УДК 004.491

Р.В. Грищук,
кандидат технічних наук

АТАКИ НА ІНФОРМАЦІЮ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

У статті наведено дані про атаки на інформацію в інформаційно-комунікаційних системах та розкрито особливості їх прояву.

Ключові слова: *атака, інформація, інформаційно-комунікаційна система.*

В статье приведены сведения об атаках на информацию в информационно-коммуникационных системах и раскрыта сущность их проявления.

Ключевые слова: *атака, информация, информационно-коммуникационная система.*

Attacks on the information in the information-communication systems are developed in the article and essence of their display is resulted.

Keywords: *attack, information, CIS.*

Упровадження у практику повсякденної діяльності державних структур комп'ютеризованих інформаційно-комунікаційних систем (ІКС) відкриває широкі перспективи з надання послуг із комунікацій та обробки інформаційних ресурсів між відповідними відомствами, організаціями та установами [1]. Водночас цілковита залежність державних структур від закордонних розробників складових частин ІКС, насамперед апаратного та програмного забезпечення відкриває для зловмисників шляхи для несанкціонованого доступу до інформації, що становить реальну загрозу безпеці інформації зокрема та захищеності системі в цілому [2]. Крім того, ймовірність реалізації відповідних загроз підвищується через широку доступність комп'ютерних технологій для всіх бажаючих. Тому проблема захисту ІКС від відповідних загроз та способів їх реалізації – атак, носить надзвичайно актуальний характер.

У рамках визначеної проблеми актуальною є задача розроблення ефективних комплексних систем захисту інформації ІКС [3], одним із етапів на шляху вирішення якої є визначення усього спектра зазначених атак на інформацію у відповідних системах.

Як показав аналіз останніх досліджень і публікацій [4–15], питанням дослідження атак на інформацію в ІКС приділено значну увагу фахівців з інформаційної безпеки. Але більшість із досліджених підходів різняться не тільки концептуально, але й категоріально. Це пов'язано з неусталеністю термінології таких категорій як інформація, атака, інформаційно-комунікаційна система тощо, що значно ускладнює питання систематизації зазначених досліджень.

Так, у роботах [6–9] розкрито сутність атак на інформацію в локальних та глобальних ІКС, в [5, 10, 14] – у середніх та великих інтегрованих систе-

мах, у [15] наведено приклади моделювання атак на інформацію та їх наслідків для системи. У роботі [13] подано узагальнену класифікацію ймовірних способів вчинення атак на інформацію в ІКС різної топологічної конфігурації. Подана класифікація в кожному окремому випадку дозволяє складати перелік ймовірних способів вчинення атак на інформацію, але не розкриває власне сутності цих атак. Таким чином, як випливає із проведеного аналізу, на сьогодні немає єдиного загальноприйнятного підходу до опису атак на інформацію в ІКС. Отже, спираючись на дослідження [4–9, 11, 12] та з огляду на результати [10,13], у рамках норм чинного законодавства України [3, 16 та ін.] актуальним залишається питання дослідження атак на інформацію в ІКС.

Метою статті є дослідження різновидів атак на інформацію в комп'ютеризованих ІКС, розкриття їх суності та наслідків для системи.

Відомо [13], що спосіб реалізації атаки на інформацію в ІКС у першу чергу залежить від її цінності та цілей, що їх намагається досягти зловмисник, а в другу – від форми її зберігання, обробки та передачі, а також способу доступу. Так, нормативно-правовою базою чинного законодавства України визначено, що інформація – це відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [16]. З огляду на це визначення, метою зловмисника може бути незаконне заволодіння інформацією засобами комп'ютерних технологій. Реалізувати на практиці цю мету супротивник може лише здійснивши атаку на інформацію. У такому разі як фізичне середовище для здійснення атак на інформацію противник використовуватиме різні фізичні поля (електричне, магнітне, акустичне, теплове тощо) [6, 10, 13], у рамках яких реалізуватиме процеси нападу на інформацію [15]. Визначена множина фізичних полів в сукупності становить канали несанкціонованого доступу та канали несанкціонованого впливу [13]. Із високим ступенем ймовірності з технічних каналів зловмисником використовуватимуться такі їх підвиди – технічні канали витоку інформації та технічні канали несанкціонованого впливу.

Атака на інформацію в ІКС з використанням каналів НСД передбачає використання таких технічних каналів [6, 10, 13]:

– радіоканалів (атака здійснюється за рахунок електромагнітного випромінювання та наведень у радіодіапазоні);

– електричних каналів (небезпечних напруг та струмів на різних елементах комунікацій, мереж електроживлення та з ланцюгів заземлення);

– акустичних каналів (розповсюдження звукових коливань у будь-якому звукопровідному матеріалі);

– оптичних каналів (електромагнітне випромінювання в інфрачервоній, видимій та ультрафіолетовій частині спектра);

– матеріально-речових каналів (атака на інформацію здійснюється шляхом викрадення окремих компонентів ІКС, паперових, фото- та магнітних носіїв, відходів тощо).

Окреме місце відводиться віддаленим та розподіленим атакам на інформацію з використанням комунікаційних каналів ІКС та атакам з використанням закладних програмних пристроїв.

Із використанням каналів несанкціонованого впливу супротивник може реалізувати такі атаки на інформацію в ІКС [6, 10, 13, 17, 18]:

– фізичне знищення ІКС або її елементів при реалізації зовнішніх загроз (навмисних пожеж, землетрусів, потопів тощо);

– фізичне знищення ІКС або її елементів при реалізації внутрішніх загроз (знищення магнітних, оптичних, елек-

тронних носіїв, джерел живлення обслуговуючим персоналом);

– умисний силовий вплив мережами живлення;

– фізичне знищення провідних комунікацій та комунікаційного обладнання комп'ютерних мереж.

Детальніше розглянемо різновид атак на інформацію, що здійснюються зловмисником з використанням комунікаційних каналів комп'ютерних мереж. Основними категоріями таких атак є [11]: атаки доступу; атаки модифікації; атаки на відмову в обслуговуванні; атаки на відмову від зобов'язань.

Метою атаки доступу є порушення конфіденційності інформації, що зберігається, обробляється та циркулює в ІКС. Існує два механізми реалізації атаки доступу. У першому випадку зловмисник аналізує файли шляхом їх послідовного перебору. Для реалізації такого механізму зловмисник повинен мати легальний доступ до ІКС, наприклад бути співробітником цієї організації або інсайдером [17], а система захисту інформації не повинна здійснювати додаткових запитів на аутентифікацію користувача, окрім ідентифікації його за IP-адресою. Така атака називається IP-спуфінг атакою. Виявлення IP-спуфінг атаки свідчить про підготовку зловмисника до інших видів атак, наприклад розподілених атак на відмову в обслуговуванні.

У другому випадку зловмисник здійснює атаку шляхом обходу системи захисту. Для цього в ІКС встановлюється мережевий аналізатор пакетів (sniffer), призначений для захоплення цільової інформації. Зазвичай сніфери налаштовуються на інформацію, що місить дані про паролі та ідентифікаційні дані користувачів. У такому разі мережева карта кінцевого вузла, на якому зберігається інформація, зловмисником переводиться в режим *promiscuous mode* – для дротових мереж або в режим *monitor mode* – для бездротових мереж. Після входження мережевої карти в режим *promiscuous mode (monitor mode* відповідно) сніфер відсилає інформацію зловмиснику на аналіз. Особливо даний вид атаки небезпечний для бездротових мереж, які слугують засобом комунікації ІКС, оскільки зловмисник може знаходитися в безпосередній близькості від безпроводових структур та здійснювати ряд нападів на інформацію, які були б неможливі у дротовій мережі.

В окремих випадках до атак доступу відносять атаки підслуховування *(eavesdropping)* та перехоплення *(interception)*. Перший із зазначених типів атаки здійснюється в глобальних ІКС і реалізується по виділених лініях, телефонних з'єднаннях та волоконно-оптичних лініях зв'язку. В ІКС, до структури яких включаються файлові сервери мережі Інтернет, зловмисник перетворює ім'я робочої станції на неправильну адресу. Тоді робоча станція через файловий сервер перенаправляє трафік з цільовою інформацією зловмиснику. Такими діями зловмисник виключає можливість перевірки доставки інформації адресату, а атака називається атакою *Man-in-the-Middle (MIM)*. Мета *MIM* атаки полягає у фальсифікації інформації, що передається, та отриманні доступу до інформаційних ресурсів ІКС, наприклад баз даних.

Атака модифікації здійснюється з метою неправомірної зміни інформації шляхом порушення її цілісності. На сьогодні відомо три види таких атак: заміни, додавання та знищення. Атака заміни передбачає заміну цільової інформації іншою, нецільовою. Атака додавання здійснюється з метою додавання нових, як правило, надлишкових даних. Атака знищення призначена для переміщення інформації від законного користувача до зловмисника з використанням спеціалізованого програмного забезпечення. Атаки модифікації можливі у випадку наявності вузьких (враз-

ливих) місць в ІКС. Такий вид атаки реалізується в два етапи. Перший етап передбачає перехоплення інформації, що передається, другий – внесення в неї змін перед відправкою до пункту призначення.

Характерний прояв атаки модифікації мають у фінансовій сфері [17, 18]. Наприклад, атака заміни може бути проявлена як факт зміни заробітної плати працівника установи; атака додавання проявляється як ненадходження платіжних засобів на рахунок платника; атака знищення призводить до анулювання запису про банківську операцію.

Атаки на відмову в обслуговуванні *DoS (Denial-of-service)* мають на меті блокування доступу до інформації легальних користувачів [8].

DDoS-атаки проводяться зазвичай із метою несанкціонованого заволодіння інформацією про номери кредитних карток, логінів та паролів від електронних гаманців та з метою отримання конфіденційної інформації. Інколи зловмисник намагається отримати право на адміністрування файловим сервером системи.

Їх сутність зводиться до наступного [15]:

– на атаковану робочу станцію в складі ІКС зловмисником посилається некоректний запит, призначений для зациклення процедур обробки, які врешті-решт призводять до зависання його операційної системи;

– перекриття смуги пропускання комутаційних каналів шляхом перевантаження трафіку небажаними та непотрібними пакетами або хибними повідомленнями про поточний стан мережевих ресурсів;

– надходження великої кількості фіктивних запитів від розподілених користувачів або програм на встановлення зв'язку з файловим сервером. Сукупність розподілених користувачів та шкідливого програмного забезпечення називається *Boot*-мережами, а відповідні атаки – *DDoS*-атаками *(Distributed DoS)*;

– перевантаження зловмисником обчислюваних ресурсів файлового серверу шляхом санкціонованих запитів на використання серверних програмних додатків, наприклад таких, як *PHP, Java, Python* тощо.

Крім того, результатом дії атак на відмову в обслуговуванні є зменшення цінності інформації, її знищення, викривлення або перенесення на інші робочі станції.

Однією з різновидності атаки на відмову є відмова доступу до додатків, яка проявляється як відмова в доступі до додатків в яких обробляється та зберігається інформація, або робочої станції на якій ці додатки виконуються. Результат дії такої атаки – заборона доступу до інформації легальному користувачеві.

DoS-атаки на відмову від обслуговування ІКС мають на меті виведення з ладу власне всієї системи. Як наслідок – уся інформація в системі стає недоступною.

Відмова на обслуговування комунікацій полягає у відмові засобів зв'язку ІКС. На фізичному рівні цей вид атаки може бути реалізованим механічним пошкодженням комутаційних каналів між робочою станцію та файловим сервером. Також цей вид атаки можливий при застосуванні сил і засобів радіоелектронної боротьби та неконтрольованої розсилки спаму поштовими серверами. Метою такої атаки є блокування доступу до інформації без порушення її цілісності.

Атака на відмову від зобов'язань спрямована на виключення можливості ідентифікації інформації шляхом дезінформування реальних подій або операцій. Серед відомих атак найбільше розповсюдження отримали такі її види: атака-маскарад; атака – заперечення події; *DoS*-атака проти Інтернету.

Атака-маскарад передбачає виконання дій в ІКС над інформацією під виглядом легального користувача. Як показує аналіз [11, 12], атака-маскарад відбувається в момент передачі інформації від одного користувача ІКС до іншого.

Атака – заперечення події призводить до відмови від факту здійснення операції.

DoS-атака проти Інтернету – це атака на сервери корінних імен Інтернету. Призначена для виведення з ладу серверів Інтернету, з метою відмови від обслуговування ІКС, топологія яких побудована на інтеграції відповідних робочих станцій ІКС та веб-серверів Інтернету. На сьогодні існує достатньо публікацій щодо досліджуваної атаки, наприклад [9].

Отже, як видно з приведеного переліку атак на інформацію в ІКС, їх кількість постійно зростає. Атаки постійно ускладнюються та інтелектуалізуються. Тому наведений перелік та аналіз атак на інформацію в ІКС може бути значно розширено й доповнено. Із наведених у статті прикладів зрозуміло, що успішні атаки на інформацію в першу чергу призводять до економічних та фінансових збитків для її власників.

Таким чином, прихованість атак на інформацію в ІКС, недосконалість чинної нормативно-правової бази, безкарність відкриває сьогодні зловмисникам доступ до цільової інформації, тим самим становлячи загрозу стабільному розвитку українського суспільства, а тому потребує розробки якісної та надійної комплексної системи захисту інформації. Перспективним напрямом подальших досліджень є дослідження атак на інформацію в бездротових ІКС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Маслянко П.П.* Інформаційно-комунікаційні системи та технології обробки інформаційних ресурсів / П.П. Маслянко, П.М. Ліссов // Науковий вісник Кременчуцького університету економіки, інформаційних технологій і управління. – Кременчук : КУЕІТУ, 2007. – № 1–2. – С. 164–168.

2. *Хорошко В.О.* Информационная безопасность Украины. Основные проблемы и перспективы / В.О. Хорошко // Захист інформації. – К. : ДУІКТ, 2008. – № 40 (спец. вип.). – С. 6–9.

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (зі змінами, внесеними згідно із Законом № 1180-VI від 19.03.2009) / Верховна Рада України. – К. : ВВР, 1994. – № 31. – Ст. 286.

4. *Хорошко В.А.* Категории и виды информационных воздействий / В.А. Хорошко, В.С. Чередниченко // Захист інформації. – К. : ДУІКТ, 2007. – № 4(36). – С. 31–36.

5. *Мороз Е.С.* Методы противодействия сетевым атакам / Е.С. Мороз, В.О. Хорошко, Е.Е. Смычков // Збірник наукових праць. – Севастополь, СНУЯЕтаП, 2007. – Т. 18 (№ 5). – С. 180–187.

6. *Ленков С.В.* Методы и средства защиты информации : моногр. [в 2-х т.] Т. 1. Несанкционированное получение информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – 464 с.

7. *Кожиевский С.Р.* Пассивные методы борьбы с утечкой информации по техническим каналам в персональных компьютерах / С.Р. Кожиевский, Г.Т. Солдатенко // Захист інформації. – К. : ДУІКТ, 2006. – № 2. – С. 60–67.

8. *Андон П.І.* Атаки на відмову в мережі Інтернет : опис проблеми та підходів до її вирішення / П.І. Андон, О.П. Ігнатенко. – К. : Ін-т ПС, 2008. – 52 с. – (Препринт / НАН України, Ін-т програмних систем).

9. *Biskup J.* Security in computing systems: challenges, approaches and solutions: monogr. / J. Biskup. – Berlin : Springer, 2009. – 694 p.

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

11. Категорії атак [Електронний ресурс]. – Режим доступу : http ://it-sektor.ru/Kategorii-atak.html.

12. Основные виды и источники атак на информации [Електронний ресурс]. – 2011. – Режим доступа : http ://www.w3.org/TR/xhtml1/DTD/xhtml1- strict.dtd.

13. *Антонюк П.Є.* Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності / П.Є. Антонюк // [Електронний ресурс]. – 2011. – Режим доступу : http://www.nbuv.gov.ua/ portal/S oc_Gum/bozk/19text/g 19_2 7 .htm.

14. *Грайворонський М.В.* Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новиков ; за заг. ред. академіка НАН України М.З. Згуровського. – К. : BHV, 2009. – 608 с.

15. *Грищук Р.В.* Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : моногр. / Р.В. Грищук. – Житомир : Рута, 2010. – 280 с.

16. Про інформацію : Закон України від 02.10.1992 № 2657-XII / Верховна Рада України. – Офіц. вид. – К. : Парлам. вид-во, 1992. – № 48. – 650 с.

17. *Кавун С.В.* Инсайдер – угроза экономической безопасности / С.В. Кавун, И.В. Сорбат // Управління розвитком. – Х. : ХНЕУ, 2008. – № 6. – С. 7–11.

18. *Браіловський М.М.* Захист інформації в банківській діяльності / М.М. Браіловський, Г.П. Лазарев, В.О. Хорошко. – 2-е вид. – К. : Поліграф-Консалтінг, 2004. – 216 с.

Отримано 20.04.2011