загрози, яка знизила ефективність інформаційної системи на величину ΔE_p на момент часу t."

Звідси можна записати функцію управління безпекою підсистеми р-го рівня інформаційної системи ОВС України:

$$\Sigma Z_{jkp}(t): \Delta E_p(t+\Delta t) \le \Delta E_p(t), \text{ де } j = 1,2,\ldots J;\ k = 1,2,\ldots K;\ t > 0, \qquad (1.3)$$

де Δt – час реакції системи на виявлену загрозу.

Практика показує, що для розв'язування задач такого класу відомі методики й алгоритми формально не можуть бути подані суворими математичними виразами та співвідношеннями типу (1.1) та (1.2). Оскільки вхідними даними у подібних задач класу являються повільно мінливі у часі процеси з нечіткими кількісно-якісними параметрами, з різним ступенем достовірності, а в багатьох випадках і дезінформаційного змісту, а вихідними даними повинні бути кількісні, якісні і кількісно-якісні результати, то необхідно вибрати відповідний науково-методичний апарат (НМА) для їх отримання.

Основними вимогами, що пред'являються до науково-методичного апарату [6], який використовується для розв'язання подібних задач, є виявлення, аналіз і оцінка можливих загроз АІС, їх характеру і рівнів, аналіз причин їх виникнення і оцінка дестабілізуючих чинників, попередні оцінки їхнього спрямування та наслідків проявлення, прогнозування

тенденцій змін криміногенної обстановки та активності порушників, появи можливих загроз та оцінка їх рівнів, а також можливість обгрунтування порогів реагування на виявлений рівень інтегральної загрози ІС ОВС України.

Широко відомий НМА [7], що використовується для рішення таких задач, базується, як правило, на методах експертного оцінювання, проб і помилок, що вносить елементи суб'єктивізму в розрахунки і супроводжується досить великими похибками.

Оскільки задача оцінювання рівня інтегральної загрози АІС у формальному виді представляється у вигляді 3-рівневої ієрархічної задачі (рис. 1.1) [6], то для її вирішення доцільно вибрати НМА [7-9], який базується на використанні методів дослідження операцій, аналізу ієрархій, векторної алгебри, експертного оцінювання і математичного моделювання.

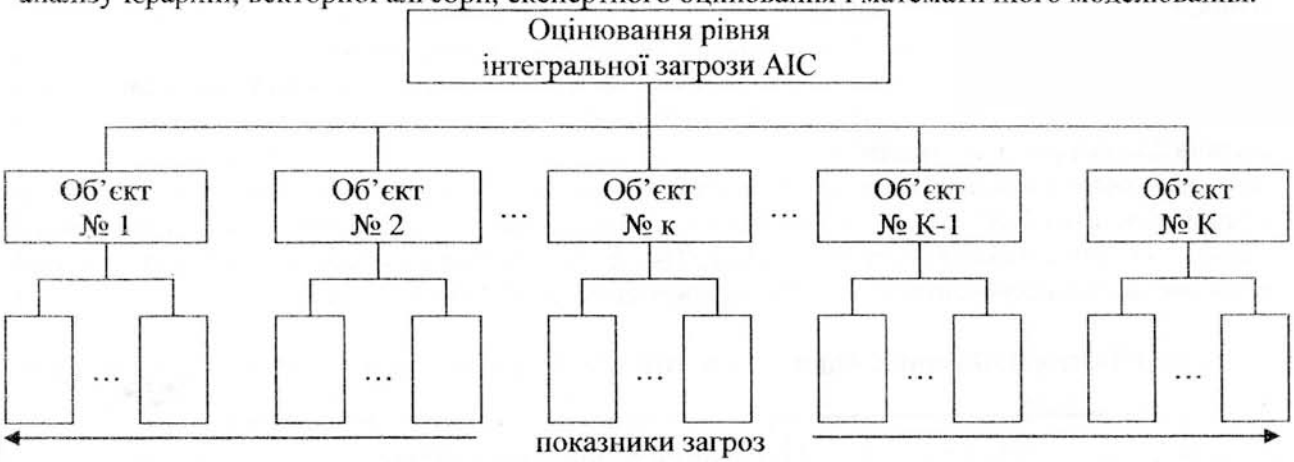

Рис. 1.1. Ієрархія побудови задачі оцінювання рівня інтегральної загрози АІС

Вибраний НМА дозволяє на основі всебічного аналізу проявів загроз об'єктам захисту отримувати кількісні оцінки рівня інтегральної загрози U, що еквівалентно оцінці зниження ефективності ІС в цих умовах (U ~ ΔE).

Пропонується при рішенні задачі вибрати 3 рівні ієрархії (див. рис. 1.1):

1-й рівень – формулюється мета оцінювання;

2-й рівень – визначається множина $\{M_к\}$ об'єктів захисту відповідної підсистеми, яким можуть проявлятися загрози;

3-й рівень – визначаються показники прояву загроз функціонуванню об'єктів у складі підсистеми, що розглядається.

Вибраний НМА дозволяє отримувати на вибраний момент оцінювання t кількісне значення підсумкового рівня інтегральної загрози U в системі координат: рівень загрози – час. На рис.1.2 наведено гіпотетичний приклад оцінки зростання рівня інтегральної загрози U на інтервалі $[T_0, T_1]$.

Рис. 1.2. Гіпотетичний приклад з оцінки зростання рівня інтегральної загрози U на інтервалі $[T_0, T_1]$

Для якісного та всебічного оцінювання рівня інтегральної загрози U необхідно вибрати достатньо повну систему (вектор) показників прояву загроз об'єктам захисту. Слід зауважити, що для кожної підсистеми такий вектор має бути свій. Для полегшення побудови ієрархії пропонується типова (базова) система показників, яку в кожному конкретному випадку доповнюють або скорочують відповідно до обстановки та регіону (області), по відношенню до якої організовується згадане оцінювання.

Оцінювання рівня загрози к-му об'єкту (к=1,2…К) здійснюється по сукупності окремих показників U_{kn} для відповідного об'єкта. Кожний n-й показник відображає події, що зв'язані із зростанням (дійсним чи імітованим) загрози функціонуванню підсистеми АІС р-го рівня, яка розглядається.

Об'єкти захисту АІС ОВС України та типові загрози для них

Дійсні події спостерігаються в ході повсякденної діяльності підсистеми, а імітовані – нав'язуються ОВС та суспільству для приховування істинних намірів щодо вибору сил та засобів для порушення роботи АІС.

На основі аналізу подій, що характеризували прояви небажаного впливу на аналогічні за призначенням АІС деяких провідних країн світу в останнє десятиліття, була сформована базова множина (вектор $U_k = U_1,..., U_n,..., U_N$, де N – розмірність вектора для к-го об'єкта) показників для оцінювання рівня інтегральної загрози АІС ОВС України.

Таблиця 1 Вектор показників оцінювання загроз автоматизованим інформаційним системам (U_{AIC})

№ з/п	Показники оцінювання загроз
1.	несанкціонований доступ до конфіденційної інформації сторонніх осіб та користувачів АІС;
2.	перехват за рахунок несанкціонованих підключень інформації, що циркулює в корпоративній телекомунікаційній мережі та локальних обчислювальних мережах ОВС України, або передається комутованими каналами електронної пошти та телефонними голосовими каналами;
3.	зараження інформаційної системи програмними кодами, направленими на завдання шкоди (віруси, "троянські коні" тощо);
4.	несанкціоноване копіювання, спотворення або знищення інформації;
5.	викрадення носіїв інформації;
6.	техногенні фактори – збої комп'ютерного обладнання, дискових систем, систем резервного копіювання, елементів кабельної системи, активного обладнання мережі, перебої електроживлення, пожежі, повені, надмірна вологість, запилення тощо;
7.	втрати інформації через некоректну роботу програмного забезпечення;
8.	помилки обслуговуючого персоналу ("людський фактор"): випадкове знищення або зміна даних; некоректне використання програмного забезпечення та апаратних засобів, що веде до зміни, знищення даних та появи каналів витоку інформації; втрати інформації, пов'язані з неправильним застосуванням систем резервного копіювання та неправильного збереження резервних копій; помилки в адмініструванні інформаційної системи та баз даних тощо;
9.	повторне використання об'єктів (тимчасових файлів тощо);
10.	хакерські атаки через локальну (корпоративну, Інтернет) мережу;
11.	перехват інформації по каналах побічних електромагнітних випромінювань, наведень та по відвідним колам.

Таблиця 2 Вектор показників оцінювання загроз структурним підрозділам персоналу і працівникам ($U_{сп}$)

№ з/п	Показники оцінювання загроз
1.	відсутність підготовленого персоналу;
2.	несвоєчасне призначення (непризначення) посадових осіб, відповідальних за захист інформації, адміністрування, здійснення контролю, технічне обслуговування, реєстрацію та облік;
3.	тимчасова відсутність посадової особи, що виконує ключову роль в тому чи іншому процесі обробки інформації і не може бути замінена іншою особою із-за режимних обмежень або недостатку досвіду;
4.	відсутність контролю з боку керівництва, режимно-секретних органів, підрозділів технічного захисту інформації, відповідальних посадових осіб або формальність, недостатність такого контролю;
5.	невиконання, неякісне виконання керівництвом, персоналом та користувачами своїх обов'язків, інструкцій, встановлених вимог, ігнорування обов'язків, організаційних обмежень, правил;
6.	необізнаність персоналу та користувачів з покладеними на них обов'язками;
7.	незнання (в межах покладених на особу завдань) вимог чинних нормативно-правових актів, положень, інструкцій тощо;
8.	комп'ютерна, технічна неграмотність, незнання технічної, експлуатаційної документації, опису програм і т.ін.;
9.	невміння працювати з програмними і технічними засобами;
10.	відсутність політики безпеки, плану захисту інформації, однозначних інструкцій і правил, їх недостатня повнота та взаємна неузгодженість;
11.	відсутність або недостатність документації на АІС;
12.	неправильна організація роботи декількох користувачів на одному робочому місці;
13.	втрата засобів розмежування доступу;
14.	втрата матеріальних носіїв, що містять інформацію про систему захисту в АІС, користувачів, технічне, програмне забезпечення тощо;
15.	помилки користувачів під час введення даних в систему;
16.	помилки при конфігуруванні, неправильне використання настроювання або неправомірне відключення засобів захисту;
17.	порушення порядку зберігання та обліку: документів, носіїв інформації, даних, технічних засобів;
18.	порушення порядку доступу в приміщення;
19.	порушення порядку допуску до інформації з обмеженим доступом та матеріальних носіїв;
20.	виведення даних за невірними адресами;
21.	порушення технології друкування;
22.	порушення порядку копіювання інформації;
23.	порушення порядку передачі матеріальних носіїв інформації;
24.	видалення файлів без фізичного стирання інформації;
25.	порушення порядку передачі технічних засобів в ремонт;
26.	порушення порядку організації технічного обслуговування та відновлювальних робіт;
27.	дії, що приводять до відмови АІС або окремих її елементів;
28.	виведення з ладу технічних засобів та носіїв інформації;
29.	порушення режимів функціонування АІС;
30.	несанкціоноване копіювання вихідних документів;
31.	розкрадання магнітних носіїв, документів, отримання необлікованих копій;
32.	включення в програми програмних закладок та вірусів;
33.	збір за допомогою спеціальних технічних засобів електромагнітних випромінювань та паразитних наведень;
34.	використання підслуховуючих пристроїв тощо.

Таблиця 3 Вектор показників оцінювання загроз обчислювальній та оргтехніці, носіям інформації та архівам ($U_{от}$)

№ з/п	Показники оцінювання загроз
1.	несанкціоноване підключення до АІС технічних засобів (в тому числі приватних) (модемів, жорстких магнітних дисків, сканерів та т.ін.);
2.	порушення режимів функціонування АІС;
3.	несанкціоноване копіювання вихідних документів;
4.	можливість включення в програми програмних закладок та вірусів;
5.	збір за допомогою спеціальних технічних засобів електромагнітних випромінювань та паразитних наведень;
6.	використання підслуховуючих пристроїв тощо;
7.	несанкціонований доступ до засобів розмежування доступу;
8.	виведення даних за невірними адресами;
9.	наявність залишкової інформації в запам'ятовуючих пристроях;
10.	порушення роботи АІС у разі одночасного підключення декількох користувачів;
11.	втрата інформації у разі переривання енергоживлення;
12.	відключення систем фіксації відправлених даних;
13.	перебої в роботі антивірусних програм і т. ін.

Таблиця 4 Вектор показників оцінювання загроз зовнішнім каналам інформаційного зв'язку (комунікацій) ($U_{зкз}$)

№ з/п	Показники оцінювання загроз
1.	несанкціонований доступ до баз даних та інформації, що циркулює та обробляється в АІС;
2.	копіювання або руйнування інформації в системі;
3.	зараження інформаційної системи програмними кодами, направленими на завдання шкоди (віруси, "троянські коні" тощо);
4.	дистанційне внесення програмних закладок в програмне забезпечення системи;
5.	хакерські атаки через локальну (корпоративну, Інтернет) мережу;
6.	несанкціоноване підключення до алгоритмів обробки з метою інформаційного впливу на процес обробки інформації.

Таблиця 5 Вектор показників оцінювання загроз внутрішнім каналам зв'язку (комунікацій) ($U_{вкз}$)

№ з/п	Показники оцінювання загроз
1.	несанкціонований доступ до баз даних та інформації, що циркулює та обробляється на різних рівнях АІС;
2.	копіювання, руйнування або знищення інформації в підсистемах;
3.	дистанційне внесення вірусів та інших програмних закладок в програмне забезпечення системи;
4.	хакерські атаки через локальну (корпоративну, Інтернет) мережу;
5.	несанкціоноване підключення до алгоритмів обробки з метою інформаційного впливу на процес обробки інформації.

Таблиця 6 Вектор показників оцінювання загроз приміщенням, офісам ($U_{оф}$)

№ з/п	Показники оцінювання загроз
1.	несанкціоноване ознайомлення з конфіденційною інформацією сторонніми особами;
2.	несанкціоноване копіювання, руйнування або знищення інформації;
3.	застосування пристроїв для дистанційного підслуховування та спостереження.

Таблиця 7 Вектор показників оцінювання загроз системам електроживлення, зв'язку, теле- та радіомовлення ($U_{еж}$)

№ з/п	Показники оцінювання загроз
1.	руйнування баз даних, інформації;
2.	знищення файлів, що розроблялися в момент виключення системи живлення;
3.	руйнування жорстких дисків, системних блоків.

Необхідно відмітити, що вище наведені об'єкти захисту та типові загрози характерні для всіх 3-х рівнів підсистем інформаційної системи ОВС України. Змінюватися будуть скоріше за все масштаби загроз та їх кількість, що буде враховуватися експертами при проведенні конкретного оцінювання.

Природно, що в кожному конкретному випадку базова система показників може доповнюватися або скорочуватися експертами, що залучаються для оцінювання рівня загрози АІС ОВС України.

Враховуючи викладене, у формалізованому виді рівень інтегральної загрози АІС на момент оцінювання t можна оцінити функціоналом

$$U(t) = F\{M_{kp}, V_{skp}, t\}. \quad (1.4)$$

Звісно, що встановити сувору математичну залежність функціоналу (1.4) не представляється можливим, тому доцільно йти шляхом часткових розрахунків U(t) у фіксовані моменти часу t на основі використання технології методу аналізу ієрархій (MAI), а потім по окремим точкам встановити функціональну залежність, яку можна використовувати у подальшому для прогнозування зміни рівня інтегральної загрози з плином часу.

Вибираємо межі існування функціоналу

$$0 \le U(t) \le 1, \quad (1.5)$$

де U(t) = 0 – означає повну відсутність загрози для АІС; U(t) = 1 – означає вивід з ладу АІС (ефективність АІС нейтралізована на 100 %), що не суперечить фізичному змісту введеного функціоналу (1.5) і забезпечує адекватність математичного опису процесу, який вивчається.

Таким чином, процес відстеження рівня інтегральної загрози АІС з боку вибраної моделі порушника, вплив якого характеризується вектором показників U, у формалізованому виді запропоновано описувати функціоналом (1.4), числове значення змін якого знаходиться у межах від нуля до одиниці.

Оскільки рівень інтегральної загрози оцінюється за допомогою вектора обраних показників, то необхідно здійснення постійного моніторингу для добору фактів, що характеризують ці показники. Практика показує, що накопичення інформації по фактам доцільно робити стосовно до обраних об'єктів АІС, а всередині кожного об'єкту "сортування" інформації проводити відносно вибраних показників.

Висновки

Запропонований методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України, яка поєднує принципи територіально-розподіленої та централізованої топології і організована у вигляді трирівневої ієрархічної моделі. Показано, що відновлення ефективності АІС можливо лише за рахунок проведення адекватного рівню інтегральної загрози комплексу заходів безпеки.

Задачу оцінювання рівня інтегральної загрози АІС запропоновано вирішувати за допомогою науково-методичного апарату, який базується на використанні методів дослідження операцій, аналізу ієрархій, векторної алгебри, експертного оцінювання і математичного моделювання.

Для якісного та всебічного оцінювання рівня інтегральної загрози запропоновано вибрати достатньо повну систему вектор-показників прояву загроз об'єктам захисту АІС ОВС України. Така система включає наступні вектори показників оцінювання загроз: 1.) автоматизованим інформаційним системам; 2.) структурним підрозділам, обслуговуючому персоналу і працівникам; 3.) обчислювальній та оргтехніці, носіям інформації та архівам; 4.) зовнішнім каналам інформаційного зв'язку (комунікацій); 5.) внутрішнім каналам зв'язку

(комунікацій); 6.) приміщенням, офісам; 7.) системам електроживлення, зв'язку, теле- та радіомовлення.

Процес відстеження рівня інтегральної загрози АІС з боку вибраної моделі порушника, вплив якого характеризується вектором показників загроз, у формалізованому виді запропоновано описувати функціоналом, а розраховувати шляхом часткових розрахунків рівня інтегральної загрози у фіксовані моменти часу на основі використання технології методу аналізу ієрархій, потім по окремих точках встановлювати функціональну залежність, яку можна використовувати у подальшому для прогнозування зміни рівня інтегральної загрози з плином часу.

Список літератури

1. *Саницький В.А., Карацюба А.М., Святобог В.В. та ін.* Система інформаційного забезпечення ОВС України: Навчально-практичний посібник / За ред. Л.В. Бородича.-К., Редакційно-видавничий відділ МВС України, ТОВ АНТЕКС, 2000.-144 с.: іл., табл.
2. Програма інформатизації органів внутрішніх справ України на 2000-2005 роки // Рішення колегії МВС України від 28 грудня 1999 року № 8км/1.
3. Наказ МВС України від 30 червня 2002 р. № 635 "Про заходи щодо організації проведення науково-дослідних робіт та впровадження їх результатів у практичну діяльність органів внутрішніх справ України".
4. *Пустовит С.Н., Степанов В.Д., Хорошко В.А.* Распределение ресурсов в многорубежной комплексной системе технической защиты информации / Науково-технічний журнал "Захист інформації".-2003. - № 3.- С. 4-10.
5. *Кудінов В.А.* Аналіз проблем створення захисту конфіденційної інформації, що обробляється в системі оперативного інформування МВС України // Защита информации: Сборник научных трудов.-К.: НАУ, 2003.- с.60-67.
6. *Богданович В.Ю.* Воєнна безпека України: методологія дослідження та шляхи забезпечення. Монографія.-К.: ПП "Дельта", 2002.
7. *Саати Т.* Принятие решений: Метод анализа иерархий / Пер. с англ. В.Г. Вогнадзе.-М.: Радио и связь, 1993.
8. *Саати Т., Кернс К.* Аналитическое планирование. Организация систем / Пер. с англ.-М.: Радио и связь, 1991.
9. Термінологічний довідник з питань технічного захисту інформації / За редакцією проф. Хорошка В.О.-К.: Єй-Би-Си, 1999.-206 с.

Надійшла 27.04.2004

УДК 681.3.

Стишенко И.К.

КЛАССИФИКАЦИЯ СПОСОБОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ОПТИЧЕСКОМУ ВОЛОКНУ

Возможность существования побочных оптических излучений с боковой поверхности оптического волокна обусловлена рядом физических, конструктивных и технологических факторов:

- существование вытекающих мод на достаточно протяженном начальном участке волокна, обусловленное физическими процессами распространения оптического излучения в диэлектрическом волноводе при возбуждении его источником излучения с пространственной диаграммой, превышающей апертуру волокна;

- излучение вытекающих и излучательных мод на всем протяжении оптического волокна за счет рэлеевского рассеяния на структурных неоднородностях материала оптического волокна, характерные размеры которых существенно меньше длины волны излучения;