УДК 354.31(477)(004.7+65.012.8)

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

ОЦІНКА ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

У статті наведено оцінку ефективності комплексної системи захисту інформації в інформаційно-телекомунікаційній системі оперативного інформування МВС України з використанням показника надійної її роботи.

***Ключові слова**: оперативна інформація. система оперативного інформування МВС України, комплексна система захисту інформації, інтенсивність атак, бар'єр захисту.*

В статье приведена оценка эффективности комплексной системы защиты информации в информационно-телекоммуникационной системе оперативного информирования МВД Украины с использованием показателя надежной ее работы.

***Ключевые слова**: оперативная информация, система оперативного информирования МВД Украины, комплексная система защиты информации, интенсивность атак, барьер защиты.*

An evaluation of the effectiveness of an integrated system of information security in information and telecommunications system of informing of MIA of Ukraine by using a reliable indicator of its work.

***Keywords**: operational information, system of informing of MIA of Ukraine, an integrated information security system, intensity of the attacks, a barrier of protection.*

Для забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України була створена та ефективно функціонує інформаційно-телекомунікаційна система оперативного інформування (СОІ) МВС України [1]. Вона становить комплекс нормативно-правових, організаційно-кадрових, програмно-апаратних та інших заходів та засобів, за допомогою яких здійснюється цілодобова обробка оперативної інформації про резонансні злочини та інші надзвичайні події, які сталися на території України [2].

Метою функціонування даної інформаційно-телекомунікаційної системи (ІТС) оперативного інформування МВС України є своєчасне, достовірне, повне та якісне інформування керівництва МВС, зацікавлених інстанцій, держави про реальний стан та динаміку оперативної обстановки в цілому в Україні та окремих її регіонах для прийняття важливих управлінських рішень для її покращання, а також постійне стеження за своєчасністю вирішення і розкриттям резонансних злочинів, ліквідації наслідків інших надзвичайних подій.

Враховуючи важливість оперативної інформації, що обробляється в ІТС оперативного інформування МВС України, можна зробити висновок про існування проблеми щодо необхідності її захисту від загроз порушення цілісності, доступності, конфіденційності [3–5]. Для її вирішення запропоновано побудувати комплексну систему захисту інформації (КСЗІ), яка б дозволила запобігти або ускладнити можливість реалізації загроз для інформації, а також знизити потенційні збитки у разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [6–8]. Основним завданням КСЗІ визначено: забезпечити цілісність, доступність та конфіденційність інформації про резонансні злочини та інші надзвичайні події під час її обробки в ІТС оперативного інформування МВС України, відповідний захист ресурсів з обробки інформації, а також спостереження за роботою системи. КСЗІ повинна забезпечити на кожному структурному рівні СОІ МВС України функціонування інформаційних систем класу "2", а функціонування СОІ МВС України в цілому – як інформаційної системи класу "3". Таким чином, КСЗІ в ІТС оперативного інформування МВС України передбачає об'єднання в єдину систему всіх необхідних заходів та засобів захисту від різних загроз безпеці інформації на всіх етапах її життєвого циклу. Безпека інформації забезпечується на технологічних етапах збору, накопичення, оброблення та передачі інформації.

Загальні підходи до оцінювання ефективності КСЗІ в інформаційно-телекомунікаційній системі розглянуто в низці робіт. З'ясовано, що завдання розробника полягає в забезпеченні максимального рівня захищеності інформації в ІТС за мінімальної вартості КСЗІ і максимальної вартості інформації, що захищається. Крім того, система захисту інформації повинна бути адекватною – витрати на безпеку не повинні перевищувати вартості самої інформації і розмірів можливих втрат, які викликані успішною реалізацією загроз.

У роботі [9] наведено аналіз ефективності функціонування КСЗІ в ІТС оперативного інформування МВС України з використанням низки показників, зокрема: результативності, адекватності, доцільності, гнучкості, здійсненності, простоти в адміністративному забезпеченні, ефективності створення, впливу на характеристики СОІ МВС України. З'ясовано, що впровадження КСЗІ дозволяє суттєво підвищити пропускну спроможність та надійність ІТС, оперативну готовність апаратно-технічних засобів та програмного забезпечення до обробки інформації, захищеність інформації, швидкість її обробки в ІТС, якість оперативної інформації, що вводиться до відповідної бази даних.

Проте оцінювання ефективності КСЗІ в ІТС оперативного інформування МВС України з використанням показника надійної роботи КСЗІ дотепер не було проведене. Тому ми спробуємо зробити це в нашій статті.

Під показником надійної роботи КСЗІ розуміють ймовірність надійного перекриття загроз для об'єкта захисту. Таким чином, показник надійної роботи КСЗІ буде визначатись через показники надійної роботи його бар'єрів захисту. Для конкретного бар'єру захисту показник його надійної роботи визначається ймовірністю надійного перекриття загрози: $P_{NB}(t) = K_{OG}(t)\, P_{PAB}(t)$, де $K_{OG}(t)$ – коефіцієнт оперативної готовності бар'єрів КСЗІ; $P_{PAB}(t)$ – ймовірність попадання атаки на бар'єр захисту.

Остання може бути вирахувана за формулою Ерланга:

$$P_{PAB}(t) = \frac{a^n(t)/n!}{\sum_{k=1}^{n} a^k(t)/k!},$$

де $a(t)$ – наведена щільність потоку атак на систему захисту; n – сумарна кількість атак, що впливають на систему захисту; k – умовна кількість шляхів впливу атак на бар'єр.

При цьому $a(t) = \lambda t$, де λ – інтенсивність появи атак за одиницю часу; t – середній час роботи бар'єру.

Вважається, що потік атак на бар'єри КСЗІ є найпростішим засобом, що задовольняє властивостям: 1) стаціонарності (ймовірність атак на ділянку часу залежить від його довжини і не залежить від його розташування на осі часу); 2) ординарності (ймовірність попадання на елементарну ділянку часу двох і більше атак достатньо мала відносно ймовірності попадання однієї атаки); 3) відсутністю наступної дії (для будь-яких ділянок часу, що не перетинаються, атаки на кожну з них не залежать від іншої).

Як видно з рис. 1, збільшення інтенсивності появи атак за одиницю часу призводить до збільшення ймовірності попадання атаки на бар'єр захисту.

Рис. 1. Залежність $P_{PAB}(t)$ при $n = 5$, $k = 1$, $\lambda(1) = 5$, $\lambda(2) = 10$, $\lambda(3) = 25$

На рис. 2 представлено графік для оцінки ефективності комплексної системи захисту інформації, що проектується. При цьому вважається, що КСЗІ складається з трьох механізмів захисту (кожний з яких має у своєму складі по одному організаційному, апаратно-технічному та програмному бар'єру), коефіцієнт живучості дорівнює 1, а допустима інтенсивність відмовлень – 50.

Як видно з графіків цього рисунку, ефективність КСЗІ зберігається максимальною, тобто дорівнює одиниці, при збільшенні інтенсивності атак на КСЗІ до $\lambda = 20$ для часу впливу t до 20. Надалі при збільшенні інтенсивності атак на КСЗІ від 20 до 40 для часу впливу t від 30 до 50 ефективність КСЗІ різко зменшується до нуля. Таким чином, ефективність КСЗІ буде найкращою

для часу впливу t до 20, при якому вона буде надійною при інтенсивності атак на КСЗІ λ до 50.

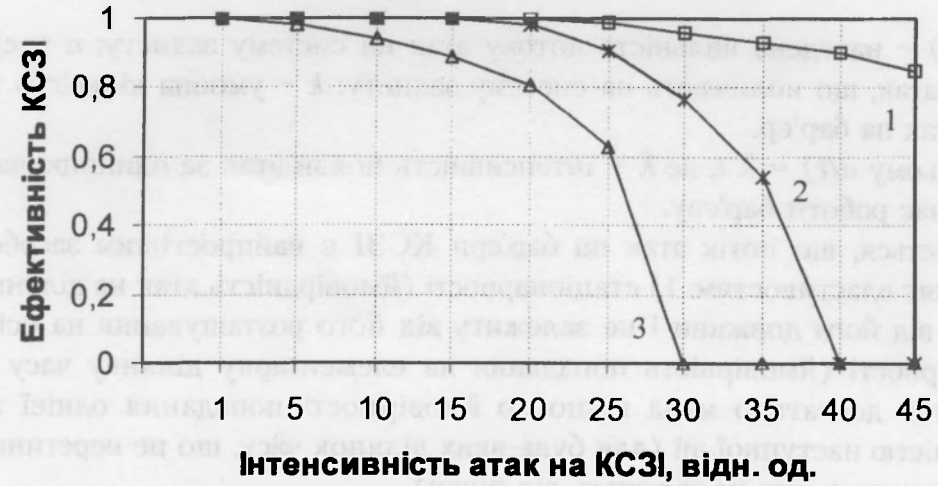

Рис. 2. Залежність $Э(\lambda)$ для КСЗІ при t (1) = 20, t (2) = 30, t (3) = 50

Аналізуючи графіки на рис. 3, можна зробити висновок, що живучість КСЗІ тісно пов'язана з її ефективністю. При цьому зменшення живучості КСЗІ буде приводити також до зменшення її ефективності у такій самій пропорції.

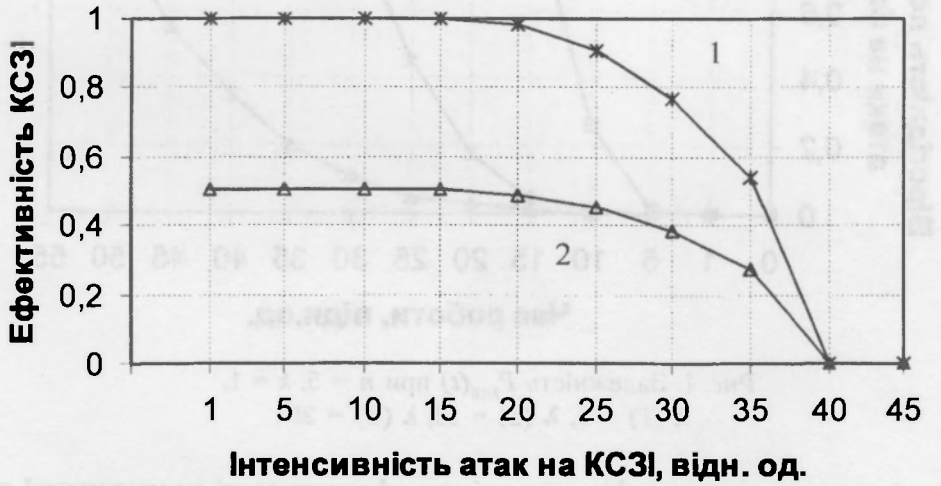

Рис. 3. Залежність $Э(\lambda)$ для КСЗІ при t = 50, коефіцієнт живучості дорівнює 1 (для графіка 1), 0.5 (для графіка 2)

Слід зазначити, що на ефективність роботи КСЗІ основний вплив чинить збільшення програмних і апаратно-технічних бар'єрів у складі її механізмів захисту. А збільшення організаційних бар'єрів не викликає суттєвого збільшення ефективності роботи КСЗІ.

Аналізуючи графіки на рис. 4, можна зробити висновок про те, що ефективність створюваної КСЗІ в ІТС оперативного інформування МВС України порівняно з наявною збільшується на 5–27 %.

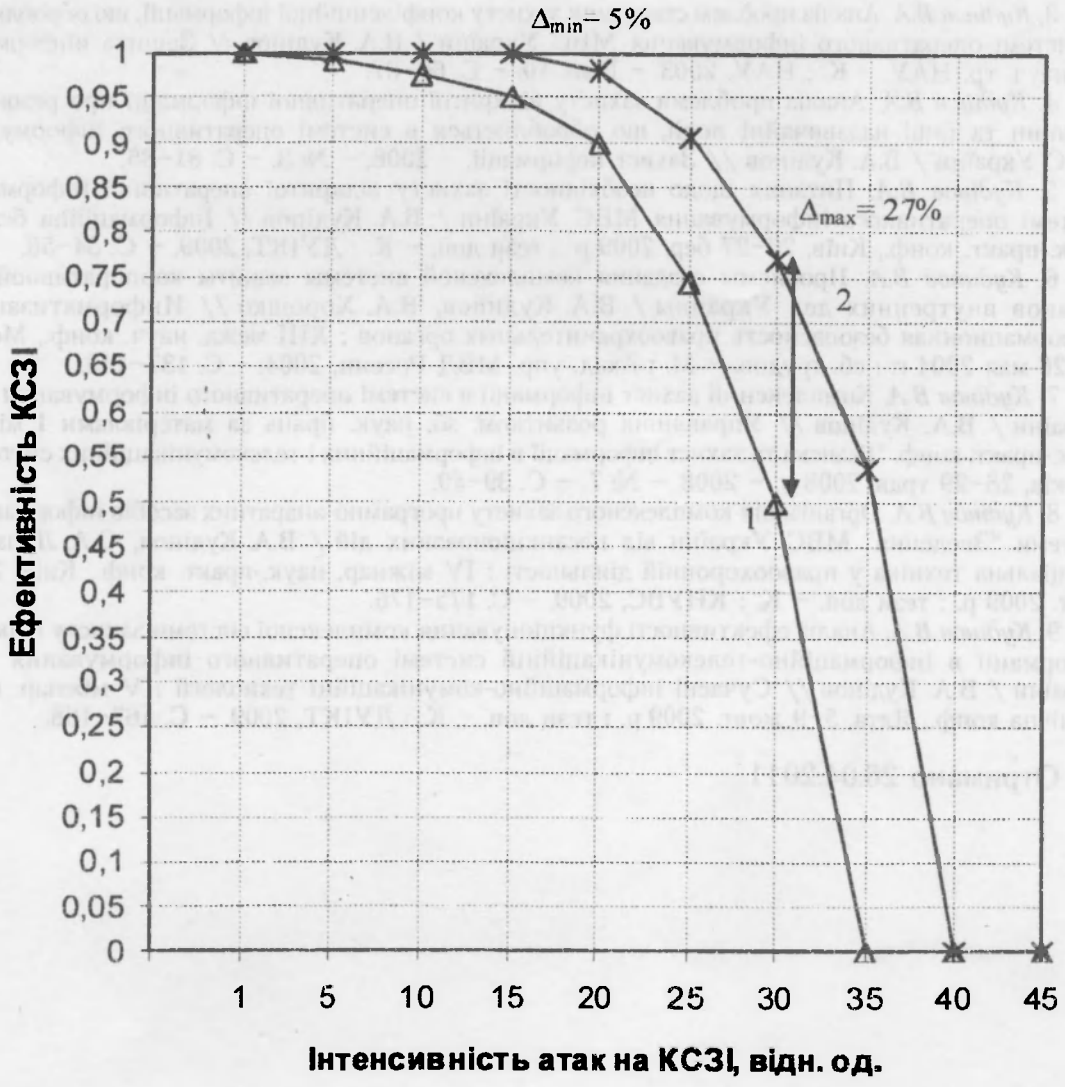

Рис. 4. Залежність $Э(\lambda)$ при t = 30
для КСЗІ наявної (1) та створюваної (2)

Таким чином, створення комплексної системи захисту оперативної інформації про резонансні злочини та інші надзвичайні події в інформаційно-телекомунікаційній системі оперативного інформування МВС України дозволяє забезпечити ефективний захист інформації та ресурсів з її обробки від можливих загроз, тим самим забезпечуючи ефективне інформування керівництва міністерства, зацікавлених інстанцій, держави про резонансні злочини та інші надзвичайні події, що сталися в країні, прискорює розкриття резонансних злочинів "за гарячими слідами" та ліквідацію на-слідків інших надзвичайних подій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України : Наказ МВС України від 4 жовтня 2003 року № 1155.

2. *Кудінов В.А.* Функціонування системи оперативного інформування МВС України / В.А. Кудінов, П.П. Артеменко, О.В. Золотар та ін. ; за ред. В.А. Кудінова // Спеціальна техніка. Загальна частина : посібник. – К. : КНУВС, 2007. – С. 156–172.

3. *Кудінов В.А.* Аналіз проблем створення захисту конфіденційної інформації, що обробляється в системі оперативного інформування МВС України / В.А. Кудінов // Защита информации: сб. науч. тр. НАУ. – К. : НАУ, 2003. – Вып. 10. – С. 60–67.

4. *Кудінов В.А.* Аналіз проблеми захисту відкритої оперативної інформації про резонансні злочини та інші надзвичайні події, що обробляється в системі оперативного інформування МВС України / В.А. Кудінов // Захист інформації. – 2008. – № 3. – С. 81–85.

5. *Кудінов В.А.* Питання щодо необхідності захисту відкритої оперативної інформації в системі оперативного інформування МВС України / В.А. Кудінов // Інформаційна безпека: наук.-практ. конф., Київ, 26–27 бер. 2009 р. : тези дон. – К. : ДУІКТ, 2009. – С. 54–56.

6. *Кудинов В.А.* Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины / В.А. Кудинов, В.А. Хорошко // Информатизация и информационная безопасность правоохранительных органов : XIII межд. науч. конф., Москва, 25–26 мая 2004 г. : сб. трудов. – М. : Акад. упр. МВД России, 2004. – С. 137–140.

7. *Кудінов В.А.* Комплексний захист інформації в системі оперативного інформування МВС України / В.А. Кудінов // Управління розвитком: зб. наук. праць за матеріалами І міжнар. наук.-практ. конф. "Безпека та захист інформації в інформаційних і телекомунікаційних системах", Харків, 28–29 трав. 2008 р. – 2008. – № 7. – С. 39–40.

8. *Кудінов В.А.* Організація комплексного захисту програмно-апаратних засобів інформаційної системи "Зведення" МВС України від несанкціонованих дій / В.А. Кудінов, О.А. Лунало // Спеціальна техніка у правоохоронній діяльності : IV міжнар. наук.-практ. конф., Київ, 26–27 лист. 2009 р. : тези доп. – К. : КНУВС, 2009. – С. 175–176.

9. *Кудінов В.А.* Аналіз ефективності функціонування комплексної системи захисту відкритої інформації в інформаційно-телекомунікаційній системі оперативного інформування МВС України / В.А. Кудінов // Сучасні інформаційно-комунікаційні технології : V міжнар. наук.-технічна конф., Ялта, 5–9 жовт. 2009 р. : тези дон. – К. : ДУІКТ, 2009. – С. 167–168.

Отримано 26.04.2011