УДК 343.98:343.7

Антонюк Поліна Євгенівна –
науковий співробітник навчального відділу
ННІПСК Київського національного
університету внутрішніх справ

Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності

У статті розглядаються основні способи вчинення атак на інформацію, а також пропонується їхня класифікація, що слугує одним з напрямів протидії комп'ютерній злочинності.

Сьогодні в Україні продовжуються процеси формування системи технічного захисту інформації. Дана система є складовою системи національної безпеки (СНБ), а отже від рівня її досконалості залежить і стабільність усієї СНБ в цілому. Питання організації ефективної діяльності СНБ та взаємодії її складових є предметом окремого дослідження. Серед робіт, присвячених вивченню проблем національної безпеки, в яких між іншими розглядається також дане питання, слід назвати праці Ліпкана В.А. [1], Левицької М.Б. [2], Бодрука О.С. [3], Гурковського В.І. [4]. Поряд з цим існує досить велика кількість досліджень, присвячених виключно проблемам технічного захисту інформації (ТЗІ) – це роботи Домарева В.В. [5], Хорошко В.О., Чекаткова А.О. [6], Ярочкіна В.І. [7] та інших.

Проведений нами аналіз вищезазначених робіт дозволив дійти висновку, що у працях, присвячених проблемам національної безпеки, питанням ТЗІ приділено явно недостатньо уваги. Поряд з цим у роботах з технічного захисту інформації досить рідко використовується методологія націобезпекознавчого підходу, що, на нашу думку, не дозволяє у повній мірі дослідити деякі з аспектів цієї діяльності. Відповідно до даного підходу, національну безпеку слід розглядати в усій розмаїтості форм вияву [1, с. 261]. Однією з таких форм є технічний захист інформації як складова інформаційної безпеки. Переконані, що дослідження проблемних питань у галузі технічного захисту інформації з використанням найновіших наукових доробок сфери націобезпекознавства дозволить удосконалити систему ТЗІ, включивши процес її формування до основних напрямів протидії комп'ютерній злочинності і розвитку системи національної безпеки в цілому.

Використання концепції адекватності, запропонованої у процесі дослідження системи забезпечення національної безпеки Ліпканом В.А. [1, с. 387] по відношенню до системи технічного захисту інформації України, дозволяє дійти висновків, аналогічних отриманим автором монографії [1]: *обсяг та складність завдань, що розв'язуються системою забезпечення ТЗІ України, залежить від проведеної на основі моніторингу оцінки тих чи інших безпекогенних чинників, рівня їх небезпеки і можливих наслідків у випадку реалізації*. По відношенню до предмету нашого дослідження, такий підхід дозволяє визначити перелік ймовірних способів вчинення атак на захищувану інформацію, як один із основних факторів, що має вирішальне значення для обрання того чи іншого варіанту організації захисту інформації у кожному випадку, коли власник визначає її як таку, що потребує захисту.

Від того, якими ймовірними способами зловмисник намагатиметься вплинути на інформацію, залежить обрання засобів захисту, кількісний та якісний склад сил, що залучатимуться до побудови системи технічного захисту інформації тощо. Відповідно, якщо розглядати *систему технічного захисту секретної інформації* – ймовірні способи вчинення атак на таку інформацію мають важливе значення для

прийняття рішення про використання тих чи інших технічних засобів захисту і повинні обов'язково враховуватись при розробці нормативно-правової бази, що регламентує порядок здійснення технічного захисту на підприємстві в установі чи організації, що використовують у своїй діяльності державну таємницю. Для *системи технічного захисту інформації, яка не становить державної таємниці*, ймовірні способи вчинення атак безпосередньо впливатимуть на обсяг коштів, що слід виділити на створення та забезпечення функціонування такої системи.

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. У загальному вигляді, шляхи несанкціонованого впливу на інформацію перераховані в державному стандарті ДСТУ 3396.0–96 (Технічний захист інформації. Основні положення). Відповідно до цього документу атаки можуть здійснюватися [8]:

– 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 й інші науково обґрунтовані класифікації. Більше того, досвід використання стандарту ДСТУ 3396.0-96 у практичній діяльності дозволяє нам зробити висновки щодо неоптимальності вищезгаданих його положень. Загалом нинішні дослідники проблем технічного захисту інформації не дійшли згоди щодо виокремлення та обґрунтування існування тих чи інших способів вчинення атак на інформацію. Проведений нами аналіз останніх наукових досліджень у галузі ТЗІ вказує, що існуюча множина підходів до вирішення цієї задачі наскільки 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 моментів, 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 на сьогодні відсутнє, не дивлячись на те, що дана понятійна категорія широко використовується як у нормативно-правовій базі України [8, 9], так і у роботах провідних вчених [5, 6, 10]. Більшість авторів пропонують під ТКВІ розуміти сукупність: **носія інформації** (автори [10] пропонують використовувати термін "джерело інформації"), **середовища розповсюдження інформаційного сигналу** та **засобу технічної розвідки**. Хорошко В.О. та Чекатков А.О. вважають, що крім вищеперерахованих компонентів, до ТКВІ слід також включити **завади та шуми, що заважають передаванню сигналу** [6, с. 107], однак конкретного визначення ТКВІ, з урахуванням даного застереження автори у своїй роботі, на жаль, не надали. Російські фахівці Бузов Г.О., Калінін С.В. та Кондратьєв А.В. [10] пропонують під технічними каналами витоку інформації розуміти сукупність джерела інформації, лінії зв'язку (фізичного середовища), якою розповсюджується інформаційний сигнал, шумів, що заважають його передаванню в лінії зв'язку, та технічних засобів перехоплення інформації. Авторське бачення є у даному випадку достатньо обґрунтованим, однак деякі моменти мають бути уточнені з урахуванням положень, викладених нами вище. Тому у своєму дослідженні ми

будемо користуватися власним формалізованим визначенням, що поєднує у собі обидва підходи: ***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, як уже зазначалося вище, технічні канали витоку інформації, на думку фахівців у галузі ТЗІ, є одним із **способів несанкціонованого доступу до інформації**. Такої думки притримуються Домарев В.В. [5], Хорошко В.О. та Чекатков А.О. [6], Ярочкін В.І. [7] 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 А.Ю. Ільницького, який у дослідженні [11] звертає увагу на той факт, що канали несанкціонованого доступу законодавець у документі [8] визначив окремою групою. А.Ю. Ільницький пропонує 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 автор зауважує, що загрози несанкціонованого доступу, на думку західних фахівців, посідають пріоритетніше місце і, відповідно, досить часто використовуються як єдиний показник захищеності інформації в цілому, а отже потенційним каналам несанкціонованого впливу не приділяється належна увага [11, с. 16].

В.О. Хорошко та А.О. Чекатков [6] 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 [6, с. 252], хоча і відмічається, що можливості сучасних вірусів значно ширші і окремі з їхніх представників призначені саме для отримання інформації. Російські фахівці Бузов Г.О., Калінін С.В. та Кондратьєв А.В. питання несанкціонованого впливу на інформацію (знищення, блокування тощо) у роботі [10] не згадують взагалі, однак відмова в обслуговуванні автоматизованою системою вказана як один із методів несанкціонованого доступу (НСД), причому метою НСД у такому разі вказано часткове або повне виведення автоматизованої системи з ладу [10, с. 18]. З усіх запропонованих, на нашу думку, найбільш обґрунтованим є підхід А.Ю. Ільницького, який, по відношенню до предмета нашого дослідження, дозволяє зробити висновок, що поряд з **потенційними каналами несанкціонованого доступу,** існують **потенційні канали несанкціонованого впливу** щодо захищуваної інформації.

Таким чином, на основі узагальнення отриманих висновків, ми 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**.

Таким чином, на підставі отриманих результатів, ми пропонуємо виокремлювати два види ймовірних способів вчинення атак на інформацію (рис. 1.1): 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).

Рис. 1.1 Ймовірні способи вчинення атак на інформацію

Ми вважаємо, що критерієм для розподілу всієї сукупності зазначених каналів на технічні та інші канали мають стати визначення "технічного каналу витоку інформації" та "технічного каналу несанкціонованого впливу". Як уже зазначалося вище, під технічним каналом витоку інформації ми розуміємо сукупність носія інформації, середовища розповсюдження інформаційного сигналу, завад та шумів, що заважають передаванню сигналу та засобу технічної розвідки. Визначення технічного каналу несанкціонованого впливу до цього часу не використовувалося і є новелою. За аналогією з терміном "технічний канал витоку інформації", ми пропонуємо під ***технічним каналом несанкціонованого впливу*** *розуміти сукупність носія інформації, середовища його поширення, завад та шумів, що заважають передаванню сигналу та засобу несанкціонованого деструктивного впливу на них.*

Існування технічних каналів несанкціонованого впливу на інформацію, як підвиду каналів несанкціонованого впливу, є науково обґрунтованим і підтверджується аналізом значного масиву науково-практичних досліджень у галузі ТЗІ.

Так, наприклад, запропонований В.О. Хорошко та А.О. Чекатковим [6] перелік методів та засобів знищення комп'ютерної інформації, що включає **умисний силовий вплив мережею живлення**, **вірусні методи знищення інформації** та **деструктивні програмні засоби**, з урахуванням отриманих нами результатів, може бути уточнений: умисний силовий вплив мережею живлення слід включити до каналів несанкціонованого впливу (так як у даному випадку засіб несанкціонованого деструктивного впливу не впливає безпосередньо на середовище розповсюдження інформації), а вірусні методи знищення інформації разом з деструктивними програмними засобами слід віднести до технічних каналів несанкціонованого впливу на інформацію.

Тоді, якщо говорити про **ймовірні способи вчинення атак на інформацію в електронному вигляді, що реалізуються шляхом використання каналів несанкціонованого впливу**, на нашу думку, перелік може мати вигляд, вказаний на рис.1.2.

Атаки, що реалізуються шляхом використання каналів несанкціонованого впливу:

1. Фізичне знищення АС, або її складових (наприклад, організація пожежі у приміщенні, де знаходиться така АС).
2. Знищення магнітних, оптичних та електронних носіїв.
3. Знищення джерел живлення АС.
4. Умисний силовий вплив мережами живлення.
5. Знищення провідних комунікацій та комунікаційного обладнання комп'ютерних мереж.
6. Атаки, що реалізуються шляхом використання технічних каналів несанкціонованого впливу на інформацію:
– вірусний вплив;
– вплив шляхом використання деструктивних програмних засобів.

Рис. 1.2 Ймовірні способи вчинення атак на інформацію в електронному вигляді

Якщо говорити про **ймовірні способи вчинення атак на інформацію в електронному вигляді, що реалізуються шляхом використання каналів несанкціонованого доступу**, можна запропонувати наступний перелік, вказаний на рис. 1.3.

Атаки, що реалізуються шляхом використання каналів несанкціонованого доступу:
1. Викрадення окремих компонентів автоматизованої системи, або всієї АС.
2. Викрадення магнітних, оптичних та електронних носіїв інформації.
3. Підміна окремих компонентів автоматизованої системи на аналогічні.
4. Атаки, що реалізуються шляхом використання технічних каналів витоку інформації:
– отримання інформації за рахунок використання побічних електромагнітних випромінювань та наведень;
– отримання інформації з використанням комп'ютерної мережі (так звані "дистанційні атаки");
– отримання інформаційних сигналів з мережі електроживлення;
– отримання інформаційних сигналів з ланцюгів заземлення;
– отримання інформації з екрану монітора шляхом підглядування;
– отримання інформації з використанням закладних пристроїв (у тому числі – програмних).

Рис. 1.3 Ймовірні способи вчинення атак на інформацію в електронному вигляді

У своїй роботі до вищенаведених переліків ми включили найбільш розповсюджені способи вчинення атак, відповідно дані переліки є певною мірою формалізованими і у кожному окремому випадку можуть бути відкориговані, з урахуванням конкретних особливостей інформації, що підлягає захисту середовища в якому вона циркулює, та інших чинників.

Слід зауважити, що питання визначення повного переліку потенційних способів вчинення атак на ті чи інші категорії інформації є предметом окремого дослідження, що виходить за рамки даної роботи. Вивченням цього питання займалися зокрема Д. Мусієнко [12], [13]; А.М. Юрченко [14]; М.П. Нестеренко, В.В. Шорошев [15]; С.Л. Ємельянов, В.В. Носов [16]; О.В. Казарін [17] та інші.

У даній статті ми спробували узагальнити існуючі підходи до класифікації ймовірних способів вчинення атак на інформацію та на їх підставі розробити узагальнену класифікацію, яка б дозволила у процесі побудови системи технічного захисту інформації у кожному окремому випадку скласти повний перелік

характерних ймовірних способів вчинення атак на інформацію, що стало б вагомим на шляху формування концепції протидії комп'ютерній злочинності.

Ми вважаємо, що дане дослідження в світлі впровадження в Україні європейських та міжнародних стандартів інформаційної безпеки, актуалізації проблем протидії комп'ютерній злочинності сприятиме скорішому та більш якісному формуванню вітчизняних вимог із захисту інформації, які найбільш повно відповідатимуть національним пріоритетам та вимогам сьогодення, передусім на магістральних напрямах боротьби з транснаціональною організованою злочинністю. Результати дослідження можуть бути корисними як науковцям, яуі проводять свої дослідження в галузі національної безпеки та ТЗІ, так і практичним працівникам. Зокрема, запропонована класифікація має стати системоутворюючою у процесі дослідження всієї сукупності ймовірних способів вчинення атак на інформацію і може бути використана в процесі побудови систем ТЗІ, що призначені для захисту відкритої інформації та інформації з обмеженим доступом на загальнодержавному рівні та на рівні окремих установ, підприємств, організацій, під час оперативно-розшукових дій щодо встановлення осіб, які вчинили комп'ютерні злочини. У даному аспекті нерозривна єдність технічного захисту інформації з ОРД влучно підкреслюється в одному із фундаментальних досліджень проблем ОРД сучасності М.А. Погорецького, в якому, з-поміж іншого, зазначається, що ОРД виступає самостійною пізнавальною діяльністю, якій властиві особливі форми й засоби, що дозволяють пізнавати приховані, замасковані ознаки злочинної діяльності в умовах активної протидії осіб, які готують, вчиняють чи вчинили злочини [18].

Основними напрямами розвитку положень даного дослідження мають стати роботи щодо складання повних переліків ймовірних способів вчинення атак на кожну з категорій захищуваної інформації (інформація в електронному вигляді, у вигляді матеріальних носіїв чи мовна інформація).

Список використаних джерел

1. *Ліпкан В.А.* Теоретичні основи та елементи національної безпеки України: Монографія. – К.: Текст, 2003. – 600 с.

2. *Левицька М.Б.* Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: Дис. … канд. юрид. наук: 12.00.01 / Національна академія внутрішніх справ України – К., 2002. – 206 с.

3. *Бодрук О.С.* Системи національної та міжнародної безпеки в умовах формування нового світового порядку 1991–2001 роки: Дис. … д-ра. політ. наук: 21.01.01 / Нац. ін-т проблем міжнар. безпеки. – К., 2003. – 415 с.

4. *Гурковський В.І.* Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис. … канд. юрид. наук: 25.00.02 / Нац. акад. держ. управ. при Президентові України. – К., 2004. – 225 с.

5. *Домарев В.В.* Безопасность информационных технологий. Системный подход. – К.: ООО "ТИД "ДС", 2004. – 992 с.

6. *Хорошко В.А.,* Чекатков А.А. Методы и средства защиты информации / Под ред. Ю.С. Ковтанюка – К.: Издательство Юниор, 2003. – 504 с.

7. *Ярочкин В.И.* Предприниматель и безопасность. Часть I. – М.: "Экспертное бюро", 1994. – 64 с.

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

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

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

11. *Ільницький А.Ю.,* Саницький В.А., Шорошев В.В. та ін. Основи захисту інформації від несанкціонованого доступу: Наук. – метод. посібник – К.: Національна академія внутрішніх справ України, 2002. – 208 с.

12. *Мусиенко Д.* Защита акустической информации // Бизнес и безопасность. – 2005. – № 4. – С. 58–63.

13. *Мусиенко Д.* Защита компьютерных систем по цепям электропитания // Бизнес и безопасность. – 2005. – № 4. – С. 71–76.

14. *Юрченко А.М.* Технологии сотовой телефонной связи как объект защиты интеллектуальной собственности // Бизнес и безопасность. – 2004. – № 6. – С. 61–63.

15. *Нестеренко М.П.,* Шорошев В.В. Стільниковий телефон – новітнє джерело соціальних проблем та загроз // Бизнес и безопасность. – 2004. – № 5. – С. 64–66.

16. *Емельянов С.Л.,* Логвиненко Н.Ф., Марков С.И., Носов В.В. Технические методы защиты каналов утечки информации по электросети // Бизнес и безопасность. – 2000. – № 2. – С. 8–9.

17. *Казарин О.В.* Безопасность программного обеспечения компьютерных систем: Монография. – М.: МГУЛ, 2003. – 212 с.

18. *Погорецький М.А.* Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: Монографія. – Х.: Аріс, ЛТД, 2007. – 576 с.

The article is examined the main methods of realization attacks on the information, their classification which serve as one of the directions of counteraction computer crime is offered.

Стаття надійшла до редакції журналу19 грудня 2008 року.