УДК 355.415.7:[355.405.1]

І.О. Ляшенко, Р.К. Мурасов, О.В. Поплінський

Національний університет оборони України, Київ

ПРОГНОЗУВАННЯ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИМ СИСТЕМАМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Запропоновано підхід щодо прогнозування реалізації загроз живучості інформаційно-управляючих систем спеціального призначення на підставі класифікації та моделі прогнозування реалізації даних загроз.

Ключові слова: інформаційно-управляючі системи, загрози, збитки, імовірність реалізації, живучість

Предложен поход к прогнозированию возможности реализации угроз живучести информационно-управляющим системам специального назначения с помощью классификации и модели прогнозирования.

Ключевые слова: информационно-управляющие системы, угрозы, убытки, вероятность реализации, живучесть

A hike is offered to prognostication of marketability of threats of vitality to the informatively-managing systems of the special setting by means of classification and model of prognostication.

Keywords: information-control systems, threat, losses, the probability of realization, survivability

Постановка проблеми

Бурхливе впровадження інформаційних технологій практично у всі сфери діяльності людини на сьогодні – об'єктивна реальність. Процес інформатизації триває на всіх рівнях управління, в результаті чого автоматизовані робочі місця (АРМ) об'єднуються в локальні мережі, локальні мережі – в корпоративні або в регіональні, а останні – в локальні з можливим підключенням до всесвітньої мережі Інтернет.

Внаслідок розподілення мереж в просторі, недосконалості програмної та апаратної компонент, а також халатності та недбалості персоналу існує досить реальна загроза інформаційній безпеці – особливо інформаційно-управляючим системам спеціального призначення як системам, які містять значний обсяг цінної конфіденційної інформації.

Аналіз останніх публікацій

Питаннями аналізу розробки та застосування математичних моделей процесів функціонування системи управління на сьогодні приділяється значна увага [1-5].

Однак, в даних джерелах головна увага приділяється автоматизації основних процесів управління з метою забезпечення обґрунтованості та оперативності управління. При цьому живучості систем управління, як однієї з найважливіших вимог до управління належної уваги не приділено. Під живучістю інформаційних та інформаційно-управляючих систем спеціального призначення розуміється властивість цих систем зберігати або швидко відновлювати свою боєздатність в умовах деструктивного впливу противника [6; 7].

Мета статті

Метою статті є класифікація та обґрунтування структури моделі можливих загроз живучості інформаційно-управляючих систем спеціального призначення.

Основний матеріал

Основними вимогами до управління є:

- висока постійна готовність систем управління до роботи;
- оперативність управління підрозділами;
- висока якість управління;
- стійкість управління.

Досягнення цих вимог повністю, або якнайбільше буде залежати від живучості інформаційно-управляючих систем спеціального призначення.

Тому для задоволення усіх наведених вимог до управління підрозділами необхідно особливу увагу привернути такому вирішальному напряму у справі

подальшого вдосконалення управління, як живучість інформаційно-управляючих систем.

З цією метою, насамперед, необхідно побудувати модель можливих загроз, яка буде містити в собі три складові: джерела загроз, методи реалізації загроз та об'єкти захисту.

Джерела загроз живучості можна розглядати як зовнішні і внутрішні, так і комбіновані (рис.1).

Наступною складовою моделі є методи, якими будуть реалізовуватись загрози.

Методи впливу розрізняють:

- за мотивацією (випадкові, навмисні);
- за характером впливу (конфіденційність, достовірність, цілісність та доступність);
- за ступенем автоматизації (мануальні, автоматизовані та автоматичні);
- за ініціалізацією (умовні та безумовні);
- за взаємодією з політикою безпеки (політичні та постполітичні);
- за інструментальними засобами (технічні, апаратні та програмні);
- за природою взаємодії (фізичні, логічні);
- за специфікою реалізації (фрагментовані – за принципом декомпозиції та поетапної реалізації; без замовчувань – для систем основаних на сигнатурних технологіях; приховані, пікібенгові – несанкціонований доступ до тимчасово неконтрольованого ресурсу; маскарадні – поведінка порушника подібна легальному джерелу; непрямі – через третю особу; соціотехнічні – соціальний інжиніринг; криптоаналітичні та неспецифічні – такі, що не мають вищенаведених особливостей);
- за реляційною ознакою (мономономні – з одного джерела по одному об'єкту, полімономні – з декількох джерел по одному об'єкту, монополічні – з одного джерела на декілька об'єктів, поліполічні – з декількох джерел на декілька об'єктів);
- за наявністю зворотнього зв'язку (зі зворотнім зв'язком або без);
- за ступенем складності (прості, складні та системні);
- за імовірністю виникнення (імовірна, малоімовірна та з великою імовірністю);
- за формою (кібероперації – легальні, тактичні, стратегічні та спеціальні; кібератаки);
- за направленістю результату (розширюючі – отримання більших повноважень щодо доступу; викривлюючі – прямі зміни в цільовому ресурсі; розповсюджуючі – отримання доступу до ресурсу та його розкриття; розкрадаючі – несанкціоноване використання ресурсу без нанесення збитку; перевантажуючі – завантаження ресурсу до втрати ним функціональних властивостей; інформаційні – збирання даних без обов'язкового доступу до ресурсу; стримуючі – тимчасова затримка ресурсу з метою втрати його актуальності; знищуючі – безповоротна втрата ресурсу);
- за місцем прикладення зусиль (до зовнішніх запам'ятовуючих пристроїв, до ліній зв'язку, до основної пам'яті комп'ютера, до жорсткого диску автоматизованого робочого місця, до жорсткого диску сервера, до апаратури зв'язку, до даних на периферійних пристроях).

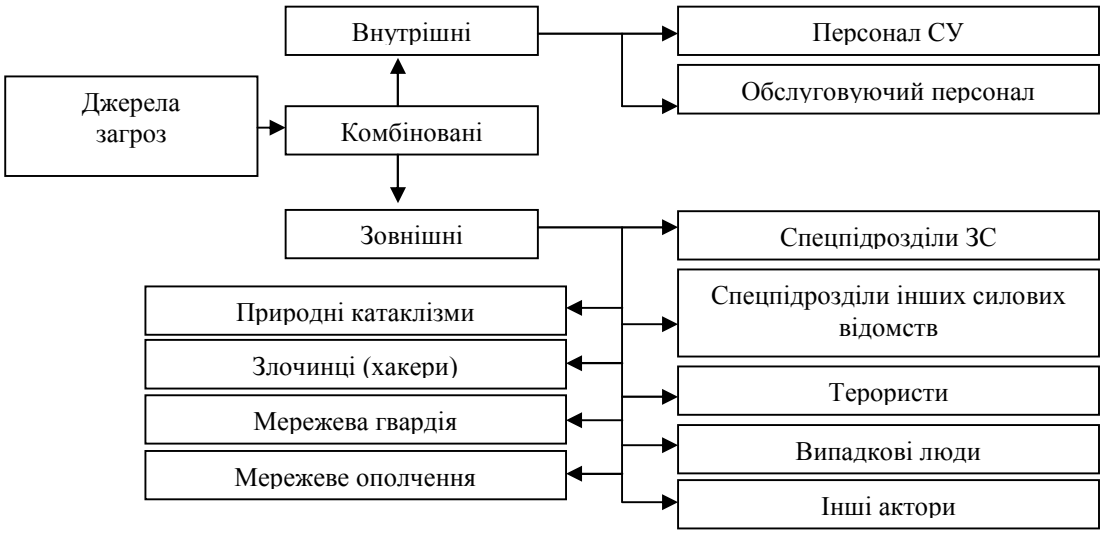

Рис. 1. Класифікація джерел загроз живучості інформаційно-управляючих систем

Під третьою складовою моделі розглядаються об'єкти (рис. 2), на які може здійснюватись напад.

Таким чином, проблема опису моделі загроз може бути вирішена лише після побудови моделі джерела загроз, методів впливу та об'єкта захисту.

Питанням виключної важливості є визначення пріоритетів у процесі вибору конкретного набору актуальних загроз. Під пріоритетом доцільно розглядати ваговий коефіцієнт, який має відображати імовірність її реалізації. Адже саме імовірність реалізації загроз є найбільш динамічною характеристикою впливу на живучість інформаційно-управляючої системи спеціального призначення. Імовірність реалізації загроз пропонується оцінювати з одного боку як оцінку на підставі наявного досвіду, а з іншого боку як суб'єктивні оцінки, сутність яких визначається особливостями процесів, які перебігають в інформаційно-управляючій системі спеціального призначення та оцінки фахівців стосовно можливого прояву небезпек-загроз.

Ще одним фактором оцінки можливості реалізації загроз є оцінка можливих збитків, які можна оцінювати не тільки з економічної точки зору, а, насамперед, з точки зору можливої втрати управління підлеглими військами (силами) повністю, чи на деякий період. При цьому необхідно враховувати витрати на засоби забезпечення живучості (закупівлю та обслуговування), які повинні оптимально співвідноситись з можливими збитками.

Взаємозв'язок факторів можливих загроз відображено на рис. 3, де під першою фазою розуміють проникнення в систему, а під другою – взяття під контроль активів та ресурсів у результаті чого здійснюється нанесення реального збитку.

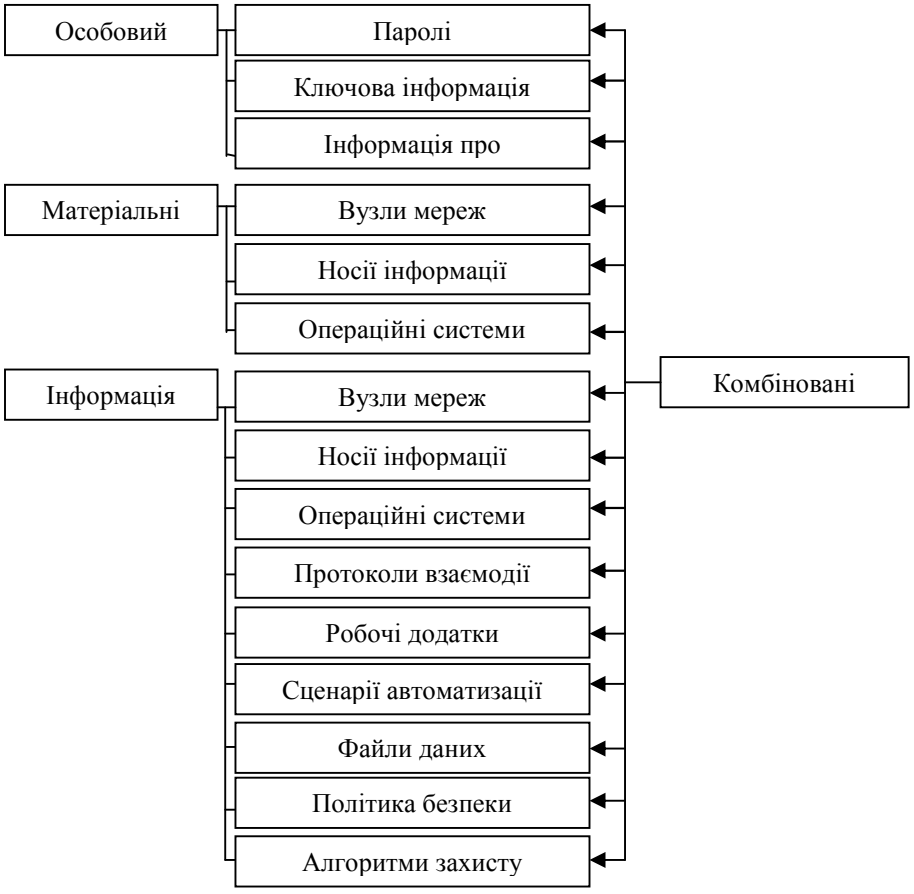

Рис. 2. Класифікація логічних ознак об'єктів, на які здійснюється напад

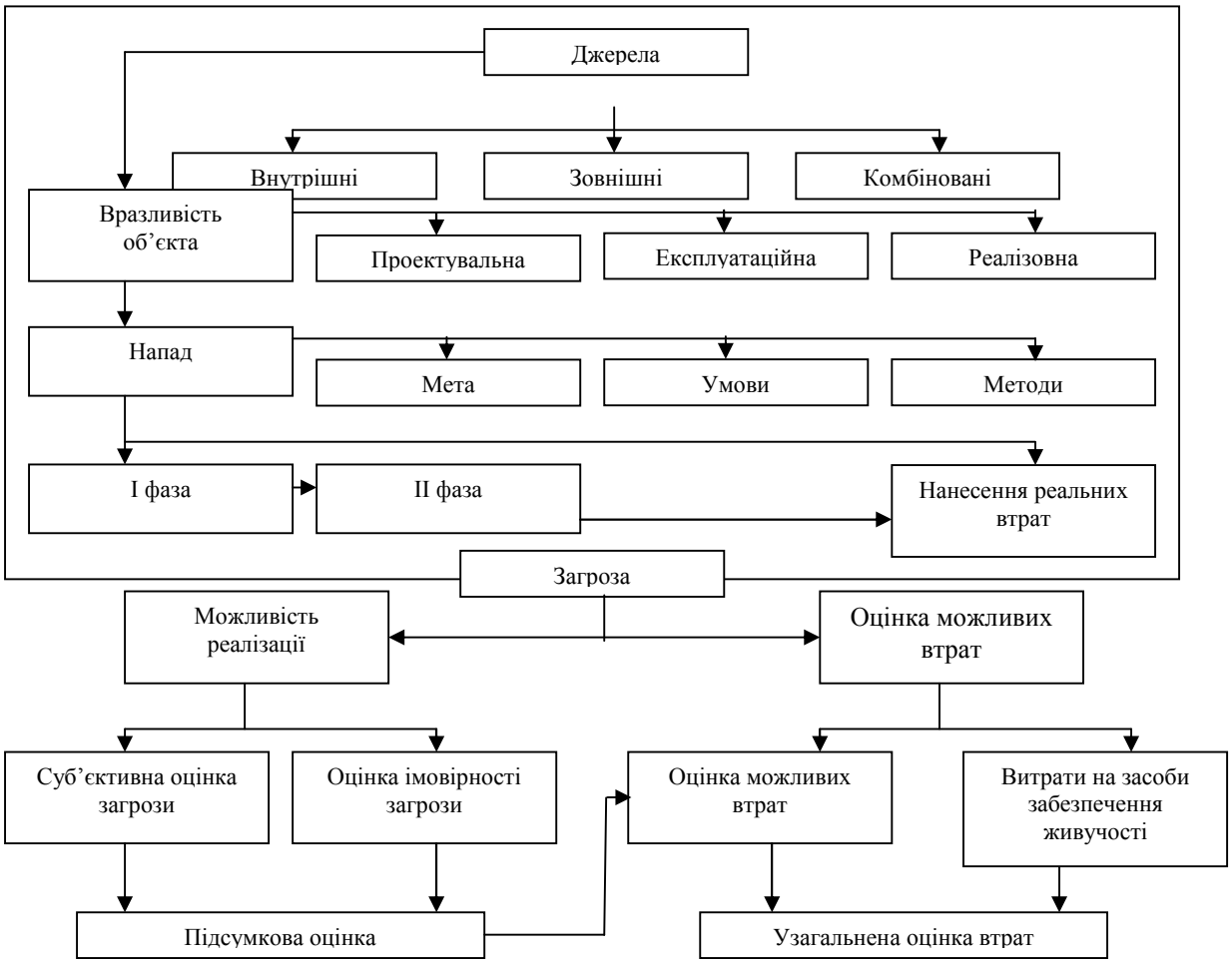

Рис. 3. Взаємозв'язок факторів категорій загроз живучості інформаційно-управляючих систем

Висновки і напрямки подальших досліджень

Узагальнення міжнародної практики в галузі забезпечення живучості інформаційно-управляючих систем дає змогу навести основні завдання системи забезпечення живучості:

- забезпечення стабільної, ефективної діяльності органів управління;
- високу постійну готовність систем управління до роботи;
- оперативність управління підрозділами;
- високу якість управління;
- стійкість управління.

Лише забезпеченням живучості інформаційно-управляючих систем спеціального призначення можна досягти визначених завдань.

У подальшому пропонується здійснити конкретне наповнення та деталізацію факторів представлених фактично в структурі моделі загроз інформаційно-управляючим системам спеціального призначення.

Список літератури

1. Синявский В.К. Возможные подходы к созданию автоматизированных систем управления войсками (силами) / В.К. Синявский // Наука и военная безопасность. – 2008. №3. – С.21-27.

2. Барвиненко В.В. Об автоматизации управления группировками Вооруженных Сил / В.В. Барвиненко. – М: Военная мысль. – 1999. – №2.

3. Азаров Г.И. Направление развития средств и систем военной связи / Г.И. Азаров. – М: Военная мысль. –2003. – №4.

4. Вервейко Б.М. Разработка формальной модели оценки эффективности функционирования СУ ВС / Б.М. Вервейко. – Мн.: Государственное учреждение "НИИ Вооруженных Сил Республики Беларусь". – 2008. – С.125-196.

5. Системы и средства управления вооруженных сил ведущих зарубежных стран и направления их развития (информационно-аналитический обзор). – Мн.: ГУ "НИИ ВС РБ". – 2007. – 303с.

6. Надійність техніки. Терміни та визначення. ДСТУ 2860-94. –К.: Держстандарт України, 1995. – 92 с.

7. *Автоматизированные системы управления. Общие требования. ГОСТ 24.104-85. –М.: Государственный стандарт СССР, 1987.*

Стаття надійшла до редколегії 28.02.2013

Рецензент: д-р техн. наук, проф. Ю.В. Кравченко, Національний університет оборони України, Київ.