УДК 623.618:355.40

С.О. Сідченко, В.В. Бєлімов, К.І. Хударковський

Харківський університет Повітряних Сил ім. І. Кожедуба

МОЖЛИВА ОРГАНІЗАЦІЙНА СТРУКТУРА ПІДРОЗДІЛУ РОЗВІДКИ В КІБЕРНЕТИЧНОМУ ПРОСТОРІ

У статті розглянутий можливий варіант структури підрозділу "віртуальної" розвідки в кібернетичному (телекомунікаційному, віртуальному) просторі.

"віртуальна" розвідка, кіберрозвідка, кібернетичний простір

Вступ

Постановка проблеми. Останнім часом провідними державами світу проводяться заходи щодо створення підрозділів, здатних вести розвідку в кібернетичному просторі в умовах інформаційної протидії. Так, пентагонівський проект "Бойові системи майбутнього" припускає досягнення збройни-

ми силами США до 2010 року повної інформаційної переваги над будь-яким супротивником. Їхня концепція "мережної війни" (network-centric warfare) покладена в основу програми військового будівництва в США до 2010 року ("Joint Vision 2010"). Для її ведення створюється нова глобальна інформаційна мережа Пентагона (проект Defense Information Grid).

Разом з тим, в Америці (як і в інших країнах-виробниках засобів телекомунікації) вже давно прийнятий федеральний закон про те, що всі приватні компанії, що спеціалізуються в області телекомунікації, зобов'язані випускати обладнання, яке оснащене стандартизованими пристроями для підключення спецзасобів для знімання і запису інформації. Так, у програмне забезпечення вбудовуються "дірижучки" для одержання доступу до конфіденційної інформації. Наприклад, програмне забезпечення фірми Netscape (програма SmartDownload) дозволяло зчитувати конфіденційну інформацію з персонального комп'ютера без відома користувача.

Аналіз літератури. Загальна характеристика форм і способів ведення інформаційної війни (і її складової війни в кібернетичному просторі), напрямків її розвитку на сучасному етапі розглянута в роботах Толубко В.Б., Рося А.О., Жука С.Я., Руснака І.С., Фоміна В.А., Гриняєва С.М. і ін.

Основи обробки розвідувальної інформації наведені у [1]. Технічні системи і засоби розвідки, їх класифікація, порядок оцінки дальності радіотехнічної і радіолокаційної розвідок представлені в [2].

У [3, 4] проведена систематизація й аналіз розрізнених відомостей про види і засоби застосування інформаційної зброї при проведенні інформаційних наступальних і оборонних операцій.

У [5] розглянуті основні характеристики (дальність, точність і час) розвідки інформації за допомогою різних видів програмно-математичного впливу в кібернетичному (телекомунікаційному, віртуальному) просторі.

Разом з тим, структура підрозділів "кіберрозвідки" не розглядалася.

Мета статті. Навести можливий варіант структури підрозділу розвідки в кібернетичному (телекомунікаційному, віртуальному) просторі.

Виклад основного матеріалу

На думку світових країн-лідерів, війна в кібернетичному просторі повинна бути прирівняна до воєнних операцій на землі, у небі і на морі, а вторгнення в національний кібернетичний простір є настільки ж серйозним, як порушення державного суверенітету у реальному світі [6].

У газеті "Народна Армія сьогодні", що є офіційним органом Міністерства оборони Китаю, також говориться: "Китаю необхідно перейти в наступ на кібернетичному фронті, для чого потрібно розвивати програмне забезпечення й Інтернет-технології для проведення атак і оборонних операцій у мережі". Це стосується програмного забезпечення для глушіння і дезінформації, перехоплення управління, а також технології спостереження за мережею, злому кодів, викрадення даних, "замітання слідів" й ін.

За інформацією Washington Post, Пентагон давно розглядає китайські технології "електронної війни" як реальну загрозу.

При цьому Агентство національної безпеки США розробило автоматизовану систему перехоплення електросигналів "Ешелон" [7].

Система основана на орбітальному угрупованні космічних апаратів радіоелектронної розвідки супутників системи Intelsat (120 космічних супутників і різних станцій спостереження в різних куточках земної кулі), більш 20-и наземних станцій перехоплення повідомлень, розташованих у США, Новій Зеландії, Австралії, Гонконгу, Великобританії, Канаді.

Система здатна перехопити й обробити до 3 мільярдів повідомлень у годину. Вона може копіювати, розшифровувати і за допомогою спеціальних комп'ютерних програм переводити на англійську мову будь-яку інформацію, отриману з будь-якої країни: телефонні розмови, факсимільні і телексні повідомлення, електронну пошту й ін. Система сама розпізнає, у якому випадку яку програму підключити до роботи.

За ключовими словами відбирається тільки те, що стосується економіки, політики, збройних сил, технологічних розробок, терористичних організацій і іншого. Потім дані сортуються і передаються аналітикам і оперативним відділам в Агентство національної безпеки США.

Виходячи з приведених прикладів, можна зробити висновок, що "кіберпідрозділи", швидше за все, стануть окремим родом військ, що будуть взаємодіяти з іншими військами для успішного застосування на новому, об'єднаному театрі воєнних дій, куди будуть входити суша, море, небо і кібернетичний простір.

Для успішного ведення бойових дій будь-якого рівня необхідне безперервне надходження у розпорядження командирів і штабів інформації про можливості супротивника в масштабі часу, близькому до реального. При цьому знання потенційних бойових можливостей супротивника необхідно, щоб уникнути його раптових дій, а достовірні дані про супротивника необхідні для визначення його намірів. Це збільшує роль підрозділів розвідки в кібернетичному просторі.

Найбільша ефективність бойових дій у кібернетичному просторі досягається в тому випадку, коли вони є складовим елементом проведених операцій, а не доповненням до них. Через обмежену кількість

спеціального радіоелектронного обладнання потрібне ретельне планування бойових дій у кібернетичному просторі для того, щоб оптимально визначати конкретний комплекс сил і засобів для забезпечення максимальної ефективності розв'язуваних задач.

Під "віртуальною" розвідкою будемо розуміти комплекс заходів щодо добування, обробки й аналізу розвідувальної інформації в кібернетичному (телекомунікаційному, віртуальному) просторі за допомогою різних видів програмно-математичного впливу.

Нами пропонується варіант організаційної структури підрозділу "віртуальної" розвідки (кіберрозвідки), що призначений для ведення розвідки в кібернетичному (телекомунікаційному) просторі і контролю за роботою своїх телекомунікаційних систем і підсистем їхнього захисту (рис. 1).

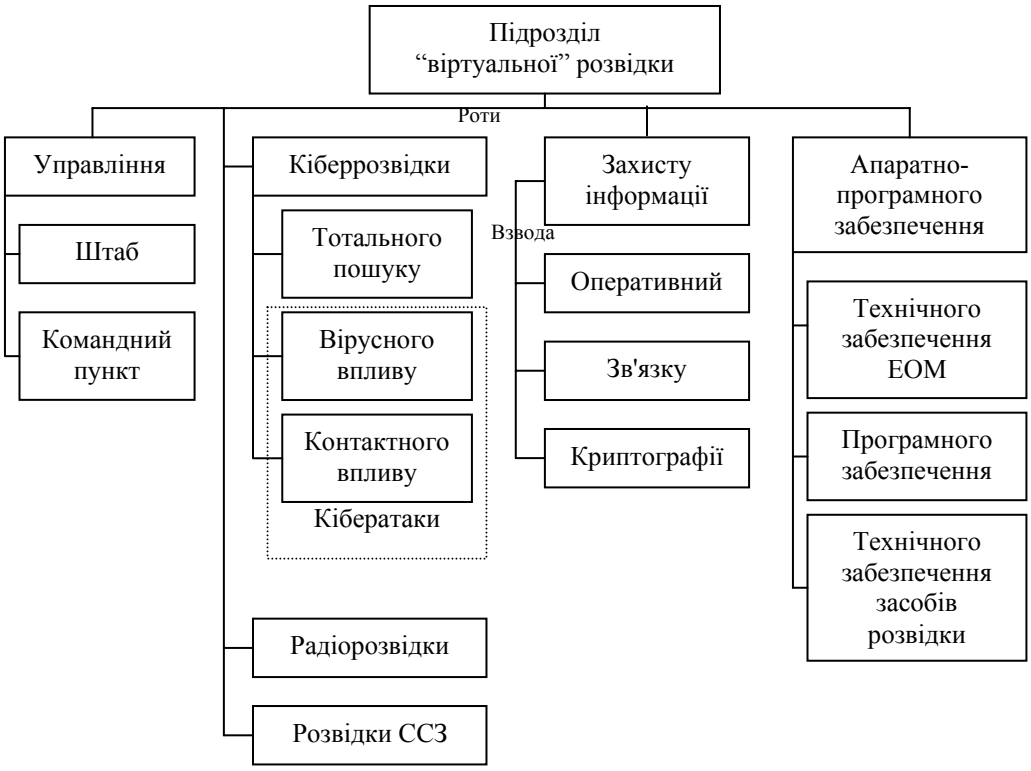

Рис. 1. Варіант організаційної структури підрозділу "віртуальної" розвідки в кібернетичному просторі

Надалі ці підрозділи, як і сам вид розвідки, можуть носити різну назву: кіберрозвідки, "віртуальної" розвідки, спеціальної розвідки й ін.

Управління складається зі штабу і командного пункту.

Штаб призначений для централізованого управління штатними (і додатковими) силами і засобами розвідки.

Командний пункт призначений для збору, аналізу й обробки розвідувальної інформації, управління силами і засобами розвідки, забезпечення безпеки і проведення заходів щодо захисту.

Рота кіберрозвідки призначена для ведення кібернетичної розвідки в телекомунікаційних системах. Складається з управління і трьох взводів: тотального пошуку, вірусного впливу, контактного впливу.

Управління призначене для організації взаємодії між підрозділами роти кіберрозвідки.

Взвод тотального пошуку призначений для віддаленого пошуку доступної інформації в телекомунікаційній системі (сканування телекомунікаційної системи, наприклад, Internet).

Взвод вірусного впливу призначений для виявлення, створення і впливу вірусами, хробаками, троянськими конями і логічними бомбами на програмні засоби й інформацію серверів-джерел інформації.

Взвод контактного впливу призначений для здійснення віддалених атак на інформаційні об'єкти (сервери-джерела інформації) телекомунікаційної системи.

Рота радіорозвідки призначена для ведення радіорозвідки систем передачі інформації короткохвильових, ультракороткохвильових, радіорелейних і тропосферних ліній зв'язку.

Рота розвідки систем супутникового зв'язку (ССЗ) призначена для ведення розвідки супутникових систем передачі інформації.

Рота захисту інформації проводить контркіберрозвідку, контроль виконання вимог прихованого управління військами, безпеки зв'язку і захищеності телекомунікаційних систем підрозділів кібер-

розвідки.

Оперативний взвод проводить контррозвідку, допити військовополонених і вплив на телекомунікаційні системи методами "соціальної інженерії".

Взвод зв'язку призначений для організації зв'язку між підрозділами і підключення до зовнішніх відкритих телекомунікаційних систем.

Взвод криптографії призначений для закриття (відкриття) інформації при передачі її по каналах зв'язку і розшифровки перехоплених закритих даних.

Рота апаратно-програмного забезпечення призначена для технічного і програмного забезпечення апаратури розвідки. Складається з розрахунків для технічного і програмного забезпечення.

Обслуга технічного забезпечення ЕОМ призначена для проведення обслуговування і ремонту апаратури засобів телекомунікації. На практиці його функції збігаються з функціями стандартного сервісного центра.

Обслуга програмного забезпечення призначена для розробки і створення математичного і програмного забезпечення засобів розвідки.

Обслуга технічного забезпечення засобів розвідки призначена для проведення обслуговування і ремонту апаратури розвідки.

Для ведення розвідки в кібернетичному просторі може бути використана інформаційна зброя впливу на програмно-математичне забезпечення, мережі і телекомунікаційні засоби обміну даними автоматизованих систем управління і семантичного впливу на інформацію [3].

Основними властивостями інформаційної зброї, що може бути застосована для розвідки інформації в кібернетичному просторі, є:

– наявність "інформаційного розвідника" (наприклад, деструктивна частина програми – вірусу збирача паролів);

– наявність засобів управління процесом розвідки елементів автоматизованих систем управління "інформаційними розвідниками" (програмне забезпечення, що веде розвідку протоколів обміну даними, паролів, параметрів операційних систем, засобів радіо- і радіотехнічної розвідки);

– наявність засобів доставки "інформаційного розвідника";

– висока скритність організації впливу;

– багатоваріантність форм програмно-апаратної реалізації;

– широкий діапазон дальностей впливу (від десятків до сотень тисяч кілометрів);

– висока швидкість доставки;

– комплексність впливу;

– універсальність;

– розсереджуваність;

– економічність;

– воно легко маскується під універсальне програмне забезпечення і засоби захисту;

– можливість діяти анонімно.

Висновки

Запропоновано варіант організаційної структури підрозділу "віртуальної" розвідки в кібернетичному просторі. Він є умовним і призначений для розгляду й обговорення можливості його гіпотетичного існування і функціонування.

Подальші напрямки розвитку. Надалі планується розглянути структуру комплексу програмно-апаратних засобів, необхідних для ведення розвідки в кібернетичному просторі, і різні варіанти застосування підрозділу "віртуальної" (кібернетичної) розвідки.

Список літератури

1. Кудрявцев А.М. Обработка разведывательной информации. – Л.: ВАС, 1989. – 332 с.

2. Основи радіоелектронної боротьби в радіотехнічних військах. Конспект лекцій / І.С. Добринін, О.М. Бовкун, В.І. Писаревський, А.В. Снігуров, В.П. Фінаєв. – Х.:ООО "Контур", 2006. – 108 с.

3. Шолохов С.Н., Сидченко С.А. Информационное оружие – новый класс вооружения для дезорганизации автоматизированных систем управления войсками и оружием при проведении информационных наступательных операций // Сборник научных трудов ХВУ. – Х.: ХВУ, 2002. – № 1 (39). – С. 10-14.

4. Сидченко С.А., Хударковский К.И., Петров В.Л. Информационное оружие защиты как новый класс вооружения при проведении информационных оборонительных операций // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 11 (39). – С. 163-169.

5. Сидченко С.А., Петров В.Л., Белимов В.В., Залкин С.В. Основные характеристики разведки информации в кибернетическом пространстве // Радіоелектронні і комп'ютерні системи. – Х.: ХНАУ "ХАІ". – 2006. – Вип. 3 (15). – С. 90-95.

6. Горицкий В.М. Проблемы информационной безопасности в условиях развития информационного общества // Материалы третьего Международного Форума "Технологии безопасности и бизнес". Заседание секции "Информационная безопасность сетей связи в открытом пространстве" [Електрон. ресурс]. – Режим доступа: http://www.diprozvyazok.kiev.ua/?id=33&lang=ru.

7. Система перехвата радиосигналов "Эшелон". Сайт агентства национальной безопасности (National Security Agency) [Електрон. ресурс]. – Режим доступа: http://www.patriotica.ru/books/pyh_usa/p05.html.

Надійшла до редколегії 18.08.2006

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.