УДК 355.415.7:[355.405.1]
Ляшенко І.О. к.військ.н.[1];
Цвєтков Є.В. к.військ.н.[1];
Гаценко С.С.[2]

[1] - Національний університет оборони України імені Івана Черняховського;
[2] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

Модель загроз інформаційно-управляючим підсистемам розвідки

Резюме. Запропоновано підхід для проведення класифікації та обґрунтування моделі загроз живучості інформаційно-управляючих підсистем розвідки, яка включає: джерело загроз, методи реалізації загроз та об'єкт впливу.

Ключові слова: інформаційно-управляючі підсистеми розвідки, загрози, збитки, імовірність реалізації, живучість.

Модель угроз информационно-управляющим подсистемам разведки

Резюме. Предложен подход для проведения классификации и обоснования модели угроз живучести информационно-управляющих подсистем разведки, которая включает: источник угроз, методы реализации угроз и объект воздействия.

Ключевые слова: информационно-управляющие подсистемы разведки, угрозы, убытки, вероятность реализации, живучесть.

Model of threats to information management intelligence subsystems

Resume. An approach to the classification and rationale for the threat model survivability of information and intelligence management subsystems, which includes: a source of threats and methods of threats implementation and impact object.

Keywords:. information and control intelligence subsystems, threats, losses, probability of realisation, vitality.

Постановка проблеми. Досвід війн та збройних конфліктів кінця XX – початку XXI ст., висвітлений у закордонних і вітчизняних джерелах [1 - 6], свідчить про те, що у збройному протиборстві із застосуванням як традиційних, так і новітніх засобів збройної боротьби все більшого значення набуває інформаційна перевага, досягненням якої, перш за все, займається розвідка.

У провідних країнах світу внаслідок своєчасного усвідомлення цієї тенденції різко активізувався процес створення так званої мережевої системи управління бойовими діями. При цьому, на сьогодні, стратегії інтеграції в цю систему підпорядковано всі передові розробки у сфері інформаційних технологій.

Відповідно, Україна не могла стояти осторонь світових тенденцій, тому в 2001 році було затверджено Концепцію створення єдиної автоматизованої системи управління (ЄАСУ) Збройними Силами України (ЗСУ), до складу якої мають увійти інформаційно-управляючі підсистема розвідки (далі – ІУПР).

Ці підсистеми будуть пронизувати всю вертикаль системи розвідки України. При цьому, вже тепер мережа цих підсистем має точки доступу до всесвітньої глобальної мережі Інтернет, присутність в якій таких складових як дефекти архітектури, програмного та апаратного забезпечення і зростання кількості самих систем, які працюють у режимі реального часу, забезпечує значну уразливість цієї мережі, як від загроз випадкових, так і загроз навмисного характеру. При цьому останні будуть реалізовуватись у вигляді різноманітних атак та їх комбінацій.

Тому проблема забезпечення живучості інформаційно-управляючих підсистем розвідки на наш час є досить актуальною.

Аналіз останніх публікацій. Питаннями аналізу розробки та застосування математичних моделей процесів функціонування інформаційно-управляючих підсистем на сьогодні приділяється значна увага [7 - 11].

Однак, у зазначених джерелах основна увага зосереджена на автоматизації основних функціональних процесів із метою забезпечення обґрунтованості та оперативності роботи цих систем. При цьому живучості системи, як однієї з найважливіших вимог до розвідки, належної уваги не приділяється. Під живучістю інформаційних та інформаційно-управляючих підсистем спеціального призначення розуміється властивість цих підсистем зберігати або за максимально короткий час відновлювати свою боєздатність в умовах деструктивного впливу противника [12, 13]. З метою своєчасного реагування на загрози ІУПР необхідно створити модель цих загроз.

Метою статті є класифікація та обґрунтування моделі можливих загроз живучості інформаційно-управляючих підсистем розвідки.

Основний матеріал. Для забезпечення живучості інформаційно-управляючих підсистем, перш за все, 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).

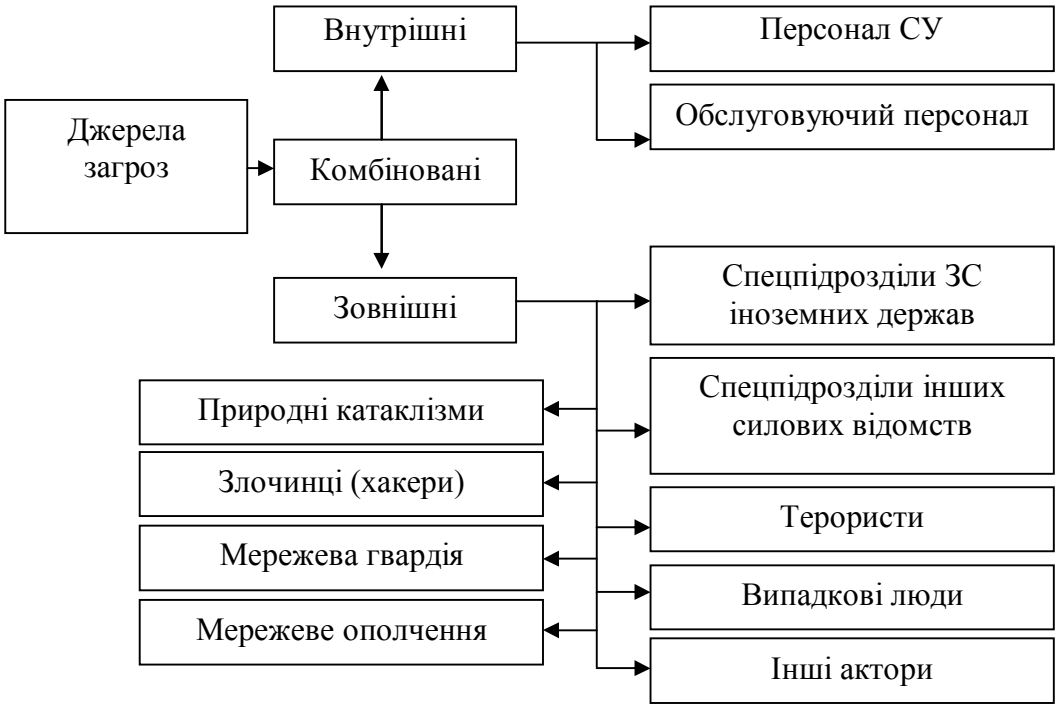

Рис. 1. Класифікація джерел загроз живучості інформаційно-управляючих систем

До внутрішніх джерел загроз можна віднести персонал ІУСР, який використовує ці системи та такий, що їх обслуговує.

До зовнішніх джерел загроз можна віднести:

природні катаклізми (землетруси, повені, пожежі тощо);

злочинців (хакерів);

мережеву гвардію (спеціальні інформаційні центри, що створюються на період надзвичайних подій, діяльність яких закріплена законодавчо та підтримується державою);

мережеве ополчення (мережеві добровольці, нерегулярні мережеві комбатанти);

спецпідрозділи ЗС (диверсійно-розвідувальні, диверсійні тощо);

та інші джерела (підрозділи кіберрозвідки та кібершпіонажу).

Наступною складовою моделі є методи, якими будуть реалізовуватись загрози.

Методи впливу розрізняють:

- за мотивацією (випадкові, навмисні);
- за характером впливу (на конфіденційність, достовірність, цілісність та доступність);
- за ступенем автоматизації (мануальні, автоматизовані та автоматичні);
- за ініціалізацією (умовні та безумовні);
- за взаємодією з політикою безпеки (дополітичні та постполітичні);
- за інструментальними засобами (технічні, апаратні та програмні);
- по природі 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 інжинірінг, криптоаналітичні та неспецифічні – такі, що не мають вищеперерахованих 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 зворотного зв'язку (зі зворотним зв'язком та без нього);

- за ступенем складності (прості, складні та системні);

- за імовірністю виникнення (імовірна, малоімовірна і з великою імовірністю);

- за формою (кібероперації – легальні, тактичні, стратегічні та спеціальні; кібератаки);

- за направленістю результату (розширяючі – отримання більших повноважень щодо доступу; викривляючі – 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 – збір 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. 2. Класифікація логічних ознак об'єктів, на які здійснюється напад

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, визначення методів впливу та об'єктів захисту.

Питанням виключної важливості є визначення пріоритетів при виборі конкретного набору актуальних загроз. Під пріоритетом доцільно розглядати ваговий коефіцієнт, який повинен відображати імовірність її реалізації. Адже саме імовірність реалізації загроз є найбільш динамічною характеристикою впливу на живучість інформаційно-управляючої системи спеціального призначення.

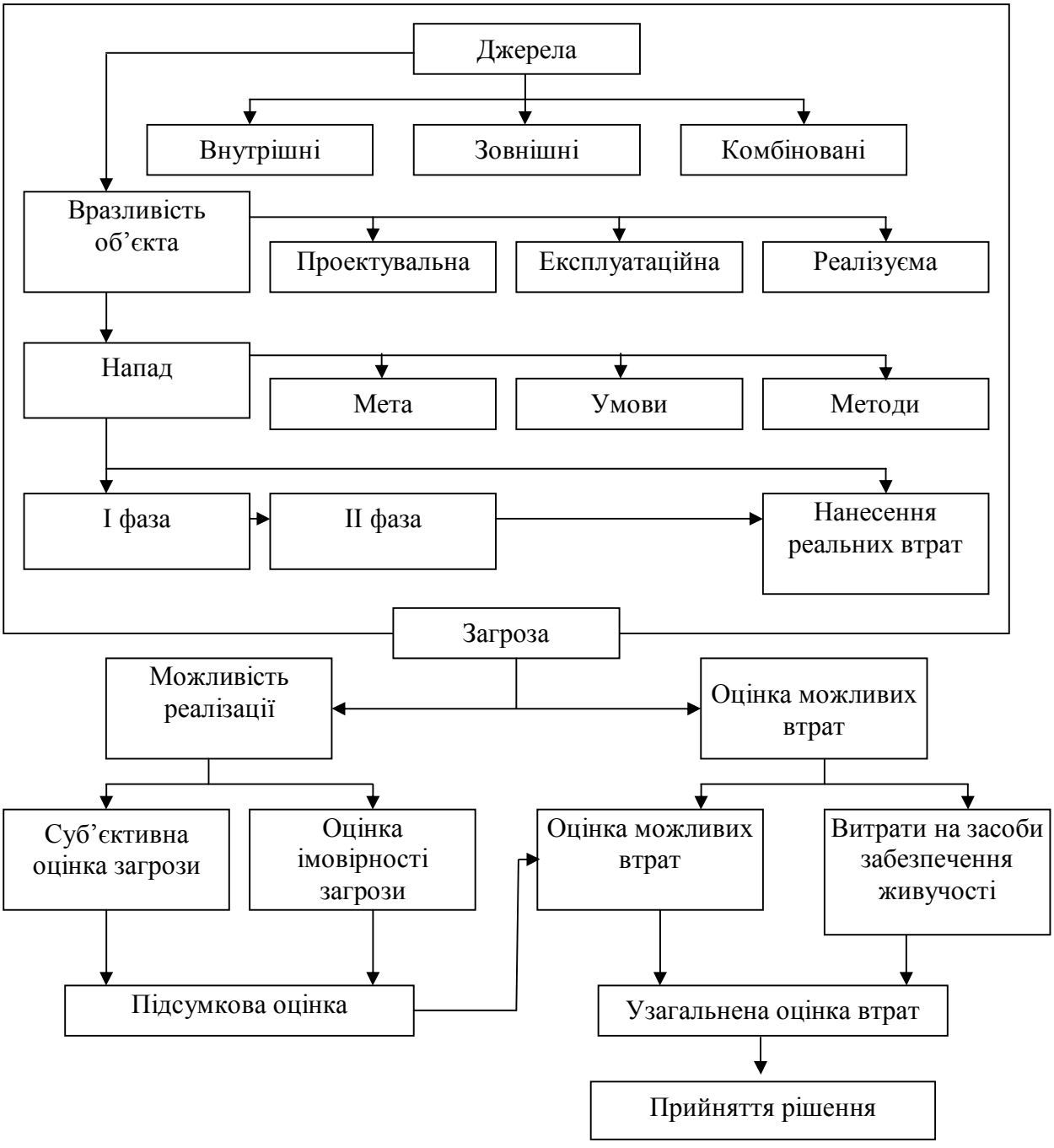

Рис. 3. Взаємозв'язок категорій загроз живучості інформаційно-управляючих систем

Висновки та напрями подальших досліджень. Таким чином, запропонована модель містить наступні складові:

- джерела загроз;
- методи реалізації загроз;
- об'єкти загроз.

Застосування моделі в інформаційно-управляючих системах розвідки дасть змогу підвищити їх живучість, адже лише забезпеченням живучості інформаційно-управляючих систем розвідки можна досягти визначених завдань.

У подальшому пропонується здійснити конкретне наповнення та деталізацію факторів представлених в моделі загроз інформаційно-управляючим підсистемам спеціального призначення, а також обґрунтування кількості показників пріоритетів загроз та ймовірності реалізації цих загроз.

СПИСОК ЛІТЕРАТУРИ

1. Мальцев Л.С. Военная безопасность государства и характер будущих войн / Л.С. Мальцев. – Минск: Наука и военная безопасность. – 2003. – № 1.
2. Гурулев С.П. Взгляды на развитие вооруженной борьбы, способы решения задач военной безопасности государства. Перспективный облик Вооруженых Сил Республики Беларусь / С.П. Гурулев. – Минск, Армия. – 2008. - № 1.
3. Литошенко А. АСУ: выбор вектора развития. Будущее – за глобальным информационным полем // Литошенко А. // Воздушно-космическая оборона. – 2007. – №6(37). – С.38-45.
4. Куликов А. Война в едином информационном пространстве / Куликов А. / Воздушно-космическая оборона. – 2008. – № 2. – С.54-60.
5. Ляшенко І.О. Еволюція розвитку концепцій ведення збройної боротьби /І.О.Ляшенко / Сучасні інформаційні технології у сфері безпеки і оборони. К., 2009. – № 3 (6). С. 91 – 93.
6. Ляшенко І.О. Мережоцентризм у військовій справі / І.О.Ляшенко / Сучасні інформаційні технології у сфері безпеки і оборони. К., 2009. – № 2 (5). С. 78 – 81.
7. Синявский В.К. Возможные подходы к созданию автоматизированных систем управления войсками (силами) // В.К. Синявский // Наука и военная безопасность. – 2008. №3. – С.21-27.
8. Барвиненко В.В. Об автоматизации управления группировками Вооруженных Сил / В.В. Барвиненко. – М: Военная мысль. – 1999. – №2.
9. Азаров Г.И. Направление развития средств и систем военной связи / Г.И. Азаров. – М: Военная мысль. – 2003. – №4.
10. 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.
11. Системы и средства управления вооруженных сил ведущих зарубежных стран и направления их развития (информационно-аналитический обзор). – Мн.: ГУ "НИИ ВС РБ". – 2007. – 303с.
12. Надійність техніки. Терміни та визначення. ДСТУ 2860-94. – К.: Держстандарт України, 1995. – 92 с.
13. Автоматизированные системы управления. Общие требования. ГОСТ 24.104-85. – М.: Государственный стандарт СССР, 1987.