УДК 004.056.5

О. В. Захарова, А. Т. Рудий

ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДРОЗДІЛІВ МВС

Розглядаються загальні принципи організації системи захисту інформації у інформаційних системах підрозділів Міністерства внутрішніх справ. Обґрунтовано запровадження принципу поетапного здійснення технічного захисту інформації з урахуванням динаміки зміни загроз.

Ключові слова: *інформаційні технології, інформаційна система, захист інформації, інформаційні загрози, технічні заходи.*

Постановка проблеми. Інформація та мережеве оточення, у яких вона функціонує, є невід'ємними активами сучасних інформаційних систем (ІС) підрозділів МВС. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення належного рівня режиму безпеки. Поширення інформаційних і комунікаційних систем надає дедалі нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати ІС і мережеве оточення. Вимогою сьогодення висувається необхідність вирішення питань фізичної безпеки, управління інцидентами, розроблення сучасної системи менеджменту інформаційної безпеки (СМІБ).

Визначальними у процесі вирішення окреслених завдань є нормативні чинники – закони України, нормативні документи у галузі ЗІ, стандарти, відомчі акти, практики тощо. Організаційно усе підпорядковується єдиній меті – забезпечити виконання правових вимог і технічних рішень, спрямованих на забезпечення необхідного рівня захищеності активів ІС.

Порушення режиму безпеки ІС може істотно ускладнити реалізацію обраних завдань, тому вирішення проблеми формування ефективної системи захисту інформації (ЗІ) набуває важливого значення.

Це пояснюється тим, що у процесах розроблення і удосконалення систем ЗІ є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності й надійності функціонування системи безпеки загалом.

Стан дослідження. Питанням створення і функціонування систем ЗІ присвячено достатньо публікацій. З доступних наукових і науково-технічних джерел слід виокремити праці професорів В. Б. Дудикевича [1; 2], М. П. Карпінського [3], В. П. Захарова [4; 5], О. С. Петрова [6; 7], В. О. Хорошка [8].

Аналіз наукових публікацій дає підстави стверджувати, що у процесі проектування, створення і експлуатування систем ЗІ трапляються помилки та недоречності, які суттєво знижують показники ефективності їх функціонування. Вимагає обґрунтування розроблення політики інформаційної безпеки, яка визначає стратегію і тактику системи ЗІ у ІС підрозділів МВС і враховує динаміку процесів зміни типів і рівня загроз інформації, яка є одним з активних і значущих ресурсів у правоохоронній діяльності [9].

Вважаємо, що система ЗІ в ІС підрозділів МВС повинна ґрунтуватися на засадах комплексності і адаптивності.

Водночас вважаємо доцільним розробляти організаційну структуру і впроваджувати систему ЗІ відповідно до рекомендацій міжнародних стандартів та чинного законодавства України. Такими стандартами є: ISO/IEC 27002 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою [10]; ISO/IEC 27003 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації [11]; ISO/IEC 27004 Інформаційні технології. Методи захисту. Вимірювання [12]; ISO/IEC 27005 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки [13]; ISO/IEC 27006 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою [14]; ISO/IEC 27011 Інформаційні технології. Керівництво з управління інформаційною безпекою для телекомунікацій [15].

Дотримання принципів стандартів серії ISO 27000 забезпечує керування і контроль за доступом, розроблення та обслуговування апаратно-програмних систем, керування безперервністю інформаційних процесів. Відповідність вимогам стандартів серії ISO 27000 і дотримання національних правових норм з інформаційної безпеки є запорукою створення ефективної системи ЗІ.

Метою статті є визначення методів і засобів ЗІ у ІС підрозділів МВС. Пропонується використовувати набір організаційно-технічних методів і засобів, які дозволяють формувати ефективні системи ЗІ. Зауважимо, що ці методи є лише одним з аспектів реалі-

зації цілісної концепції управління інформаційною безпекою у ІС підрозділів МВС [1].

У публікації не розглядаються методи ЗІ, які ґрунтуються на системному адмініструванні та спеціальних математичних методах і алгоритмах. Основна увага зосереджена на розробленні та аналізі організаційно-технічних заходів, які будуть зрозумілими і для безпосередніх виконавців, і для вищого керівництва підрозділів МВС.

Виклад основних положень. Законодавчі заходи щодо ЗІ полягають у виконанні чинних у державі або введенні нових законів, нормативних документів, настанов, що регулюють правову відповідальність посадових осіб за витік, втрату або модифікування службової інформації, яка підлягає захисту, зокрема за спроби виконувати аналогічні дії за межами своїх повноважень, а також відповідальність сторонніх осіб за спробу навмисного несанкціонованого доступу до інформації. Мета правових заходів полягає у запобіганні можливим правопорушенням і встановленні відповідальності за здійснені правопорушення [2].

Ієрархічна структура нормативно-правових актів України, які безпосередньо або опосередковано стосуються регулювання відносин у інформаційній сфері, може бути відображена так: Конституція України; закони України; укази та розпорядження Президента України; постанови та розпорядження Кабінету Міністрів України; нормативні акти міністерств і відомств.

Правову основу у вирішенні проблем ЗІ в Україні формують Конституція України [16], закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість яких надана Верховною Радою України. Окрім того, діє низка відомчих актів, тлумачень, методик, які є обов'язковими для виконання усіма державними органами, підприємствами, установами, організаціями під час виконання функцій щодо забезпечення захисту інформації з обмеженим доступом (ІзОД), і насамперед це стосується державної таємниці.

Регулятивно-правову основу забезпечення ЗІ у ІС підприємств України різної форми власності становлять: Конституція України [16]; Концепція національної безпеки України [17]; закони України: «Про державну таємницю» [18]; «Про доступ до публічної інформації» [19]; «Про інформацію» [20]; «Про науково-технічну інформацію» [21].

З метою протидії процесам неконтрольованого витоку, несанкціонованого доступу (НСД), модифікування службової інформації та зменшення збитків від реалізування цих загроз потрібно фахово формувати заходи і вибирати засоби забезпечення ЗІ. Необхідно також володіти знаннями основних правових положень у цій галузі, вміти ефективно реалізовувати організаційні, програмно-технічні та інші заходи для забезпечення безпеки інформації.

Актуальність вирішення окресленої проблеми пов'язана із суттєвим зростанням можливостей сучасних інформаційних технологій (ІТ). Розвиток програмно-апаратних засобів, методів і способів оброблення інформації та широке застосування ІТ роблять інформацію більш уразливою.

Процедура проектування системи ЗІ та вибору засобів ЗІ в ІС – складне комплексне завдання, у вирішенні якого потрібно враховувати різні типи імовірних загроз для безпечного функціонування ІС, вартість реалізування ЗІ і наявність численних зацікавлених сторін.

Під час забезпечення ЗІ основним елементом є процедура аналізу можливих загроз для функціонування ІС, тобто загроз, що підвищують уразливість інформації, яка обробляється в ІС, призводять до її неконтрольованого витоку, випадкового або цілеспрямованого модифікування, знищення.

Засоби для системи ЗІ не варто проектувати, закуповувати або встановлювати доти, поки не буде виконаний аналіз ризиків та імовірних загроз [10]. Тільки ґрунтовний аналіз ризиків та загроз дає об'єктивну оцінку наслідків реалізації загроз, зниження коефіцієнта готовності системи ЗІ, правових проблем, інформацію для визначення найпридатніших методів і засобів забезпечення належного рівня безпеки ІС підрозділів МВС.

Розглядаючи загальні засади ЗІ в ІС, доцільно зазначити, що комплексний ЗІ в ІС передбачає використання спеціальних правових, фізичних, організаційних та програмно-апаратних засобів ЗІ, які повинні забезпечувати ідентифікування та автентифікування користувачів, розподіл повноважень доступу до технічних, інформаційних активів і сервісів ІС, реєстрування та облік спроб НСД.

Організаційні заходи ЗІ в ІС, як правило, спрямовані на чіткий розподіл відповідальності персоналу в процесах опрацювання інформації, створення декількох рубежів контролю, запобігання зовнішнім та інсайдерським загрозам, навмисному або випадковому знищенню та модифікуванню інформації.

Об'єктом технічного захисту, згідно з чинним законодавством, є інформація, яка становить державну або іншу, передбачену чинним законодавством України, таємницю, службова інформація, яка є державною власністю або передана державі у володіння, користування, розпорядження.

Технічний захист інформації (ТЗІ) здійснюється у кілька етапів: перший – визначення і аналіз загроз; другий – розроблення системи ЗІ; третій – реалізація плану ЗІ; четвертий етап – контроль за функціонуванням і керуванням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об'єктів ТЗІ, ситуаційного плану, умов функціонування ІС, оцінювання ймовірності прояву загроз та очікувані збитки від їх реалізування, підготування даних для побудови моделі загроз.

Загрози можуть здійснюватися: технічними каналами, які охоплюють канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи ЗІ або порушення цілісності інформації; НСД шляхом під'єднання до апаратури та ліній зв'язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту Web-ресурсів, застосуванням закладних пристроїв, програм та вкоріненням комп'ютерних вірусів.

На другому етапі ТЗІ розробляється план, який містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначаються зони безпеки інформації. Організаційні заходи регламентують порядок інформаційної діяльності (ІД) з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ІД.

Первинні технічні заходи передбачають ЗІ з блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають ЗІ з використанням засобів ТЗІ.

Заходи захисту інформації повинні: бути адекватні загрозам; бути розроблені з урахуванням можливих збитків від реалізування загроз і вартості захисних заходів та обмежень, які вносяться ними; забезпечувати задану ефективність ЗІ на встановленому рівні упродовж часу обмеження доступу до неї або можливості здійснення загроз.

Мінімально необхідний рівень ЗІ забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

На третьому етапі ТЗІ слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні

зони безпеки інформації, здійснити атестування технічних засобів забезпечення інформаційної діяльності (ІД), технічних засобів ЗІ, робочих місць (приміщень) на відповідність вимогам безпеки інформації [22].

ТЗІ передбачає застосування захищених програм і технічних засобів забезпечення ІД, програмних і технічних засобів ЗІ та контролю їх ефективності, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

На четвертому етапі здійснюється контроль за функціонуванням та управлінням системою ТЗІ на об'єктах ІД з метою визначення й удосконалення стану ЗІ в ІС, виявлення та запобігання порушенням системи ЗІ. Контроль стану ЗІ в ІС організовується відповідно до планів, затверджених керівниками підрозділів, шляхом проведення перевірок.

Контрольно-інспекційна робота з питань ЗІ охоплює планування та проведення перевірок стану ЗІ в ІС, щодо яких здійснюється ТЗІ, здійснення аналізу та надання настанов з удосконалення заходів із ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

Під час комплексної перевірки вивчається та оцінюється стан ЗІ у ІС, щодо яких здійснюється ТЗІ.

Під час цільової (тематичної) перевірки вивчаються окремі напрями ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ЗІ в ІС, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності у галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ЗІ.

Під час контрольної перевірки установлюється усунення недоліків, які були виявлені попередньою комплексною або цільовою перевірками. Ці перевірки можуть бути планові та позапланові, з попередженням і раптові.

Позапланова перевірка здійснюється за вказівкою вищого керівництва у разі виникнення потреби визначення повноти та достатності заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів із питань ЗІ.

Перевірки здійснюються комісіями, на які покладено виконання завдань здійснення контролю за функціонуванням системи ЗІ.

Контроль за організаційними заходами ЗІ в ІС охоплює перевірку: переліку відомостей, які підлягають захисту; окремої моделі загроз для ІС та периметру КМ; контрольованої зони, стосовно якої здійсню-

ється ТЗІ; здійснення категоріювання виділених приміщень та інформаційних активів ІС.

Система менеджменту інформаційної безпеки полягає в адаптуванні заходів з ТЗІ до поточного завдання ЗІ. За фактами зміни умов здійснення або виявлення нових загроз заходи з ТЗІ реалізовуються за найкоротший часу.

Зазначимо, що СМІБ застосовують до обраного керівництвом набору процесів функціонування, який є важливим для основного процесу функціонування ІС, тобто визначається як сфера діяльності (СД) СМІБ. У СД повинні відзначатися критичні для функціонування ІС процеси, від коректної роботи яких залежить рівень захисту інформаційних активів. Виконання цієї умови надає практичного сенсу впровадженню СМІБ – така система гарантуватиме безпечний процес функціонування ІС підрозділів МВС.

За своєю суттю СМІБ є вибором і управлінням відповідними заходами щодо захисту інформаційних активів ІС від визначених загроз відповідно до їх критичності функціонування [2].

Висновки. Сутність викладеного дає підстави стверджувати, що обмеженість національного законодавства і відсутність єдиної правової бази правоохоронних органів у боротьбі з кіберзлочинністю – одна з головних причин зростання кількості злочинів у інформаційній сфері. Тому для удосконалення ефективності правового захисту інформації необхідно провести роботу зі створення нових законодавчих та нормативно-правових документів щодо захисту інформації.

Система ЗІ у ІС підрозділів МВС повинна ґрунтуватися на засадах комплексності і адаптивності.

Заходи з ТЗІ у виділених приміщеннях, ІС та периметру КМ, роботи з атестування системи ЗІ виконуються власними силами, або передаються на аутсорсинг суб'єктам підприємницької діяльності у галузі ЗІ, які мають дозвіл і ліцензію від уповноваженого Кабінетом Міністрів України органу.

1. Гарасимчук О. І. Комплексні системи санкціонованого доступу: навч. посіб. / О. І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака. – Львів: Видавництво Львівської політехніки, 2010. – 212 с.

2. Ромака В. А. Системи менеджменту інформаційної безпеки: навч. посібник / В. А. Ромака, В. Б. Дудикевич, Ю. Р. Гарасим, П. І. Гаранюк, І. О. Козлюк. – Львів: Видавництво Львівської політехніки, 2012. – 232 с.

3. Karpinski M. Information Security / M. Karpinski. Warsaw: – Measurements, Automation and Monitoring. – 2012. – 280 p.

4. Захаров В. П. Організаційно-технічні аспекти керування захистом інформації у комп'ютерних мережах / В. П. Захаров, О. І. Зачек / Боротьба з Інтернет-злочинністю: матеріали міжнародної науково-практичної конференції, (м. Донецьк, 12–13 червня 2013 р.). – Донецьк, ДЮІ, 2013. – С. 223–225.

5. Захаров В. П. Проблеми інформаційного забезпечення правоохоронних структур: навч. посібник / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2007. – 372 с.

6. Головань С. М. Нормативне забезпечення інформаційної безпеки: підручник / С. М. Головань, О. С. Петров, В. О. Хорошко, Д. В. Чирков; за ред. проф. В. О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

7. Lahno V. A. The information protection in automated systems on transport: monograph / V. A. Lahno, A. S. Petrov. – Krakow (Poland): Knowledge press. – 2012. – 169 p.

8. Головань С. М. Нормативне забезпечення інформаційної безпеки: підручник / С. М. Головань, О. С. Петров, В. О. Хорошко, Д. В. Чирков; за ред. проф. В. О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

9. Сєвєрінов О. В. Управління інформаційною безпекою згідно міжнародних стандартів / О. В. Сєвєрінов, В. І. Черниш, М. Є. Молчанова // Системи управління, навігації та зв'язку. – К.: ЦНДІ НіУ, 2011. – Вип. 4 (20), –С. 250–253.

10. Міжнародний стандарт ISO/IEC 27002. [Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27002.html

11. Міжнародний стандарт ISO/IEC 27003. –[Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27003.html

12. Міжнародний стандарт ISO/IEC 27004. [Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27004.html

13. Міжнародний стандарт ISO/IEC 27005. –[Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27005.html

14. Міжнародний стандарт ISO/IEC 27006. [Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27006.html

15. Міжнародний стандарт ISO/IEC 27011. [Електронний ресурс]. – Режим доступу: http:// www.iso27000security.com/html/27011.html

16. Конституція України. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

17. Концепція національної безпеки України. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/3/97-вр

18. Про державну таємницю: Закон України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3855-12

19. Про доступ до публічної інформації: Закон України. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2939-17

20. Про інформацію: Закон України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

21. Про науково-технічну інформацію: Закон України. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3322-12

22. Когут В. В. Порядок атестування систем технічного захисту інформації. / В. В. Когут, Т. В. Рудий, Я. Ф. Кулешник / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави: матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. – Львів: ЛьвДУВС, 2010. – С. 90–97.

Захарова А. В., Рудий А. Т. Принципы защиты информации в информационных системах подразделений МВД

Рассматриваются общие принципы организации системы защиты информации в информационных системах подразделений МВД. Обосновано внедрение принципа поэтапной реализации технической защиты информации с учетом динамики изменения угроз.

Ключевые слова: *информационные технологии, информационная система, защита информации, информационные угрозы, технические мероприятия.*

Zakharova O. V., Rudiy A. T. Principles of information system security in the law enforcement subdivisions

General principles of organization of information security in information systems of the subdivisions of the Ministry of Internal Affairs are considered. Application of the principle of phased implementation of technical information in view of the dynamics of threat changes is grounded.

Key words: *information technologies, information security system, information security, information threats, technical measures.*

Стаття надійшла 26 вересня 2013 р.

УДК 343.85

А. І. Кунтій

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ПСИХОЛОГІЧНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ УМИСНОГО ВБИВСТВА ВЧИНЕНОГО В СТАНІ СИЛЬНОГО ДУШЕВНОГО ХВИЛЮВАННЯ

Розглядаються способи застосування спеціальних психологічних знань під час досудового розслідування умисного вбивства, вчиненого в стані сильного душевного хвилювання. Досліджуються підстави та порядок залучення спеціаліста-психолога під час здійснення огляду місця події, допиту та слідчого експерименту у провадженнях цієї категорії злочинів, порядок та особли-