УДК 354.31(477)(004.7+65.012.8)

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

ОРГАНІЗАЦІЯ КОМПЛЕКСУ ЗАХОДІВ ЗАХИСТУ АПАРАТНО-ТЕХНІЧНИХ ЗАСОБІВ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

Запропоновано комплекс основних заходів захисту апаратно-технічних засобів та програмного забезпечення з обробки оперативної інформації про резонансні злочини та інші надзвичайні події в системі оперативного інформування МВС України.

***Ключові слова**: комплексна система захисту інформації, оперативна інформація, апаратно-технічні засоби, програмне забезпечення, система оперативного інформування МВС України.*

В статье предложен комплекс основных мероприятий защиты аппаратно-технических средств и программного обеспечения по обработке оперативной информации о резонансных преступлениях и других чрезвычайных событиях в системе оперативного информирования МВД Украины.

***Ключевые слова**: комплексная система защиты информации, аппаратно-технические средства, программное обеспечение, система оперативного информирования МВД Украины.*

The complex of the main measures on the protection of device techniques and software for the processing of operational information on resonant crimes and other extraordinary events in the Ministry of Internal Affairs of Ukraine is offered.

***Keywords**: complex system of information protection, device techniques, software, system of operative informing of the Ministry of Internal Affairs of Ukraine.*

Серед основних напрямів державної інформаційної політики в Україні, відповідно до Закону України "Про інформацію" в редакції від 9 травня 2011 року, є створення інформаційних систем (ІС) 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 України.

В органах і підрозділах внутрішніх справ (ОВС) України на сьогодні функціонують різноманітні інформаційні та інформаційно-телекомунікаційні системи (ІТС) оперативно-розшукового та інформаційно-довідкового призначення. Значна їх частина працює вже понад 20 років і за цей час в них неодноразово відбувалися зміни інформаційних процесів у зв'язку з використанням новітніх засобів оргтехніки й інформаційних технологій. При цьому важливою проблемою, яка потребує постійного та належного вирішення, є здійснення комплексу заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), щодо забезпечення збереження заданих

властивостей інформації під час її обробки в зазначених системах та захисту відповідних ресурсів із її обробки.

Порушена проблема стосується не тільки МВС України. В органах державної влади налічується майже 40 інформаційних ресурсів баз даних, які становлять найбільший інтерес для правоохоронних органів. Покращання стану функціонування інформаційних систем в умовах використання новітніх інформаційно-комунікаційних технологій в суспільстві та органах державної влади вимагають різноманітні нормативно-правові акти, зокрема: закони України "Про захист інформації в інформаційно-телекомунікаційних системах" від 1 січня 2006 року, "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" від 9 січня 2007 року, Укази Президента України "Про Стратегію національної безпеки України" від 12 лютого 2007 року № 105, "Про Доктрину інформаційної безпеки України" від 8 липня 2009 року № 514, постанови Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29 березня 2006 року № 373, "Про затвердження Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю" від 8 квітня 2009 року № 321.

У якості об'єкта дослідження обрано ІТС оперативного інформування МВС України про резонансні злочини та інші надзвичайні події, що сталися на території України. Ця система функціонує в чергових частинах ОВС України. Її вибір пояснюється відсутністю результатів досліджень для неї із зазначеної проблеми, а також важливістю її функціонування для суспільства та держави. Метою функціонування інформаційно-телекомунікаційної системи оперативного інформування МВС України є своєчасне, достовірне, повне та якісне інформування керівництва Міністерства внутрішніх справ України, зацікавлених інстанцій, держави про реальний стан й динаміку оперативної обстановки в цілому в Україні та окремих її регіонах для прийняття впливових управлінських рішень задля її покращання, а також постійне стеження за своєчасністю вирішення і розкриттям резонансних злочинів, ліквідації наслідків інших надзвичайних подій [1]. Зазначена система становить комплекс нормативно-правових, організаційно-кадрових, програмно-апаратних та інших заходів та засобів, що здійснює цілодобову обробку оперативної інформації про резонансні злочини та інші надзвичайні події, які сталися на території України [2].

Питанням захисту оперативної інформації, що обробляється в ІТС оперативного інформування МВС України, присвячені роботи [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 в разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [6–8]. Основним завданням КСЗІ визначено: забезпечити цілісність, доступність та конфіденційність оперативної інформації про резонансні злочини та інші надзвичайні події під час її обробки в ІТС оперативного інформування МВС України, а також відповідний захист ресурсів із обробки інформації. Оцінка та аналіз ефективності КСЗІ в ІТС оперативного інформування МВС України наведено в роботах [8, 9].

Таким чином, на сьогодні залишається досі невирішеною проблема організації комплексу заходів захисту ресурсів (апаратно-технічних засобів та програмного

забезпечення) з обробки інформації ІТС оперативного інформування МВС України, що обумовлює актуальність теми дослідження.

Ефективне функціонування ІТС оперативного інформування МВС України безпосередньо визначається ефективним функціонуванням ІС "Зведення" МВС України [10, 11]. Тому важливим і актуальним завданням для ОВС України є вирішення проблеми організації належних заходів захисту її апаратно-технічних засобів та програмного забезпечення (далі – об'єктів захисту) з обробки оперативної інформації. При цьому вважається, що в ІС використовуються апаратно-технічні засоби та програмне забезпечення з високою оперативною готовністю до обробки оперативної інформації [12].

Слід відзначити, що зазначена проблема для інформаційної системи потребує комплексного розв'язання, тобто необхідно розробити низку належних базових заходів захисту вказаних об'єктів захисту та використовувати їх у комплексі. Наведений далі перелік базових заходів не є вичерпним, він може доповнюватися й удосконалюватися.

Обмеження доступу сторонніх осіб до вказаних об'єктів захисту через побудову низки зон захисту, у яких функціонують відповідні засоби охорони. В загальному випадку виділяють шість послідовних зон захисту об'єктів захисту інформаційної системи [12]. Дана ситуація характерна для ІС "Зведення" МВС України. Якщо розглядати функціонування даної системи в чергових частинах обласного та територіального рівня ОВС України, то для них в схемі захисту можуть бути відсутні дві зони, а саме: периметр території та територія.

Слід враховувати також те, що приміщення чергових частин належать до режимних, а тому заходи обмеження доступу до них осіб вживаються обов'язково, а самі приміщення цілодобово перебувають під охороною [13]. В них використовуються різні методи автентифікації (символьні та графічні паролі, біометричні системи, смарт-карти тощо). Для випадку, що розглядається, достовірність виявлення порушника в контрольованій зоні, яка охоплює всі зони охорони, буде дорівнювати $\sum P = 1$ ($i = \overline{1,6}$), тобто порушник обов'язково буде виявлений.

Створення резерву аналогічних апаратно-технічних засобів, що функціонують, та підтримка їх у належному стані передбачає наявність додаткових працездатних апаратно-технічних засобів, які можна було б використовувати для заміни засобів, які вийшли з ладу.

Слід відзначити, що в черговій частині МВС України одночасно може працювати з ІС "Зведення" вся чергова зміна у кількості 4 працівників, тобто їх автоматизовані робочі місця (АРМ), підключені до цієї системи. Крім того, є ще 3 додаткових АРМ, які дозволяють також працювати із системою. На них, за необхідністю, працюють працівники Оперативного управління Головного штабу МВС України. Таким чином, вихід із ладу будь-якої абонентської станції не є критичним для обробки оперативної інформації про резонансні злочини та інші надзвичайні події в ІС "Зведення" МВС України. Існує також резерв інших апаратно-технічних засобів, зокрема принтерів, ксероксів, модемів, клавіатур, що іноді буває дуже корисним під час можливої їх збійної роботи в нічний час або святковий день.

Для нормального функціонування ІС у чергових частинах ОВС України та забезпечення цілісності їх баз даних необхідно забезпечити чергові частини комп'ютерами у кількості не менше двох із повним комплектом периферійних пристроїв та відповідним сучасним програмним забезпеченням.

Створення архівних копій програмного забезпечення та постійне їх оновлення дозволяє у випадку знищення або пошкодження без зайвих проблем своєчасно відновити його. Особливо це важливо, коли програмне забезпечення удосконалюється й відбуваються окремі зміни у ньому. У черговій частині МВС України існують всі версії програмного забезпечення ІС "Зведення" з 2000 року й дотепер.

Створення архівних копій баз даних оперативної інформації та періодичне їх оновлення є найбільш важливим та актуальним завданням працівників чергової частини, оскільки знищення або пошкодження інформаційних баз даних унеможливить виконання ними своїх функціональних обов'язків у повному обсязі.

У черговій частині МВС України налагоджено таку процедуру створен-ня копій баз даних поточного року: 1) файл-сервер баз даних містить також другий, дзеркальний до основного, "вінчестер", на який автоматично системою записується копія поточної бази даних, з якою відбувається робота користувача; 2) щоранку виготовляється копія поточної бази даних ІС "Зведення" в поточну базу даних ІС "Пошук" (дані інформаційні системи ідентичні; створення двох однакових ІС дозволяє розмежувати операції введення та пошуку оперативної інформації, а також є певним заходом безпеки бази даних); 3) на "вінчестер" кожної з чотирьох абонентських станцій чергової частини МВС України почергово (по днях) робиться копія поточної бази даних ІС "Зведення", тобто кожна або-нентська станція оновлює копію поточної бази даних один раз на чотири дні; 4) періодично (1 раз на тиждень або місяць) створюється копія бази даних на компакт-диск або флеш-карту відповідальним за це працівником чергової частини.

Здійснення цих заходів дозволяє працівникам чергової частини МВС України упевнитися у збереженні поточної бази даних оперативної інформації щодо резонансних злочинів та інших надзвичайних подій, що сталися в країні. Зазначимо, що інструкцією користувача автоматизованої системи в Міністерстві економіки та з питань європейської інтеграції України [14] також передбачено зберігання копій електронних документів великого обсягу, іншої трудомісткої і цінної інформації на змінних носіях інформації або на файловому сервері АС класу "3".

Створення спеціальної системи захисту окремого програмного забезпечення передбачає наявність додаткового програмного забезпечення, яке здійснює захист основного. Наприклад, використання програм, які дозволяють: 1) шифрувати інформацію в зображенні та звуці, за допомогою архіваторів, паролів документів; 2) захистити інформацію вінчестера від несанкціонованого отримання шляхом її знищення під час форматування накопичувача при спробі вилучити його, при викраденні комп'ютера, при проникненні людини в зону обслуговування комп'ютера, при натисканні визначеної кнопки тощо; 3) захистити інформацію дискети, вінчестера; 4) шифрувати логічний диск.

Існує також можливість реалізації механізму фізичної безпеки комп'ютерної системи (КС) з використанням апаратного компонента системи захисту і плати, яка встановлюється у вільний слот комп'ютера, що захищається. У цьому випадку порушнику для того, щоб видалити (модифікувати) програмний компонент, що реалізує всі механізми розмежувальної політики доступу користувачів до ресурсів, які захищаються, необхідно попередньо видалити з КС цю плату.

Здійснення спеціальних заходів захисту апаратно-технічних засобів від підмін, порушення цілісності тощо. У роботах [15, 16] наведений метод радіоізотопного маркування матеріальних носіїв інформації КС від підмін, порушення цілісності

тощо для забезпечення їх фізичної безпеки, а також запропонований метод захисту від несанкціонованого розкриття апаратури, у тому числі, корпусу комп'ютера, що захищається.

Використання ліцензійного антивірусного програмного забезпечення з його періодичним оновленням дозволяє захистити від спотворювання чи знищення даних та програм, внесення порушень в нормальний режим роботи комп'ютерів, програм, мережі, пристроїв. У черговій частині МВС України використовується різноманітне сучасне антивірусне програмне забезпечення, що відповідає вимогам роботи [14]. Слід зазначити, що одночасне використання різних антивірусних програм може призводити до їх некоректної роботи. Користувачу ІС слід обережно використовувати виконавчі файли, які надійшли електронною поштою, якщо отримання таких файлів не було передбачено.

Закріплення відповідальної особи за належне функціонування об'єктів захисту дозволить налагодити систематичне проведення запланованих належних заходів захисту та своєчасно вносити до них відповідні корективи. У черговій частині МВС України в 90-х роках була передбачена в її штатному розкладі посада старшого інженера-програміста. На сьогодні вона відсутня, і обов'язки інженера-програміста покладено на працівника Головного управління інформаційного забезпечення при Головному штабі МВС України, який супроводжує функціонування ІС "Зведення". Допомогу йому надає помічник оперативного чергового з обробки інформації на комп'ютері чергової частини МВС України.

Проведення заходів належного підбору персоналу інформаційної системи дозволить істотно зменшити ймовірність скоєння як суб'єктивних внутрішніх загроз для інформаційних ресурсів системи, так і суб'єктивних зовнішніх загроз (у разі змови окремих представників персоналу з кримінальними групами або окремими злочинними суб'єктами). Слід зазначити, що неправомірні дії персоналу призводять до найбільших збитків в організації (відповідно до статистики – 65 %).

Враховуючи специфіку підбору працівників для роботи в ОВС України та відповідні вимоги наказу МВС України від 28 квітня 2009 року № 181 [13] до працівників чергових частин ОВС України, є вагомі підстави вважати, що ці заходи будуть виконані на належному рівні. Однак, ясна річ, все ж таки існує ймовірність впливу на безпеку інформаційних ресурсів "людського фактору".

Постійний моніторинг дій користувачів інформаційних систем з об'єктами захисту дозволить своєчасно виявити можливі порушення їх безпеки та самого правопорушника. Як зазначено в роботі [13], для запобігання несанкціонованому доступу сторонніх осіб до комп'ютерів АС класу "3", що може призвести до оброблення на них недозволеної інформації, користувач для входу до операційної системи має використовувати персональні паролі.

Періодичне підвищення кваліфікації користувачів інформаційних систем по роботі з об'єктами захисту дозволить істотно знизити їх можливі несанкціоновані ненавмисні дії.

Ужиття заходів дисциплінарного впливу на користувачів ІС, у разі вчинення ними протиправних дій з об'єктами захисту, підвищить їх відповідальність при обробці оперативної інформації, що потребує захисту.

Обмеження можливості ознайомлення сторонніх осіб з роботою та документацією об'єктів захисту повинно зменшити можливий ризик стороннього несанкціонованого втручання в їх роботу.

Таким чином, організація наведених базових заходів захисту та їх комплексне використання дозволить ефективно вирішити актуальні проблеми захисту апаратно-технічних засобів та програмного забезпечення з обробки оперативної інформації про резонансні злочини та інші надзвичайні події інформаційної

системи "Зведення" чергової частини МВС України, яка є складовою частиною інформаційно-телекомунікаційної системи оперативного інформування МВС України. Слід зауважити, що аналогічні організаційні заходи можна також здійснювати в інших чергових частинах різних рівнів ОВС України.

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. : Київський нац. ун-т внутр. справ, 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. : Нац. авиац. ун-т, 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 доп. – К.: ДУІКТ, 2009. – С. 54–56.
6. *Кудінов 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.* Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України / В.А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 1. – С. 91–96.
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 доп. – К. : ДУІКТ, 2009. – С. 167–168.
10. *Кудінов В.А.* Структура бази даних автоматизованої інформаційної системи "Зведення" з обліку злочинів та надзвичайних подій, які взяті на контроль МВС України / В. А. Кудінов // Безпека дорожнього руху України. – 2003. – № 1–2. – С. 57–62.
11. *Кудінов В.А.* Основні можливості АІС "Зведення" з обліку резонансних злочинів та інших надзвичайних подій, які взяті на контроль МВС України / В. А. Кудінов // Спеціальна техніка у правоохоронній діяльності : ІІ міжнар. наук.-практ. конф., Київ, 22–23 лист. 2005 р.: тези доп. – К. : Київський нац. ун-т внутр. справ, 2006. – С. 226–232.
12. *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.
13. Про організацію діяльності чергових частин органів і підрозділів внутрішніх справ України, направленої на захист інтересів суспільства і держави від протиправних посягань: Наказ МВС України від 28.04.2009 № 181.
14. Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства : Наказ Міністерства економіки та з питань європейської інтеграції України від 23.04.2002 № 121.
15. *Шорошев В.В.* Концепція фізичної безпеки комп'ютерних систем / В.В. Шорошев, Д.В. Чирков // Захист інформації. – 2007. – № 2. – С. 5–12.
16. *Шорошев В.В.* Фізична безпека комп'ютерних систем / В. В. Шорошев, І. І. Паюшик // Захист інформації. – 2008. – № 3. – С. 4–11.

Отримано 29.11.2011