УДК 354.31(477)(004.7+65.012.8)

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

МЕТОДИКА ЕКСПЕРТНОЇ ОЦІНКИ РІВНІВ ЗАХИЩЕНОСТІ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

У статті наведена методика експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України на підставі експертної оцінки ймовірності подолання засобів та заходів захисту оперативної інформації та ресурсів з її обробки.

***Ключові слова**: оперативна інформація, система оперативного інформування МВС України, комплексна система захисту інформації, об'єкти захисту, ймовірність події.*

В статье приведена методика экспертной оценки уровней защищенности интегрированной информационной системы оперативного информирования МВД Украины на основании экспертной оценки вероятности преодоления средств и мероприятий защиты оперативной информации и ресурсов по ее обработке.

***Ключевые слова**: оперативная информация, система оперативного информирования МВД Украины, комплексная система защиты информации, объекты защиты, вероятность события.*

The technique of an expert assessment of the levels of security of the integrated information system of the operative informing of the Ministry of Internal Affairs of Ukraine is given on the basis of an expert assessment of the probability of overcoming of means and actions of the protection of operational information and resources on its processing.

***Keywords**: operational information, system of operative informing of the Ministry of Internal Affairs of Ukraine, complex system of protection of information, objects of protection, probability of an event.*

Для забезпечення оперативного інформування в органах і підрозділах внутрішніх справ (далі – ОВС) України була створена та ефективно функціонує інтегрована інформаційна система оперативного інформування (далі – СОІ) МВС України [1–4]. Це єдина система збирання, опрацювання та подання до Міністерства внутрішніх справ України, головних управлінь (управлінь) МВС України в областях, містах та на транспорті, Головного управління внутрішніх військ МВС України оперативної інформації про кримінальні правопорушення, інші правопорушення, надзвичайні ситуації та інші події (далі – кримінальні правопорушення та інші надзвичайні події), а також стеження за встановленням і затриманням осіб, які вчинили кримінальні правопорушення, та реагуванням на інші надзвичайні події [1]. Вона становить єдиний інформаційно-аналітичний комплекс нормативно-правових, організаційно-кадрових, програмно-технічних,

інформаційно-телекомунікаційних та інших заходів і засобів, що здійснює цілодобову обробку оперативної інформації про кримінальні правопорушення та інші надзвичайні події, які сталися на території України [3; 4]. Ця система функціонує в корпоративній мережі ОВС України, а завдання щодо забезпечення її функціонування покладені на чергові частини.

Метою СОІ МВС України є своєчасне, достовірне, повне та якісне інформування керівництва Міністерства внутрішніх справ України, інших зацікавлених міністерств та державних органів про реальний стан й динаміку оперативної обстановки в цілому в Україні та окремих її регіонах для прийняття впливових управлінських рішень на її покращання, а також постійне стеження за розслідуванням кримінальних правопорушень і реагуванням на інші надзвичайні події [1–4].

Враховуючи важливість оперативної інформації та ресурсів з її обробки, необхідно забезпечити їх належний захист [5]. Вирішенню зазначеної проблеми присвячена низка наукових робіт.

Так, зокрема, в роботах [6–10] серед основних напрямів розвитку СОІ МВС України запропоновано розробити та впровадити відповідні комплексні заходи та засоби захисту оперативної інформації, тобто створити комплексну систему захисту інформації (далі – КСЗІ). Аналізу та оцінці ефективності функціонування КСЗІ в СОІ МВС України присвячені роботи [11; 12]. Питанням аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі присвячена стаття [13]. Загальна математична модель об'єктів захисту СОІ МВС України розглянута в роботі [14]. Стаття [15] присвячена проблемі створення комплексної системи захисту корпоративної мережі ОВС України. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України, а також аналіз множини векторів-показників прояву погроз об'єктам захисту цієї інформаційної системи наведений у статті [16]. Питанням оцінки коефіцієнта оперативної готовності програмно-апаратних засобів захищеної СОІ МВС України щодо обробки інформації присвячена робота [17]. У зв'язку з набуттям 20 листопада 2012 року чинності новим КПК України [18], збір, накопичення та обробка оперативної інформації про кримінальні правопорушення та інші надзвичайні події здійснюється з використанням можливостей Інтегрованої інформаційно-пошукової системи (далі – ІІПС) ОВС України [19]. Тому в статті [20] було розглянуто напрями подальшого розвитку методології оцінки рівнів захищеності СОІ МВС України. Оцінка коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла ІІПС ОВС України з обробки оперативної інформації СОІ МВС України наведена у статті [21].

Таким чином, створення та використання методики експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України, якій присвячена ця стаття, буде слугувати для подальшого удосконалення КСЗІ зазначеної системи.

Побудова КСЗІ в СОІ МВС України повинна дозволити запобігти або ускладнити можливість реалізації загроз порушення цілісності, доступності та конфіденційності оперативної інформації, а також належного функціонування ресурсів з її обробки, знизити потенційні збитки в разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [7; 8; 10–12; 15]. Враховуючи трьохрівневу ієрархічну модель організації функціонування ІІПС ОВС України, 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" [20]. Тобто побудова КСЗІ в СОІ МВС України передбачає об'єднання в єдину систему всіх необхідних заходів та засобів захисту від різних загроз безпеці оперативної інформації на всіх етапах її життєвого циклу [9; 10; 22].

Розглянемо методику експертної оцінки рівнів захищеності об'єктів захисту СОІ МВС України.

По-перше, необхідно виділити найбільш вірогідні об'єкти обробки оперативної інформації в СОІ МВС України з порушенням її цілісності, доступності та конфіденційності. Перелік таких об'єктів захисту наведений у роботах [14; 16].

По-друге, необхідно розглянути модель ймовірного порушника безпеки для вибраних об'єктів захисту, яка оцінює не тільки самого порушника, але також визначає загрози цим об'єктам. У роботі [13] наведена загальна модель імовірного порушника безпеки та як базові моделі захисту інформації розглянуто найпростіші моделі пасивного й активного каналів витоку інформації, моделі ненавмисного і навмисного несанкціонованого доступу.

По-третє, необхідно виділити всі наявні засоби та заходи захисту для вибраних об'єктів захисту. У роботах [8; 10; 12] запропоновано комплекс основних заходів захисту апаратно-технічних засобів та програмного забезпечення з обробки оперативної інформації.

По-четверте, необхідно здійснити на основі досвіду фахівців із захисту інформації експертну оцінку ймовірності подолання наявних засобів та заходів захисту (далі – події) $P_{под}$ для вибраних об'єктів захисту, значення якої визначається в межах від 0 до 1. З метою створення єдиного підходу до оцінки $P_{под}$ пропонується ввести таку шкалу її значень:

1) $P_{под} = 0$, якщо подія неможлива;
2) $P_{под} = 0{,}2$, якщо низька ймовірність події;
3) $P_{под} = 0{,}5$, якщо ймовірності появи події та її відсутності однакові;
4) $P_{под} = 0{,}8$, якщо висока ймовірність події;
5) $P_{под} = 1$, якщо подія відбудеться обов'язково.

Необхідно зазначити таке: а) якщо для об'єкта захисту існує низка шляхів подолання наявних засобів та заходів захисту з різними значеннями $P_{под}$, то в підсумковій експертній оцінці необхідно брати її найбільше значення; б) якщо для об'єкта захисту є низка засобів та заходів захисту від конкретного впливу порушника безпеки з різними значеннями $P_{под}$, то в підсумковій експертній оцінці необхідно брати її найменше значення.

Таким чином, використання цієї методики дозволяє отримати цифрові дані щодо рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України.

Наведена методика експертної оцінки рівнів захищеності інтегрованої інформаційної системи оперативного інформування МВС України (на підставі експертної оцінки ймовірності подолання засобів та заходів захисту оперативної інформації та ресурсів з її обробки) дозволяє провести для цієї системи всебічний аналіз комплексної системи захисту інформації та виявити в ній слабкі ланки, які потребують подальшого удосконалення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про організацію реагування на повідомлення про кримінальні правопорушення, інші правопорушення, надзвичайні ситуації та інші події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України : Наказ МВС України від 22 жовтня 2012 року № 940.

2. Про затвердження Інструкції про порядок ведення єдиного обліку в органах і підрозділах внутрішніх справ України заяв і повідомлень про вчинені кримінальні правопорушення та інші події та положень про комісії : Наказ МВС України від 19 листопада 2012 року № 1050.

3. *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. : Київський нац. ун-т внутр. справ, 2007. – С. 156–172.

4. *Кудінов В.А.* Становлення, сучасний стан і перспективи розвитку автоматизованої системи оперативного інформування МВС України про резонансні злочини та інші надзвичайні події / В.А. Кудінов // Бюлетень з обміну досвідом роботи МВС України. – 2012. – № 190. – С. 9–27.

5. Про затвердження Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ України : Наказ МВС України від 14 травня 2012 року № 423.

6. *Кудінов В.А.* Проблеми застосування інформаційних технологій в інтегрованій інформаційній системі оперативного інформування МВС України / В.А. Кудінов // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами : матеріали наук.-практ. конференції, Львів, 14 груд. 2011 р. – Львів : Львівський держ. ун-т внутр. справ, 2011. – С. 64–68.

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. Лупало // Спеціальна техніка у правоохоронній діяльності : IV міжнар. наук.-практ. конф., Київ, 26-27 лист. 2009 р. : тези доп. – К. : Київський нац. ун-т внутр. справ, 2009. – С. 175–176.

9. *Кудінов В.А.* Аналіз загальних особливостей функціонування основних об'єктів інформаційної безпеки інтегрованих інформаційних систем органів внутрішніх справ України / В.А. Кудінов // Сучасна спеціальна техніка. – 2012. – № 1. – С. 91–96.

10. *Кудінов В.А.* Організація комплексу заходів захисту апаратно-технічних засобів та програмного забезпечення системи оперативного інформування МВС України / В.А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 4. – С. 54–59.

11. *Кудінов В.А.* Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України / В.А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 1. – С. 91–96.

12. *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 доп. – К. : ДУІКТ, 2009. – С. 167–168.

13. *Кудінов В.А.* Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 1. – С. 26–35.

14. *Кудінов В.А.* Загальна математична модель об'єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України / В.А. Кудінов // Сучасний захист інформації. – 2011. – № 1. – С. 21–25.

15. *Кудинов В.А.* Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины / В.А. Кудинов, В.А. Хорошко // Тр. XIII Межд. научной конф. "Информатизация и информационная безопасность правоохранительных органов", 25–26 мая 2004 г. – М. : Академия управления МВД России, 2001. – С. 137–140.

16. *Кудінов В.А.* Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 4. – С. 11–18.

17. *Кудінов В.А.* Оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної автоматизованої системи оперативного інформування МВС України щодо своєчасної та якісної обробки відкритої інформації / В.А. Кудінов, В.О. Хорошко // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. – 2009. – № 6, Ч. 1. – С. 82–85.

18. Кримінальний процесуальний кодекс України (із змінами, внесеними згідно із Законами 2013-2014 років) : Закон України від 13.04.2012 № 4651-VI // Відомості Верховної Ради України (ВВР). – 2013. – № 9–10, № 11–12, № 13 – Ст. 88.

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

20. *Кудінов В.А.* Напрями подальшого розвитку методології оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України у зв'язку з набуттям чинності нового КПК України / В.А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 1. – С. 126–130.

21. *Кудінов В.А.* Оцінка коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України з обробки інформації / В.А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 2. – С. 58–63.

22. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

Отримано 01.08.2014