ISSN 1995-6134

УДК 351.74(477)
І.С. ОВЕРЧЕНКО, Національний університет біоресурсів і природокористування України

ІНФОРМАЦІЯ В СИСТЕМІ МВС УКРАЇНИ ЯК ОБ'ЄКТ ТЕХНІЧНОГО ЗАХИСТУ

Ключові слова: *інформація, МВС України, технічний захист*

Технічному захистові інформації в органах і підрозділах внутрішніх справ України притаманна певна специфіка, обумовлена особливостями інформації, що виступає об'єктом даного виду захисту в системі Міністерства внутрішніх справ України.

У контексті проблем, що розглядатимуться в рамках даної статті і є її метою, для аналізу масиву інформації органів внутрішніх справ як об'єкту технічного захисту, на нашу думку доцільно використати підхід, запропонований у роботі В.А. Хорошко, який для обрання того чи іншого способу захисту інформації виділяє наступні чинники: вид інформації, що циркулює на об'єкті; форма зберігання, обробки та передачі інформації, що підлягає охороні; вид носіїв інформації; імовірні способи вчинення атак на інформацію; імовірні наслідки впливу таких атак [1].

Проведемо аналіз цих факторів щодо інформації, яка циркулює в органах внутрішніх справ України. При цьому під циркуляцією інформації в ОВС України, згідно з розпорядженням МВС України від 12.07.2005 р. № 2 [2], розуміємо обговорення, формування, пересилання, приймання, перетворення, оброблення, зберігання та накопичення інформації.

У загальному випадку інформація – це відомості (або їх сукупність) про предмети, об'єкти, явища та процеси оточуючого нас світу [3, с.363]. Змістовне наповнення цього поняття серед науковців залишається дискусійним. Це обумовлюється специфічним характером принципів і методів вивчення та використання інформації в різних галузях науки і практики [4, с.70]. Зважаючи на викладене, нами було обране визначення інформації, що є найбільш розповсюдженим у галузі технічного захисту інформації (ТЗІ).

Стосовно *виду інформації,* що циркулює в ОВС – сьогодні не існує загальноприйнятої класифікації. Залежно від обраних для класифікації підстав, А.Ю. Ільницький, В.А. Саницький, В.В. Шорошев пропонують вирізняти *кримінальну, оперативно-довідкову, статистичну та аналітичну, архівну, загальносистемну та прикладну* інформацію [5, с.13].

В.М. Плішкін, відповідно до сфери виникнення, виділяє *елементарну* (нежива природа), *біологічну* (світ тварин і рослин) та *соціальну* (людське суспільство) інформацію [6, с.320].

О.О. Кулініч для класифікації інформації пропонує послуговуватись наступними підставами: *режим доступу, характер і призначення інформації, спосіб поєднання з матеріальним носієм інформації* [7, с.13–14]. К.І. Бєляков пропонує використовувати наступні категорії інформації: *статистична; масова; інформація про діяльність органів державної влади та органів місцевого самоврядування; правова; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація* [8, с.268]. О. Марценюк вирізняє: *відкриту, конфіденційну, обмежено обігоздатну та заборонену інформацію* [9, с.23].

Принципове значення для дослідження має класифікація інформації *за режимом доступу* до неї, яка запропонована в Законі України «Про інформацію», з урахуванням специфіки діяльності органів внутрішніх справ. У загальному вигляді дана класифікація представлена у додатку В. При цьому, відповідно до статті 30 згаданого закону, *конфіденційна інформація* – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. До *таємної інформації* належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Стосовно

ISSN 1995-6134

інформації, що є власністю держави і перебуває в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою збереження їй може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

В органах внутрішніх справ циркулює інформація всіх вищезазначених категорій. Зокрема, на підставі Зводу відомостей, що становлять державну таємницю [10], в системі Міністерства внутрішніх справ України розроблюється Розгорнутий перелік відомостей, що становлять державну таємницю. До даного переліку входять окремі відомості у сфері державної безпеки і охорони правопорядку (розділ 4 ЗВДТ); економіки, науки і техніки (розділ 2 ЗВДТ) та деякі інші. При цьому слід враховувати, що охорона державної таємниці, на думку фахівців у галузі ТЗІ, є одним із найважливіших завдань органів державної влади [11, с.50].

Щодо конфіденційної інформації, яка є власністю держави – вона також використовується в органах та підрозділах МВС України. Перелік такої інформації встановлено відповідними наказами з урахуванням орієнтовних критеріїв віднесення інформації до конфіденційної, визначених Кабінетом Міністрів України [12]. До такої інформації належать окремі дані у сфері оперативно-розшукової діяльності, охорони громадського порядку, боротьби з окремими видами злочинів [13] тощо.

Стосовно відкритої інформації – в органах внутрішніх справ представлені всі категорії інформації, перераховані у Законі України «Про інформацію». Зокрема, це статистична інформація, адміністративна інформація, масова інформація, інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування, правова інформація, інформація про особу, інформація довідково-енциклопедичного характеру, соціологічна інформація.

Якщо розглядати інформацію органів внутрішніх справ як об’єкт захисту від її витоку технічними каналами, слід зауважити наступне: таємна та конфіденційна інформація в системі Міністерства внутрішніх справ відповідно до чинного законодавства в обов’язковому порядку підлягає технічному захисту. Стосовно відкритої інформації – вона також має бути відповідним чином захищена, оскільки є власністю держави. У першу чергу – це комп’ютерна інформація (наприклад дані, що містяться на офіційному сайті Міністерства внутрішніх справ, його регіональних підрозділів), а також деякі інші її категорії залежно від тих чи інших конкретних обставин.

Визначення основних *форм зберігання, обробки та передачі інформації* в органах внутрішніх справ різними фахівцями реалізується неоднозначно [5–9].

Натомість, зважаючи на вивчення значного масиву емпіричних даних, переконані, що основними *формами зберігання, обробки та передачі інформації* в органах внутрішніх справ, на наш погляд, є:

– зберігання, обробка та передача інформації у вигляді матеріальних носіїв;

– зберігання, обробка та передача інформації в електронному вигляді;

– зберігання, обробка інформації у свідомості людей та її передача у мовному вигляді.

Стосовно *першої форми* зазначимо, що для органів внутрішніх справ слід враховувати відсутність матеріального виробництва в ОВС. Крім того, вважаємо за доцільне об’єднати такі категорії носіїв, як документи, публікації та технічні носії до однієї групи – документи та інші матеріальні носії інформації, оскільки порядок роботи з ними як з носіями інформації в органах внутрішніх справ з точки зору ТЗІ не матиме суттєвих відмінностей. З урахуванням особливостей інформаційної діяльності ОВС, нами пропонується наступна класифікацію носіїв (джерел) інформації, характерних для системи МВС України. Такими носіями є:

– особи, що мають (або можуть отримати)

ISSN 1995-6134

доступ до інформації;

– документи та інші матеріальні носії інформації;

– технічні засоби та системи обробки інформації;

– вдходи виробничої діяльності.

Імовірні способи вчинення атак на інформацію у значній мірі залежать від форми зберігання, обробки та передачі інформації, а також від тих цілей, що переслідує ймовірний порушник [14, 15]. У загальному вигляді, способи вчинення атак на інформацію перераховані в державному стандарті ДСТУ 3396.0-96. Відповідно до цього документу атаки можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наведень, акустичні, оптичні, радіо-, радіотехнічні, хімічні й інші канали;

– каналами спеціального впливу через формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації чи нав'язування помилкової інформації, застосування закладних пристроїв і програм, упровадження комп'ютерних вірусів.

Однак даний підхід не єдиний – існують і інші науково обґрунтовані класифікації. Більше того, досвід використання стандарту ДСТУ 3396.0-96 у практичній діяльності, дозволяє зробити висновки щодо неоптимальності вищезгаданих його положень. Загалом сучасні дослідники проблем технічного захисту інформації не дійшли згоди щодо виокремлення та обґрунтування існування тих чи інших способів вчинення атак на інформацію. Здійснений нами аналіз останніх наукових досліджень у галузі ТЗІ вказує, що існуюча множина підходів до вирішення цієї задачі настільки різноманітна та неоднозначна, що не дозволяє виокремити навіть певні групи дослідників, які притримуються схожих чи однакових поглядів на поставлену проблему.

Порівняння викладених у працях різних авторів думок дозволило нам виділити декілька суттєвих положень, що мають ураховуватись при проведенні класифікації ймовірних способів вчинення атак на інформацію.

По-перше, більшість фахівців у галузі технічного захисту інформації визнають існування *технічних каналів витоку інформації (ТКВІ),* як одного з основних джерел несанкціонованого витоку інформації. Слід однак зауважити, що єдине визначення терміну ТКВІ сьогодні відсутнє, не дивлячись на те, що дана понятійна категорія широко використовується як у нормативно-правовій базі України [16, 17] так і в роботах провідних вчених [1, 18, 19].

На наш погляд, синтезуючи положення досліджень із даної тематики, *технічний канал витоку інформації – це сукупність носія інформації, середовища розповсюдження інформаційного сигналу, завад та шумів, що заважають передаванню сигналу, та засобу технічної розвідки*.

По-друге, технічні канали витоку інформації на думку фахівців у галузі ТЗІ, є одним із *способів несанкціонованого доступу до інформації.* Причому такої думки дотримуються В.В. Домарев [19], В.О. Хорошко й А.О. Чекатков [1] та інші. У процесі аналізу наукових джерел нам не зустрілося відмінних від даного підходів до поставленого питання, отже ця точка зору прийнята нами без додаткових застережень.

По-третє, окремої уваги заслуговує думка авторів А.Ю. Ільницького, В.А. Саницького, В.В. Шорошева, які звертають увагу [5] на той факт, що канали несанкціонованого доступу законодавець у Державному стандарті ДСТУ 3396.0-96 визначив окремою групою. Дані дослідники пропонують у загальному випадку вважати, що кожний вид потенційної загрози реально і фізично здійснюється за визначеною сукупністю або *потенційних каналів несанкціонованого доступу,* або ж *потенційних каналів несанкціонованого впливу* щодо захищуваної інформації. Окремо науковці зауважують, що загрози несанкціонованого доступу, на думку західних фахівців посідають пріоритетніше місце і, відповідно, досить час-

ISSN 1995-6134

то використовуються як єдиний показник захищеності інформації в цілому, а отже потенційним каналам несанкціонованого впливу не приділяється належна увага [5, с.16]. В.О. Хорошко та А.О. Чекатков [1] вказують, що у деяких випадках зловмисник, якому не вдається отримати інформацію технічними каналами, може вдатися до її *знищення*.

Крім того, навмисне знищення інформації може застосовуватися і для приховання слідів її несанкціонованого отримання. Вірусне зараження автоматизованої системи також розглядається з точки зору потенційної можливості знищення інформації [5, с.252], хоча й відмічається, що можливості сучасних вірусів значно ширші та окремі з їхніх представників призначені саме для отримання інформації.

На наш погляд, найбільш обґрунтованим є підхід авторів А.Ю. Ільницького, В.А. Саницького, В.В. Шорошева, за яким щодо предмета нашого дослідження, дозволяє дійти висновку, що поряд з *потенційними каналами несанкціонованого доступу,* існують *потенційні канали несанкціонованого впливу* щодо захищуваної інформації. Дана позиція підтверджується результатами проведеного опитування фахівців сфери інформаційної безпеки.

Таким чином, на основі узагальнення отриманих висновків, можемо констатувати, що на сьогодні існують технічні канали витоку інформації, як підвиду каналів несанкціонованого доступу, та окремою групою канали несанкціонованого впливу. Більше того, за аналогією з існуванням *технічних каналів витоку інформації,* як підвиду *каналів несанкціонованого доступу,* можна логічно припустити існування *технічних каналів несанкціонованого впливу на інформацію,* як підвиду *каналів несанкціонованого впливу.*

На підставі отриманих результатів пропонуємо виокремлювати два види ймовірних способів вчинення атак на інформацію: атаки, що реалізуються шляхом несанкціонованого доступу (підвидом є атаки, що реалізуються шляхом використання технічних каналів витоку інформації) та атаки, що реалізуються шляхом несанкціонованого впливу (підвидом є атаки, що реалізуються шляхом використання технічних каналів несанкціонованого впливу на інформацію).

З урахуванням отриманих вище результатів, нами встановлено наступні особливості реалізації технічного захисту інформації в системі МВС України:

1) МВС України є одним із суб'єктів адміністративно-правової нормотворчості з питань ТЗІ;

2) норми адміністративного права, що містяться у відомчих документах МВС України з питань ТЗІ: встановлюють правове положення і компетенцію підрозділів ТЗІ МВС України та інших суб'єктів системи ТЗІ ОВС; регулюють діяльність з ТЗІ в системі МВС України; визначають порядок взаємодії між суб'єктами системи ТЗІ МВС України;

3) переважна більшість інформації з питань ТЗІ в ОВС є інформацією з обмеженим доступом;

4) стан відомчого регулювання не відповідає вимогам часу і потребує підвищеної уваги з боку юридичної науки.

ЛІТЕРАТУРА

1. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков ; под ред. Ю. С. Ковтанюка – К. : Изд-во Юниор, 2003. – 504 с.

2. Розпорядження МВС України «Про приведення стану ТЗІ в органах і підрозділах МВС України у відповідність до вимог законодавства» : від 12.07.2005 р., № 2.

3. Словник іншомовних слів / за ред. О. С. Мельничука. – К., 1985. – 966 с.

4. Мірошниченко С. Організація діяльності прокуратури із запобігання організованій злочинності / С. Мірошниченко // Право України. – 2006. – № 11. – С. 70–73.

5. Основи захисту інформації від несанкціонованого доступу : наук.-метод. посіб. / [А. Ю. Ільницький, В. А. Саницький, В. В. Шорошев та ін.]. – К. : Нац. акад. внутр. справ України, 2002. – 208 с.

6. Плішкін В. М. Теорія управління органами внутрішніх справ : підручник / В. М. Плішкін ; за ред. Ю. Ф. Кравченка. – К. :

ISSN 1995-6134

НАВСУ, 1999. – 702 с.

7. Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних прав : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О. О. Кулініч. – К., 2006. – 20 с.

8. Беляков К. И. Управление и право в период информатизации : монография / К. И. Беляков. – К. : Изд-во «КВІЦ», 2001. – 308 с.

9. Марценюк О. Режими доступу до інформації в системі українського права / О. Марценюк // Юридична Україна. – 2006. – № 7. – С. 23–28.

10. Наказ Служби безпеки України «Звід відомостей, що становлять державну таємницю» : від 12.08.2005 р., № 440.

11. Артемов В. Правові проблеми захисту інформації з обмеженим доступом на шляху України до НАТО / В. Артемов // Підприємництво, господарство і право. – 2006. – № 10. – С. 50–53.

12. Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави» : від 27.11.1998 р., № 1893 // Офіційний вісник України. – 1998. – № 48. – С. 31.

13. Леви А. А. Особенности предварительного расследования преступлений, осуществляемого с участием адвоката / А. А. Леви, М. В. Игнатьева, Е. И. Капица. – М. : Юрлитинформ, 2003. – 127 с.

14. Наден О. Проблеми законодавчого регулювання суспільних відносин у мережі Інтернет у контексті її протиправного використання терористичними організаціями / О. Наден // Юридична Україна. – 2006. – № 7. – С. 90–96.

15. Основи інформаційного права України : навч. посіб. / [В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін.] ; за ред. М. Я. Швеця, Р. А. Калюжного, П. В. Мельника. – К. : Знання, 2004. – 274 с.

16. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. – Введено вперше ; Чинний від 1997-01-01. – К. : Держстандарт України, 1997. – 15 с.

17. ДСТУ 3396.2-97. Технічний захист інформації. Терміни та визначення. – Введено вперше ; Чинний від 1998-01-01. – К. : Держстандарт України, 1997. – 16 с.

18. Бузов Г. А. Защита от утечки информации по техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.

19. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ТИД «ДС», 2004. – 992 с.

Оверченко І. С. Інформація в системі МВС України як об'єкт технічного захисту / І. С. Оверченко // Форум права. – 2011. – № 1. – С. 717–721 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2011-1/11oicotz.pdf

Розглянуто категорії та класифікація інформації, встановлені особливості реалізації технічного захисту інформації в системі МВС України.

***

Оверченко И.С. Информация в системе МВД Украины как объект технической защиты

Рассмотрены категории и классификация информации, установлены особенности реализации технической защиты информации в системе МВД Украины.

***

Overchenko I.S. Information in System of the Ministry of Internal Affairs of Ukraine as Object of Technical Protection

Categories and information classification are considered, features of realization of technical protection of the information in system of the Ministry of Internal Affairs of Ukraine are established.