

ПОСТАНОВКА ЗАВДАННЯ РОЗПОДІЛУ СИЛ І ЗАСОБІВ ДЛЯ ДОБУВАННЯ ІНФОРМАЦІЇ З КОМП'ЮТЕРНИХ МЕРЕЖ

Запропоновано загальну постановку завдання розподілу сил і засобів для добування інформації з комп'ютерних мереж.

Постановка проблеми. На сьогоднішній день комп'ютерні мережі (КМ) стали невід'ємною частиною інформаційного простору [1]. Їх користувачі за лічені миті одержують доступ до інформації, наявної на серверах різних країн, оминаючи кордони, цензуру й інші бар'єри. Так, Інтернет поєднує в єдине ціле тисячі комп'ютерних мереж усіх континентів. Підрахувати кількість документів, які є ресурсами Інтернету і розміщені на його серверах, практично не можливо. За приблизними оцінками [2], їх більше квадрильона (10^{12}), ця кількість подвоюється кожні три роки.

На даний час відповідні підрозділи з добування інформації (ДІ) з КМ існують не тільки в спецслужбах іноземних держав, але й структурах спеціальних операцій їх збройних сил. Сферою їх діяльності є розвідка ресурсів комп'ютерних мереж, організація каналів зв'язку з агентурою, проведення акцій інформаційного впливу, а також збір й аналіз інформації, що викликає інтерес з погляду інформаційної безпеки.

Огляд останніх досліджень і публікацій. У відомих авторах джерелах, наприклад [2 – 6], містяться відомості з окремих складових процесу добування інформації з КМ. Так, у [2] розкриваються способи отримання відомостей з ресурсів КМ. У [3] наводяться алгоритми пошуку, добування інформації та доступу до об'єктів. У [4] розглядаються основні точки уразливості інформаційних систем на базі комп'ютерних мереж. У [5 – 6] надаються пропозиції щодо кількісних та якісних характеристик засобів добування інформації. Однак авторами не знайдено джерел з описанням ефективного розподілу сил та засобів на добування інформації. На сьогоднішній день дане завдання вирішується поки що емпірично. Тому актуальним є питання забезпечення особи, яка приймає рішення про застосування сил і засобів добування інформації, рекомендаціями щодо доцільного та, якщо можливо, оптимального розподілу їх наявного ресурсу для вирішення поставлених завдань.

Формулювання завдання досліджень. Метою роботи є постановка та формалізація задачі з розподілу сил і засобів добування інформації з КМ для забезпечення своєчасного та якісного виконання завдань спеціальними частинами і підрозділами Збройних Сил (ЗС) України.

Виклад основного матеріалу. Для досягнення поставленої мети розглянемо структуру КМ. Вона складається з об'єднаних між собою за допомогою різного мережного обладнання інтернет-мереж та окремих хостів (рис. 1) [7].

Добування інформації передбачає два взаємопов'язаних процеси: пошук, під яким будемо розуміти виявлення джерел відомостей (ДВ) та їх оцінку щодо релевантності, та спостереження, яке передбачає отримання даних з виявлених джерел відомостей.

Джерелом відомостей є ресурси хостів комп'ютерних мереж та різноманітних сервісів, таких як WWW, FTP, E-mail, SQL тощо [7]. Під ресурсами розумітимемо гіпертекстові документи, файли з файлових архівів, повідомлення електронної пошти, записи баз даних, таблиці маршрутизації.

Для добування інформації у спеціальних підрозділах і частинах ЗС України доцільно розгорнути пункти ДІ, являють собою сукупність автоматизованих робочих місць (АРМ) на базі ПЕОМ, що є вузлами КМ, зі встановленим загальносистемним та спеціалізованим програмним забезпеченням.

АРМ, за яким підготовлений персонал виконує завдання з ДІ, розглядається як пост ДІ.

Враховуючи необхідність окремого вирішення завдань пошуку і спостереження [4], пропонується розділити усі пости ДІ на дві відповідні функціональні групи (рис. 1).

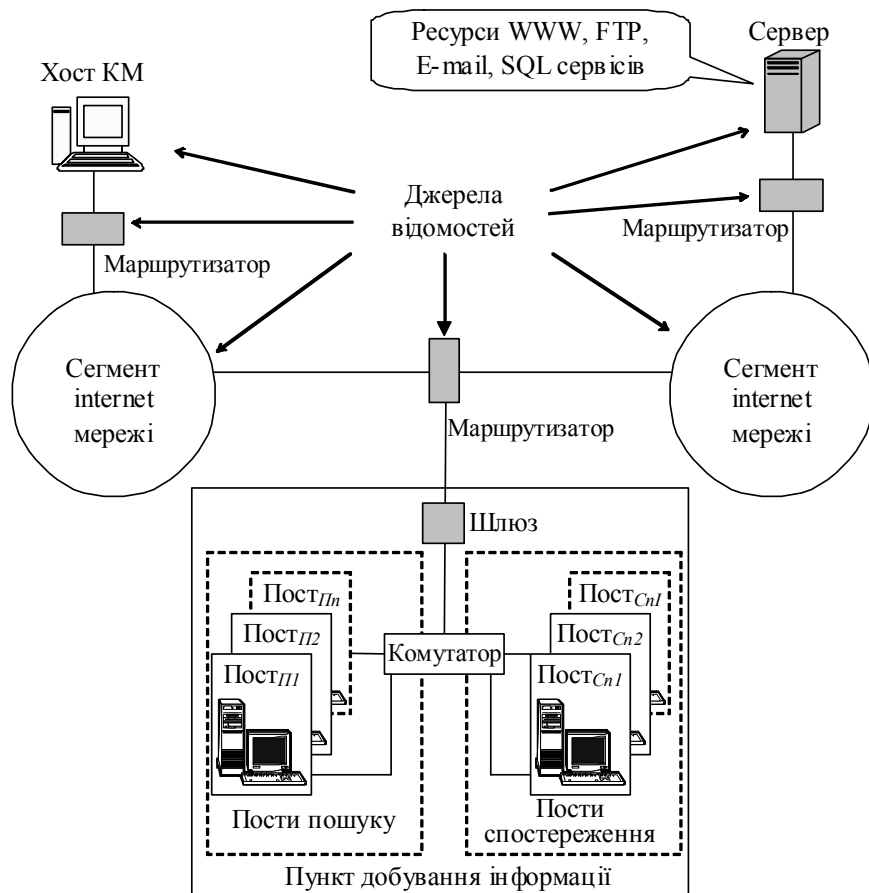


Рис. 1. Структура КМ та місце пункту ДІ в ній

Під постом пошуку будемо розуміти пост ДІ, на якому виконуються завдання з визначення доменного імені, IP-адреси, власника, користувачів, програмного забезпечення ДВ та їх оцінювання.

На посту спостереження виконуються завдання з доступу до виявлених постами пошуку ресурсів, їх перегляду, попереднього аналізу, накопичення та обробки для отримання необхідних даних про об'єкти.

Задача розподілу наявного ресурсу сил і засобів для вирішення завдань добування інформації у загальній постановці може бути сформульована таким чином.

Кількість постів пошуку $N_{П}$ та спостереження $N_{Сн}$ пов'язана із загальною кількістю постів пункту ДІ $N_{пост}$:

$$N_{пост} = N_{\Pi} + N_{Cn}. \quad (1)$$

За відсутності інформації про наявність у КМ ДВ про об'єкт усім постам пункту ДІ буде поставлено завдання з їх пошуку, спостереження за ними забезпечить виконання відповідних завдань. Згідно з виразом (1) для даного етапу співвідношення постів буде таким:

$$N_{пост} = N_{\Pi}^{max} + N_{Cn}^0, \quad (2)$$

де N_{Π}^{max} – це максимальна кількість АРМ, що може бути виділена для пошуку;

N_{Cn}^0 – це мінімально допустима кількість постів, виділених на спостереження раніше виявлених ДВ.

Будемо вважати, що пости пошуку і спостереження є однаковими щодо складу і можливостей технічних засобів, а персонал, який їх обслуговує, здатний за рівнем своєї підготовки виконувати завдання як пошуку, так і спостереження.

У процесі ведення пошуку кількість постів пошуку буде зменшуватись за рахунок постановки їм завдань зі спостереження виявлених ДВ, відповідно, кількість постів спостереження збільшуватиметься. Скорочення кількості перших і збільшення кількості других буде відбуватися доти, доки подальше скорочення постів пошуку стане неприпустимим. Для даного етапу співвідношення постів буде таким:

$$N_{пост} = N_{\Pi}^0 + N_{Cn}, \quad (3)$$

де N_{Π}^0 – кількість постів пошуку, мінімально необхідна для виявлення нових ДВ.

Розв'язати задачу розподілу сил і засобів для добування інформації пропонується шляхом складання планів пошуку та спостереження, необхідність складання яких викликана тим, що виявлення різних типів ДВ із сегментів інтернет-мереж та окремих хостів потребує різних затрат часу.

Під планом пошуку D_{Π} будемо розуміти вектор призначень на кожний p -й пост пошуку певної кількості ДВ R_p з можливих R :

$$D_{\Pi} = \{C_{\Pi 1}, R_1; \dots; C_{\Pi p}, R_p; \dots; C_{\Pi n}, R_n\}; \quad (4)$$

$$\sum_{p=1}^n R_p = R; \quad \sum_{p=1}^n C_{\Pi p} \leq N_{\Pi}; \quad 0 \leq R_p \leq R; \quad C_{\Pi p} = \overline{0,1},$$

де $C_{\Pi p}$ – кількість постів, які виділені для пошуку серед визначеної кількості ДВ.

Як зазначалося, пошук здійснюється постійно. Це призводить до того, що список знайдених ДВ буде безперервно поповнюватись. Тому завжди буде мати місце альтернатива – або відмовитись від спостереження ДВ, викритого раніше, або не призначати на спостереження щойно виявлене ДВ. Таку альтернативу повинен враховувати план спостереження.

Під планом спостереження D_{Cn} будемо розуміти вектор призначень кількості постів на спостереження кожного ДВ з множини знайдених I :

$$D_{Cn} = \{C_{Cn1}, \dots, C_{Cni}, \dots, C_{CnI}\}, \quad (5)$$

$$\sum_{i=1}^I C_{Cni} \leq N_{Cn}, \quad C_{Cni} \geq 0,$$

де C_{Cni} – кількість постів, що виділяються на спостереження ресурсів i -го ДВ.

Таким чином, завдання на добування інформації з комп'ютерних мереж для поста ДІ ставиться у вигляді загального плану добування інформації $D_{ДІ}$, який являє собою сукупність планів пошуку та спостереження:

$$D_{дл} \in [D_{пл}, D_{сн}]. \quad (6)$$

Серед усіх можливих варіантів плану ДІ необхідно обирати той, який забезпечить повноту та швидкість виконання завдання з добування інформації.

Висновки. Пропонується з наявних сил і засобів створити пункт добування інформації, у якому передбачити пости пошуку та пости спостереження для забезпечення своєчасного та якісного виконання завдань спеціальними частинами і підрозділами ЗС України. Для ефективного виконання завдання з добування інформації для пункту ДІ необхідно розробити план добування інформації, згідно з яким проводити розподіл сил та засобів. Таким чином, можливо виконати розподіл наявних сил та засобів на добування інформації з КМ.

Подальші дослідження з даної теми передбачається продовжити в напрямках: визначення об'єктів, про які здійснюється добування інформації; визначення форм, способів та методів добування інформації; вибір та опис критеріїв оптимальності плану ДІ; розрахунок оптимального плану ДІ.

СПИСОК ЛІТЕРАТУРИ

1. Нарис теорії і практики інформаційно-психологічних операцій : навч. посіб. для курсантів і слухачів / [Дзюба М. Т., Жарков Я. М., Ольховой І. О., Онищук М. І.]. – К., 2005. – С. 14 – 21.
2. Доронин А. В. Бизнес-разведка / А. В. Доронин. – К. : Ваклер, 2000. – 564 с.
3. Мак-Клар Стюарт. Секреты хакеров. Безопасность сетей – готовые решения / Мак-Клар Стюарт, Скембрей Джоел, Курц Джордж; пер. с англ. – М. : „Вильямс”, 2001. – 656 с.: ил.
4. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки / Ю. К. Меньшаков. – М. : РГГУ, 2002. – 399 с.
5. Дудихин В. В. Конкурентная разведка в Интернет / В. В. Дудихин, О. В. Дудихина. – [2-е изд., испр. и доп.]. – М. : ООО „Издательство АСТ”, издательство „НТ Пресс”, 2004. – 229 с.
6. Разведка по открытым источникам [Электронный ресурс]. – Режим доступа : <http://www.onlineci.ru/oci-in-02.htm>.
7. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб : Питер, 2001. – 672 с.: ил.

Подано 27.11.09

В. И. Шестаков, С. М. Гудзь

ПОСТАНОВКА ЗАДАЧИ РАСПРЕДЕЛЕНИЯ СИЛ И СРЕДСТВ ДЛЯ ДОБЫВАНИЯ ИНФОРМАЦИИ ИЗ КОМПЬЮТЕРНЫХ СЕТЕЙ

Предлагается рассмотреть общую постановку задачи расчета сил и средств добывания информации из компьютерных сетей.

V. I. Shestakov, S. M. Gudz

THE TASK RAISING OF DISTRIBUTION FORCES AND FACILITIES FOR GETTING INFORMATION FROM COMPUTER NETWORKS

It is suggested the general task of distribution of forces and facilities for getting information from computer networks.