УДК 354.31(477)(004.7+65.012.8)

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

НАПРЯМИ ПОДАЛЬШОГО РОЗВИТКУ МЕТОДОЛОГІЇ ОЦІНКИ РІВНІВ ЗАХИЩЕНОСТІ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ У ЗВ'ЯЗКУ З НАБУТТЯМ ЧИННОСТІ НОВОГО КПК УКРАЇНИ

У статті наведено аналіз сучасного стану методології оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України.

Ключові слова: *методологія, обробка оперативної інформації, Інтегрована інформаційно-пошукова система ОВС України, корпоративна мережа.*

В статье приведен анализ нынешнего состояния методологии оценки уровней безопасности интегрированной информационно-телекоммуникационной системы оперативного информирования МВД Украины.

Ключевые слова: *методология, обработка оперативной информации, Интегрированная информационно-поисковая система ОВД Украины, корпоративная сеть.*

The paper is an analysis of the current state of methodology for assessing the safety levels of integrated information technology system of informing the Ministry of Interior affairs of Ukraine.

Keywords: *methodology, data processing operations, the Integrated Information Retrieval System the internal affairs of Ukraine, the corporate network.*

Відповідно до п. 1.1 Інструкції про оперативне інформування в органах і підрозділах внутрішніх справ (далі – ОВС), внутрішніх військах та навчальних закладах МВС України, затвердженої наказом МВС України від 22 жовтня 2012 року № 940 [1], під оперативним інформуванням розуміють єдину систему збирання, опрацювання та подання до МВС України, головних управлінь, управлінь МВС України в Автономній Республіці Крим, областях, містах Києві та Севастополі, 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.

Для забезпечення оперативного інформування в ОВС України була створена інтегрована інформаційно-телекомунікаційна система оперативного інформування (далі – СОІ) МВС України. Вона представляє собою 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 [1–4].

Метою функціонування СОІ МВС України є своєчасне, достовірне, повне та якісне інформування керівництва МВС України, інших зацікавлених міністерств та державних органів про реальний стан й динаміку оперативної обстановки у 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 [1–5].

Ця система функціонує у корпоративній мережі ОВС України, а завдання щодо забезпечення її функціонування покладені на чергові частини. Тому вирішення проблеми забезпечення захисту оперативної інформації та ресурсів з її обробки в СОІ МВС України безпосередньо пов'язано з вирішенням зазначеної проблеми в корпоративній мережі та програмно-технічному комплексі чергових частин ОВС України, що знайшло відображення у низці наукових робіт.

Так, зокрема, в роботах [6–8] 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). У статті [9] розглядається питання аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі. Загальна математична модель об'єктів захисту СОІ МВС України розглянута у статті [10]. У роботі [11] висвітлено проблеми 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 [12]. У роботі [13] здійснена оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної СОІ МВС України щодо обробки інформації. Аналізу та оцінці ефективності КСЗІ в СОІ МВС України присвячені роботи [14, 15].

Таким чином, на сьогодні розроблено методологію оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України. Але з набуттям чинності нового Кримінального процесуального кодексу (далі – КПК) України [16] відбулись зміни у відомчій нормативно-правовій базі МВС України та заплановані зміни у програмно-технічному забезпеченні функціонування СОІ МВС України [1, 5]. Тому визначення напрямів подальшого розвитку методології оцінки рівнів захищеності зазначеної системи є актуальною проблемою, вирішенню якої присвячена ця стаття.

Наслідком важливості оперативної інформації, що обробляється в інтегрованій інформаційно-телекомунікаційній системі оперативного інформування МВС України [17], є необхідність вирішення проблем щодо її захисту від загроз порушення цілісності, доступності та конфіденційності, а також захисту ресурсів з її обробки [18–20]. Для вирішення зазначених проблем запропоновано побудувати КСЗІ, яка б дозволила запобігти або ускладнити можливість реалізації загроз для оперативної інформації, а також знизити потенційні збитки у разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [7, 8, 11, 14, 15]. Тобто створення КСЗІ в СОІ МВС України дозволить забезпечити якісне та своєчасне інформування керівництва МВС України, інших зацікавлених міністерств та державних органів про реальний стан і динаміку оперативної обстановки у цілому в Україні та

окремих її регіонах для прийняття впливових управлінських рішень на її покращання, а також безперебійне постійне стеження за розслідуванням кримінальних правопорушень і реагуванням на інші надзвичайні події.

Відповідно до наказу МВС України від 19 листопада 2012 року № 1050 у чергових частинах ОВС України планується ввести єдиний облік заяв і повідомлень про вчинені кримінальні правопорушення та інші події в електронному вигляді з 1 липня 2013 року [5] (існують також реальні пропозиції фахівців, які враховують складнощі створення зазначеної системи та її високу вартість, щодо зміни контрольного терміну на 1 липня 2014 року). Для цього Департаменту інформаційно-аналітичного забезпечення МВС України [21] наказано розробити порядок застосування в електронному вигляді єдиного обліку заяв і повідомлень про вчинені кримінальні правопорушення та інші події з дотриманням положень, визначених Інструкцією про єдиний облік злочинів. Зазначений облік впроваджується на базі Інтегрованої інформаційно-пошукової системи ОВС України [22, 23], яка побудована за трирівневою ієрархічною моделлю, що відповідає організаційній побудові МВС України. На кожному рівні зазначеної системи на відповідних серверах будуть формуватися інформаційні масиви єдиного обліку заяв і повідомлень про вчинені кримінальні правопорушення та інші події. При цьому безпека оперативної інформації повинна забезпечуватися на всіх технологічних етапах збору, накопичення, оброблення та передачі інформації. Необхідно також відмітити, що в Інтегрованій інформаційно-пошуковій системі ОВС України для користувачів установлюються чотири рівні доступу до інформаційних ресурсів системи та один рівень для внесення інформації до відповідних баз даних системи [22, 23], а база даних "Єдиний облік" створюється з урахуванням структур баз даних "Факт" [24] та "Єдиний реєстр досудових розслідувань" [25], вимог нового КПК України [16, 26].

Таким чином, 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". Тобто КСЗІ в СОІ 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 [27].

Висновок. Напрями подальшого розвитку методології оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України у зв'язку з набуттям чинності нового КПК України безпосередньо пов'язані з тим, що збір, накопичення та оброблення оперативної інформації про кримінальні правопорушення та інші надзвичайні події планується здійснювати в Інтегрованій інформаційно-пошуковій системі ОВС України, яка побудована за трирівневою ієрархічною моделлю та функціонує в корпоративній мережі ОВС України.

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 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 04 жовтня 2003 року № 1155.

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: посіб. – 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 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.

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

10. *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.

11. *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.

12. *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.

13. *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.

14. *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.

15. *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.

16. Кримінальний процесуальний кодекс : Закон України від 13 квітня 2012 року № 4651-VI / Відомості Верховної Ради України (ВВР). – 2013. – № 9–10, № 11–12, № 13. – Ст. 88.

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

18. *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. : Нац. авиац. ун-т, 2003. – Вып. 10 – С. 60–67.

19. *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.

20. *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 доп. – К. : ДУІКТ, 2009. – С. 54–56.

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

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

23. Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Наказ МВС України від 10 березня 2010 року № 75 (втратив чинність відповідно до наказу МВС України від 20 квітня 2011 року № 152).

24. Про впровадження в дослідну експлуатацію бази даних "Факт" Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Розпорядження МВС України від 10 грудня 2010 року № 1140.

25. Про Єдиний реєстр досудових розслідувань : Наказ Генеральної прокуратури України від 17 серпня 2012 року № 69.

26. *Кудінов В.А.* Проект структури бази даних Єдиного електронного реєстру звернень громадян та юридичних осіб до міліції / В.А. Кудінов // Спеціальна техніка у правоохоронній діяльності : V міжнар. наук.-практ. конф., Київ, 25 лист. 2011 р. : тези доп. – К. : Нац. акад. внутр. справ, 2012. – С. 15–18.

27. 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 15.04.2013