УДК 351.74:004.78.056.52-048.78](477)

С. В. Сеник

ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЙНИХ ОСНОВ ПОБУДОВИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розглянуто організаційно-правові засади побудови комплексних систем захисту інформації з обмеженим доступом у діяльності підрозділів Національної поліції України. На підставі аналізу наявних теоретико-правових досліджень організаційних принципів створення комплексних систем захисту інформації, з огляду на чинні державні нормативно-правові документи та міжнародні стандарти у цій галузі запропоновано розділити побудову таких систем на одинадцять логічних етапів. Для кожного з етапів визначено основний перелік заходів, які необхідно реалізувати для забезпечення захисту інформації на достатньому рівні.

Ключові слова: *інформація, захист інформації, організаційні заходи, етапи побудови, комплексна система захисту інформації.*

Постановка проблеми. Сьогодні до інформації, як до продукту діяльності людини та об'єкта її власності чи власності держави, встановлюються дедалі жорсткіші умови щодо захисту. Основи цього захисту розробляються та постійно вдосконалюються відповідними державними органами з урахуванням умов дотримання інформаційної безпеки, зокрема й національної безпеки України. Закон України «Про інформацію» [1] у статтях 20 та 21 визначає, що вся інформація за порядком доступу класифікується на відкриту та інформацію з обмеженим доступом. Водночас інформація з обмеженим доступом поділяється на таємну, службову та конфіденційну. Віднесення інформації до того чи іншого виду часто є запорукою вибору і встановлення рівня її захисту.

Чинне законодавство України, зокрема згаданий Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2], Закон України «Про захист персональних даних» [3] та Закон України «Про державну таємницю» [4] вимагають забезпечення захисту інформації, яка становить власність держави і є інформацією з обмеженим доступом. А оскільки в діяльності підрозділів Національної поліції України циркулює інформація з обмеженим доступом усіх перелічених вище видів, виникає

необхідність не лише забезпечення її захисту, а й постійного його вдосконалення.

Стан дослідження. Вивченню організаційних засад забезпечення захисту інформації з обмеженим доступом в Україні присвячено низку робіт В. Л. Бурячка, В. Б. Дудикевича, В. О. Хорошка, В. Б. Тулубка, В. М. Максимовича, М. П. Карпінського, фахівців державної служби спеціального зв'язку та захисту інформації України К. В. Пестова, В. В. Кравчука та інших. Заданим питанням у діяльності Національної поліції значну увагу у своїх розвідках приділили В. Г. Хахановський В. С. Цимбалюк, Т. В. Рудий, В. А. Ліпкан. Однак швидкий розвиток технологій ставить нові вимоги до застосування науково обґрунтованих підходів до удосконалення питань організаційних засад побудови систем захисту інформації з обмеженим доступом.

Мета статті – дослідити наявні підходи до побудови систем захисту інформації та запропонувати осучаснений організаційно-правовий підхід щодо порядку його впровадження.

Виклад основних положень. Аналіз проведених досліджень засвідчує, що для захисту інформації, надто з обмеженим доступом, як правило, застосовують комплексну систему, під якою розуміють сукупність організаційних та інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [5]. Під час побудови такої системи використовують організаційні та інженерно-технічні заходи, комплекси технічного захисту інформації, захисту від витоку інформації через побічні електромагнітні випромінювання та наведення, а також комплекс засобів захисту від несанкціонованого доступу.

Основним компонентом організаційних заходів є розробка політики інформаційної безпеки. Окрім цього, сюди відносять і заходи, які передбачають: складання посадових інструкцій для обслуговуючого персоналу та користувачів; розробку правил для адміністрування інформаційної системи (порядку обліку, зберігання, розповсюдження, розмноження, знищення носіїв інформації, ідентифікації користувачів); порядок дій у випадку виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, несправностей засобів захисту, виникнення явищ стихійного лиха чи надзвичайних ситуацій. Окреме місце в цьому займає навчання користувачів щодо безпечної роботи в інформаційній системі.

Наступним важливим компонентом у побудові комплексної системи захисту інформації є використання інженерно-технічних заходів, під якими розуміють використання спеціальних технічних засобів для захисту інформації. Вибір таких технічних засобів залежить від рівня

захисту інформації, який необхідно забезпечити. До таких заходів належать, зокрема, застосування захищеного підключення до мережі, використання міжмережевих екранів, встановлення розмежування інформаційних потоків між частинами мережі. Нині важливим аспектом щодо використання інженерно-технічних заходів є застосування методів і засобів шифрування та захисту від несанкціонованого доступу.

Не слід також забувати про можливість, а деколи і про необхідність установлення охоронної сигналізації, систем контролю та управління доступом, обладнання приміщень засобами захисту від витоку мовної (акустичної) інформації та від витоку інформації каналами побічних електромагнітних випромінювань.

Створення комплексу технічного захисту інформації, захисту від витоку інформації через побічні електромагнітні випромінювання та наведення обов'язково передбачено, якщо в інформаційній системі обробляється інформація, що становить державну таємницю (1–3 категорій об'єктів, відповідно до ТПКО-95 [6]), або у разі, якщо потребу в цьому визначено власником інформації [7]. Встановлення комплексу засобів захисту також здійснюється у випадку, якщо в інформаційно-телекомунікаційній системі опрацьовується інформація, що є власністю держави (може містити різні види інформації), необхідність захисту якої визначається законодавством, а також інформаційно-телекомунікаційні системи, де таку необхідність установив власник інформації. Цей комплекс має забезпечувати захист інформації з обмеженим доступом від витоку технічними каналами, насамперед каналами побічних електромагнітних випромінювань та наведень.

Під час створення комплексу технічного захисту інформації має застосовуватися сукупність організаційно-правових, інженерно-технічних заходів та засобів, до яких вдаються з метою захисту від витоку інформації з обмеженим доступом технічними каналами. Створення та випробовування комплексу технічного захисту інформації проводиться відповідно до положень НД ТЗІ 1.1-005-07 [8], НД ТЗІ 1.6-003-04 [9], НД ТЗІ 3.1-001-07 [10], НД ТЗІ 3.3-001-07 [11], НД ТЗІ 2.1-002-07 [12]. Задля з'ясування потреби запровадження заходів захисту інформації від витоку технічними каналами проводиться спеціальне дослідження персональних комп'ютерів, під час якого визначаються можливі канали витоку інформації. За результатами такого аналізу приймається рішення про необхідність встановлення активних та пасивних технічних засобів захисту інформації.

З метою створення єдиного підходу до питань побудови комплексних систем захисту інформації в Україні розроблено та запроваджено низку нормативних документів. Приміром, створення ком-

плексної системи захисту інформації в інформаційно-телекомунікаційних системах здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [13] на підставі технічного завдання, розробленого згідно з вимогами нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі» [14].

Вище було наголошено, що науковці в плані організації побудови комплексної системи захисту інформації по-різному виокремлюють етапи її створення. Проаналізувавши їхні роботи, а також врахувавши вимоги сьогодення щодо побудови комплексних систем захисту інформації, зокрема з використанням міжнародних стандартів [15], вважаємо, що найоптимальнішим на сьогодні є поділ на такі етапи [16]:

1. *Підготовка, створення та затвердження організаційної документації.* Під час виконання цього етапу проводиться аналіз організаційно-розпорядчих та нормативно-правових документів зі захисту інформації. До організаційно-розпорядчих документів, зазвичай, належать: організаційна структура, штатний розклад, положення про відділи і посадові інструкції співробітників, пов'язаних з експлуатацією інформаційно-телекомунікаційної системи тощо. За результатами аналізу створюються проекти документів, які визначатимуть організаційну складову комплексної системи захисту інформації, проект положення про службу захисту інформації, проекти посадових інструкцій, функціональних обов'язків тощо.

2. *Обстеження інформаційної інфраструктури.* Для кожної конкретної інформаційно-телекомунікаційної системи структура і вимоги до систем комплексного захисту інформації обумовлюються властивостями інформації, яка буде оброблятися, класом інформаційної системи й умовами її експлуатації. На цьому етапі має проводитися аналіз архітектури системи, її складових елементів та топології побудови, а також визначатися типи користувачів системи, типізуватися інформація, що обробляється в інформаційно-телекомунікаційній системі. За результатами виконання цього етапу мають бути підготовлені: акт обстеження інформаційно-телекомунікаційної системи, який включає опис, принципи побудови та архітектуру інформаційно-телекомунікаційної системи, та перелік об'єктів інформаційно-телекомунікаційної системи, які підлягають захисту.

3. *Розробка технічного завдання на створення комплексної системи захисту інформації.* Цей нормативний документ має визначити

всі основні вимоги до комплексної системи захисту інформації та можливі способи реалізації її складових сегментів. У цьому ж документі встановлюються вимоги до складу і порядку розробки та впровадження технічних засобів, які забезпечують безпеку інформації у процесі її обробки в обчислювальній системі, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза інформаційно-телекомунікаційною системою з метою доповнення до комплексу програмно-технічних засобів захисту інформації.

4. *Розробка плану захисту інформації*. Після обстеження інфраструктури (див. другий етап), грунтуючись на переліку об'єктів інформаційно-телекомунікаційної системи, що підлягають захисту, слід розробити такі документи: «Модель загроз інформації. Модель порушника»; «Положення про Службу захисту інформації»; «Політика безпеки інформації».

5. *Розробка технічного проекту на створення комплексної системи захисту інформації*. Узгодивши технічне завдання на створення комплексної системи захисту інформації, розробляється технічний проект на створення комплексної системи захисту інформації. Цей проект є комплектом документів, до якого входить частина документів, розроблених на попередніх стадіях, а також нові документи, в яких описано порядок створення, експлуатації та модернізації комплексної системи захисту інформації. Проект розробляється відповідно до технічного завдання на створення комплексної системи захисту інформації. Під час його розробки обґрунтовуються і приймаються проектні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів комплексної системи захисту інформації, а також різноманітних засобів і заходів захисту інформації. За результатами цього етапу створюється комплекс експлуатаційної і робочої документації, яка необхідна для забезпечення тестування, проведення робіт з налагодження, випробувань комплексної системи захисту інформації та управління нею.

6. *Приведення інформаційної інфраструктури у відповідність із технічним проектом на створення комплексної системи захисту інформації*. Особливістю цього етапу є те, що на момент ухвалення рішення про створення комплексної системи захисту інформації не відома вартість самого проекту. Тому на цьому етапі існує велика ймовірність підключення до його виконання інших виконавців. Тут також можуть виконуватися будівельні, монтажні, пусконалагоджувальні роботи, роботи, пов'язані зі встановленням належних технічних або криптографічних засобів захисту інформації, засобів фізичного захисту елементів інформаційно-телекомунікаційної системи тощо.

7. *Розробка документації для експлуатації на комплексну систему захисту інформації.* На цьому етапі виконавець комплексної системи захисту інформації послідовно має розробити пакет документів, у якому міститься:

– інструкції з експлуатації комплексної системи захисту інформації та її елементів;

– процедури регламентного обслуговування комплексної системи захисту інформації;

– правила і положення з проведення тестування й аналізу роботи комплексної системи захисту інформації;

– документація для адміністраторів і користувачів;

– формуляр комплексної системи захисту інформації інформаційно-телекомунікаційної системи.

8. *Впровадження комплексної системи захисту інформації.* Під час цього етапу слід виконати усі пусконалагоджувальні роботи, провести навчання та інструктаж обслуговуючого персоналу, узгодити правила та режими експлуатації комплексної системи захисту інформації. Цей етап також має передбачати проведення й інших заходів, зокрема:

– організацію захисту інформації від несанкціонованого доступу;

– організацію антивірусного захисту інформації;

– розробку програми і методики попередніх випробувань;

– проведення попередніх випробувань.

9. *Випробування комплексної системи захисту інформації.* На цьому етапі потрібно провести попередні випробування комплексної системи захисту інформації з метою підтвердження результативності її роботи і відповідності положенням, визначеним технічним завданням на створення комплексної системи захисту інформації. У процесі випробувань виконуються тестові завдання і контролюються отримані результати, які і є індикатором працездатності спроектованої комплексної системи захисту інформації. За результатами випробування комплексної системи захисту інформації робиться висновок стосовно можливості подання її на державну експертизу. Під час проведення випробувань:

– відпрацьовуються технології обробки інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів інформаційно-телекомунікаційної системи й автоматизованого контролю за діями користувачів;

– обслуговуючий персонал набуває практичних навиків з використання технічних і програмно-апаратних засобів захисту інфор-

мації, засвоює вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

– проводиться (за потреби) доопрацювання програмного забезпечення, додаткове налаштування і конфігурація комплексу засобів захисту інформації від несанкціонованого доступу;

– здійснюється (за потреби) коректування робочої та експлуатаційної документації.

10. *Проведення державної експертизи комплексної системи захисту інформації та отримання атестата відповідності*. На цьому етапі потрібно здійснити:

– підготовку комплексної системи захисту інформації до проведення державної експертизи в Адміністрації Держспецзв'язку;

– узгодження з Адміністрацією Держспецзв'язку результатів експертизи й отримати атестат відповідності.

Державна експертиза проводиться з метою визначення відповідності комплексної системи захисту інформації технічному завданню на її створення, вимогам нормативної документації та з'ясування можливості введення комплексної системи захисту інформації в експлуатацію в інформаційно-телекомунікаційній системі.

Для кожної конкретної інформаційно-телекомунікаційної системи структура, вимоги і склад визначаються властивостями інформації, яка у ній циркулює, класом та умовами експлуатації інформаційно-телекомунікаційної системи.

11. *Супровід комплексної системи захисту інформації.* На цьому етапі мають виконуватися роботи з організаційного забезпечення функціонування комплексної системи захисту інформації та управління засобами захисту інформації відповідно до плану захисту та експлуатації, гарантійного та післягарантійного технічного обслуговування засобів захисту інформації.

Висновки. Таким чином, за результатами аналізу наукових досліджень учених з питань забезпечення інформаційної безпеки та захисту інформації в Україні загалом та в діяльності Національної поліції зокрема, а також з огляду на міжнародні стандарти у цій сфері, вимоги сьогодення щодо захисту інформації, запропоновано в організаційному плані процес створення комплексних систем захисту інформації розділити на одинадцять логічних етапів їх побудови та експлуатації. Для кожного з них передбачено основний набір заходів, які потрібно провести.

Також слід звернути увагу на те, що під час побудови комплексної системи захисту інформації необхідно неухильно дотримува-

тися нормативно-правових засад їх проектування, побудови, експлуатації та розвитку.

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: http://zakon2.rada.gov.ua/laws/show/2657-12/.

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/.

3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: http://zakon2.rada.gov.ua/laws/show/2297-17/.

4. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. URL: http://zakon.rada.gov.ua/laws/show/3855-12.

5. Що таке комплексна система захисту інформації (КСЗІ). URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi.

6. Тимчасове положення про категоріювання об'єктів ТПКО-95: наказ Державної служби України з питань технічного захисту інформації від 10.07.1995 р. № 35. URL: http://zakon.rada.gov.ua/rada/show/v0035267-95.

7. Положення про державну експертизу в сфері технічного захисту інформації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z0820-07.

8. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12.2007 р. № 232. К., 2007.

9. НД ТЗІ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації: затверджено наказом ДСТСЗІ СБ України від 10.03.2004 р. № 04. К., 2004.

10. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Передпроектні роботи: затверджено наказом Адміністрації Держспецзв'язку від 12.12.2007 р. № 232. К., 2007.

11. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації: затверджено наказом Адміністрації Держспецзв'язку від 12.12.2007 р. № 232. К., 2007.

12. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення: затверджено наказом Адміністрації Держспецзв'язку від 12.12.2007 р. № 232. К., 2007.

13. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05: наказ Департаменту спеціальних телекомунікаційних систем та захисту ін-

формації Служби безпеки України від 08.11.2005 р. № 125. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835

14. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 р. (зі зміною № 1, затвердженою наказом Департаменту СТСЗІ СБ України від 18.06.2002 р. № 37 та із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 р. № 806). URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwj1x_Cyrc_eAhWBo4sKHRKVD94QFjAAegQICBAC&url=http%3A%2F%2Fwww.dsszzi.gov.ua%2Fdsszzi%2Fdoccatalog%2Fdocument%3Fid%3D106349&usg=AOvVaw244WydoNtjePKusx4FbJ9

15. Рудий Т. В., Захарова О. В., Сеник В. В., Сеник С. В., Ізьо М. І. Організаційно-правовий супровід захисту інформаційних систем підрозділів Національної поліції України на основі міжнародних стандартів. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2017. Вип. 2. С. 213–225.

16. Сеник С. В. Етапи побудови комплексних систем захисту інформації у підрозділах Національної поліції України // Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої освіти зі специфічними умовами навчання: зб. наук. статей за матеріалами доповідей учасників Всеукраїнської науково-практичної конференції (21 грудня 2018 року) / упоряд. Т. В. Магеровська. Львів: ЛьвДУВС, 2018. С. 87–90.

Senyk S. V. Investigation of organizational principles for the construction of integrated systems for the protection of information with restricted access in the units of the National Police of Ukraine

The organizational and legal principles of construction of integrated systems for the protection of information with limited access of the activities of the units of the National Police are considered. On the basis of the analysis of available theoretical and legal research of the organizational principles for the creation of integrated information security systems, taking into account the current state legal documents and international standards in this field, it is proposed to organizationally divide the construction of such systems into eleven logical stages: preparation, creation and approval of organizational documents; survey of information infrastructure; development of a technical task for the creation of a comprehensive information security system; development of information protection plan; development of a technical project for the creation of a comprehensive information security system; bringing the information infrastructure in line with the technical project to create a comprehensive information security system; development of documentation for operation on an integrated system of information security; introduction of integrated information security system; testing of integrated information security system; conducting state expertise of a comprehensive information security system and obtaining a certificate of conformity; maintenance of integrated information security system. For each of the stage defined a basic list of measures that need to be implemented to ensure the

protection of information at an adequate level is determined. Also, pay attention to the fact that during the construction of an integrated information security system, the legal and regulatory framework for their design, construction, operation and development should be strictly adhered to.

The list of the main current legal documents on information protection in Ukraine is given in the references to this publication. Compliance with these regulatory and legal principles, as well as carrying out the specified list of organizational measures (stages) during the construction of integrated information security systems will allow to achieve the necessary level of information security in the information and telecommunication systems of the National Police.

Key words: *information, information protection, organizational measures, stages of construction, complex information security system.*

Стаття надійшла 21 грудня 2018 р.

УДК 351.741.078.3(477)

В. В. Середа,
Ю. А. Хатнюк

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ, ЩО ЗДІЙСНЮЮТЬ АНАЛІТИЧНУ РОБОТУ

Розкрито зміст діяльності підрозділів Національної поліції України, що здійснюють аналітичну роботу. Аргументовано, що підрозділи організаційно-аналітичного забезпечення та оперативного реагування відіграють центральну роль в інформаційно-аналітичному забезпеченні органів Національної поліції, оскільки виконують функції з координації, аналізу, планування, контролю й узгодження дій територіальних органів (підрозділів) поліції з реалізації державної політики у сфері забезпечення публічної безпеки і порядку, охорони та захисту прав і свобод людини й протидії злочинності.

Ключові слова: *підрозділи Національної поліції, аналітична робота, організаційно-аналітичне забезпечення, ситуаційний центр, оперативна обстановка, інформаційні технології.*

Постановка проблеми. Курс на розбудову в Україні правової держави, яка забезпечує охорону прав, свобод і законних інтересів громадян, верховенство права в усіх сферах суспільного життя, залишається одним із головних напрямів державного будівництва й інтеграції до європейської спільноти. Подальший розвиток демократії, забезпечення прав і свобод громадян нерозривно пов'язані з підвищен-