6. *Корнилов А.Г.* Экранирование электронной аппаратуры от воздействия электромагнитного поля : методические указания к лабораторной работе / А Г. Корнилов; под ред. Н.Б. Куншина. – Казань : Изд-во КГТУ, 2002. – 36 с.
7. Защита танков / [Григорян В.А., Юдин В.Г., Терезин И.И. и др.] ; под ред. В.А. Григоряна [Н.Г. Гусев, В.А. Климанов, В.П. Машкович, А.П. Суворов]. М. : Изд-во МГТУ им. Н.Є. Баумана, 2007 – 327 с.
8. Защита объектов народного хозяйства от оружия массового поражения / [Демиденко Г.П., Кузьменко Е.П., Орлов.П.П. и др.] ; под ред. Г.П. Демиденко. - [2-е изд. доп.]. – К. : Вища шк., 1989. – 287 с.
9. *Кравець І.А.* Наукова гіпотеза захисту озброєння та військової техніки від зброї електромагнітного імпульсу / І.А. Кравець, О.М. Воробйов // Збірник наукових праць НУОУ „Труди Університету". – 2010. - № 2 (95). – С. 244-248.

Поступила 25.9.2013р.

УДК 007.355

І.О. Ляшенко, І.Ю. Кравченко, м. Київ

ОЦІНКА СТАНУ КРИТИЧНОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

The methods of assessment of the criticality of information and control systems for special purposes by the indicators of ability to attack, protection and dependence

Keywords: information and control systems, the state of criticality, the ability to attack, defense and independence

Вступ. Події кінця XX – початку XXI сторіччя проходять на фоні трансформації суспільства від постіндустріального до інформаційного. Відбувається бурхливий розвиток інформаційних технологій (ІТ) та їх проникнення у всі сфери діяльності людини: соціальну, економічну, політичну, воєнну тощо. До основних характерних рис процесу інформатизації суспільства на сучасному етапі відносяться глобалізація та інтенсифікація інформаційних процесів, зміна сучасної картини світу.

Завдяки революції в області інформатизації та комунікацій відбуваються значні зміни у військовій справі. З'являються нові види озброєння, засновані на застосуванні ІТ, які дозволяють вести неконтактні бойові дії. Розвиваються засоби розвідки, автоматизовані системи управління військами та зброєю.

Поширивс я континуум вимірів, в яких може вестися збройна боротьба – сьогодні можна констатувати, що вона ведеться не тільки в традиційних вимірах: "простір – час", але й в "інформаційному вимірі".

У сучасних умовах інформаційна інфраструктура держави набуває статусу критичної (життєво важливої для існування) з усіма від цього

похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. До критичної інформаційної інфраструктури належать, в першу чергу, економіка, транспорт, енергетика, фінансова система, системи управління структур, що забезпечують безпеку та оборону держави тощо. Особливої уваги заслуговують при цьому системи управління військами та зброєю, канали зв'язку, системи навігації, розвідки та інші елементи інформаційного середовища, які потребують захисту від відповідних зовнішніх впливів як випадкового, так і навмисного характеру.

Метою даної статті є обґрунтування методики оцінки стану критичності інформаційно-управляючих систем спеціального призначення.

Основна частина. Основним принципом застосування інформаційної зброї являється запуск програми самоусунення (знищення, самообмеження можливостей, зміна функцій чи приналежності). Завданням атакуючої сторони є, маніпулюючи вхідними даними, активізувати в складній інформаційній системі задані процеси чи програми. Де під складною інформаційною системою ми розуміємо таку систему, до складу якої входять елементи, що функціонують відповідно до правил сформованих відмінними одна від одної множин аксіом [1].

Під знаннями інформаційної системи розуміється сукупність відомостей, яка відображена через структуру системи та функціональні можливості її елементів [1-10].

Виходячи з даного трактування, можна визначити таке поняття як інформаційна ємність, яка визначається кількістю елементів в структурі, кількістю зв'язків між ними та вагами цих елементів та зв'язків

$$E_{ic} = \sum_{i=0}^{n} c_i + \sum_{k=0}^{s} c_k \ , \qquad (1)$$

де: n - кількість елементів у системі;

s - кількість зв'язків між елементами;

c_i, c_k - відповідні ваги.

Оцінка можливостей інформаційної системи здійснюється з урахуванням вхідної та вихідної інформації. Де під терміном інформація слід розуміти зміну параметра спостерігача, яка виникла внаслідок взаємодії спостерігача та об'єкта й може бути оцінена через величину зміни інформаційної ємності системи-спостерігача [7]

$$I_{ic} = \frac{(E_{ic}(t_2) - E_{ic}(t_1))}{(t_2 - t_1)}, \qquad (2)$$

де: $E_{ic}(t_2)$ - інформаційна ємність системи, що задіяна в момент t_2;

$E_{ic}(t_1)$ - інформаційна ємність системи, що задіяна в момент t_1.

Застосування інформаційної зброї не передбачає "виділення значної енергії" для ураження противника: апріорі вважається, що противник володіє

усіма необхідними силами та засобами для свого власного знищення. В ролі інформаційної зброї можуть виступати будь-які технічні, біологічні чи соціальні засоби.

Застосування інформаційної зброї передбачає:

проведення аналізу способів та алгоритмів активізації системи противника;

вибір чи розробку відповідної інформаційної зброї;

застосування інформаційної зброї по заданому інформаційному об'єкту у визначеному місці, періоді часу та визначеним способом.

Вимогами до застосування інформаційної зброї є:

перевага над іншими видами зброї подібного класу, впливу в оперативності, простоті та вартості;

нанесення противнику втрат заданого масштабу в визначений інтервал часу.

На сьогоднішній день виникли умови задоволення визначених вимог, а саме:

створено автоматизовані та автоматичні засоби, що здатні отримувати з даних знання;

відбулось значне знецінення виробництва даних, їх доставки та скорочення часу доставки;

значно зросла ефективність інформаційного впливу внаслідок появи нових теорій та технологій.

Як вже згадувалось вище, кінцевим об'єктом дії інформаційної зброї будуть знання конкретної інформаційної системи, шляхом цілеспрямованої зміни яких вносяться спотворення в модель жертви.

При цьому процес цілеспрямованої зміни знань інформаційної системи під впливом вхідних даних є не що інше, як перепрограмування системи. Тому інформаційне протиборство можна розглядати як зіткнення різних знань, при якому визначається знання, яке на визначений момент є найбільш адекватне виживанню інформаційної системи [1].

Цілеспрямована зміна знання системи може включати в себе:

зміну кількості елементів інформаційної системи;

зміну зв'язків між цими елементами;

зміну функціональних можливостей визначених елементів;

все перераховане вище.

Можна сформулювати висновок про те, що в інформаційному протиборстві інформаційних систем перемогу отримує та, яка:

має найбільш стійку структуру до інформаційного впливу противника;

може в найкоротші строки згенерувати та застосувати по противнику процес перепрограмування.

Отже інформаційне протиборство являє собою цілеспрямовану зміну знань конкретної інформаційної системи, через внесення спотворення в модель жертви.

Звідси слідує, що інформаційним “полем бою” будуть інформаційні моделі. В залежності від змін у внутрішньому стані інформаційних систем пропонується інформаційні моделі класифікувати за їх можливостями (рис. 1):

системи з незмінним внутрішнім станом після обробки вхідних даних;

системи зі змінним внутрішнім станом.

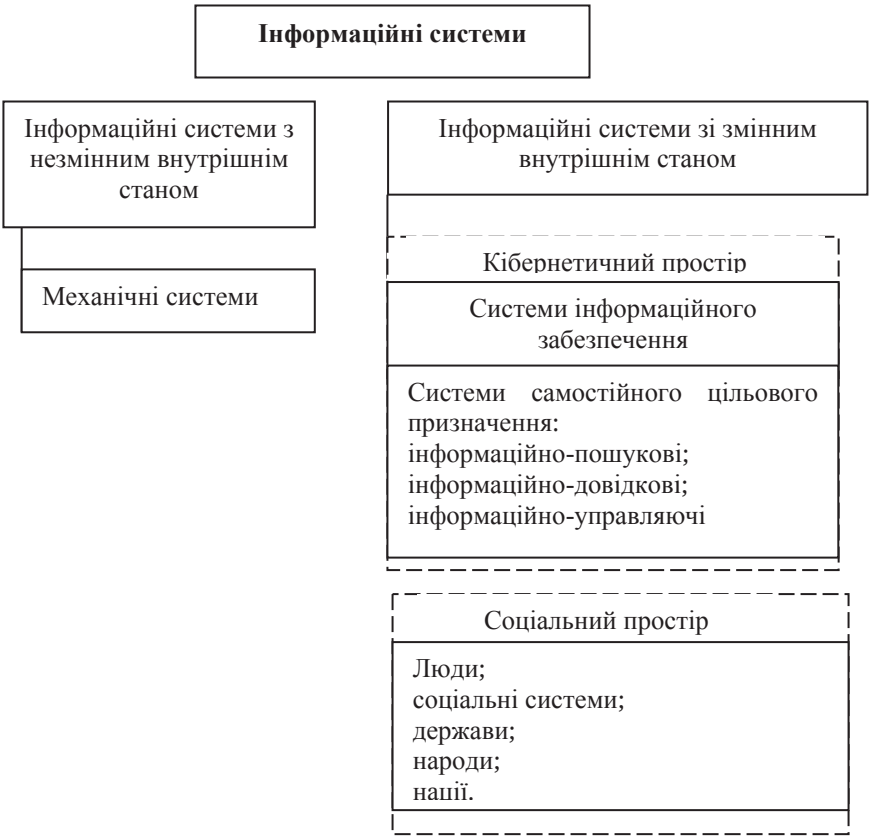

Рис.1. Класифікація інформаційних систем

До систем з незмінним внутрішнім станом відносять інформаційні системи, які після обробки даних повертаються у вихідний стан (аналоговий зв'язок).

До систем зі змінним внутрішнім станом відносять інформаційно-довідкові, інформаційно-пошукові та інформаційно-управляючі, а також інформаційні системи соціального простору.

Крім того усі системи можна розподілити на інформаційні системи загального використання та спеціального призначення.

До інформаційних систем загального використання відносять системи, що призначені для обробки будь-яких даних, незалежно від сфери застосування.

Інформаційні системи спеціального призначення призначені для вирішення завдань в конкретній предметній чи відомчій області.

Якщо порівнювати інформаційні системи з незмінним внутрішнім станом та системи зі змінним внутрішнім станом, цілком зрозуміло, що у випадку конфлікту перемогу отримають останні. Але порівняння інформаційних систем зі змінним внутрішнім станом між собою викликає деякі труднощі відносно того хто вийде переможцем у випадку конфлікту та які шляхи існують щодо посилення їх потенціалу.

Оскільки при порівнянні інформаційних систем нас більш усього буде цікавити їх інформаційні моделі, або інформаційна узагальненість безвідносно природи їх об'єктів, пропонується розглянути підхід щодо оцінки стану критичності цих систем.

При оцінці стану критичності інформаційних систем необхідно враховувати не лише здатність системи впливати на інші системи, але й здатність її захищатись від нападу та ступінь її залежності від використання кібернетичного простору.

Під залежністю системи від кібернетичного простору пропонується розуміти ступінь кібернетизації системи (вихід в інші мережі, просторові розміри системи та її мереж, залежність інших систем від неї, ступінь технічного оснащення та інш.).

Тоді під здатністю системи до захисту розуміється її здатність застосовувати сили та засоби для відбиття нападу, а також зменшення її залежності від використання кібернетичного простору.

Тобто, в загальному вигляді оцінити стан критичності $П_{sc}^{rs,}$ можна

$$П_{sc}^{rs,} = Н + Зх + Нз\,, \qquad (3)$$

де: $Н$ – коефіцієнт ефективності нападу;

$Зх$ – коефіцієнт ефективності захисту;

$Нз$ – коефіцієнт незалежності.

Коефіцієнт ефективності нападу залежатиме від:

кількості $n_{IC}^{пр-к}$ та відповідної ваги $C_{IC}^{пр-к}{}_i$ елементів системи противника які можуть бути уражені наявними засобами з заданим ступенем ураження;

відстані $l_{IC}^{нап}$ на яку може бути застосовано інформаційний вплив, причому $l_i^{пр-к} = \begin{cases} 1, & при \quad l_i^{нап} \geq l_i^{зх} \\ 0, & при \quad l_i^{нап} \prec l_i^{зх} \end{cases}$;

інтервалу часу, за який елементи системи можуть бути перепрограмовані.

В загальному вигляді розрахунок коефіцієнту ефективності нападу має вигляд

$$H = \frac{s \cdot \sum_{i=0}^{n} C_s}{t} k_0, \qquad (4)$$

де k_0 - коефіцієнт приведення.

Коефіцієнт ефективності захисту залежатиме від:

кількості n_{IC} та ваги C_{ICi} елементів системи, які можуть бути захищені від перепрограмування наявними засобами з заданим ступенем;

інтервалу часу, протягом якого елементи системи можуть бути захищені.

В загальному вигляді розрахунок коефіцієнту ефективності захисту має вигляд

$$Зх = \sum_{i=0}^{n} C_s \cdot t \cdot k_0, \qquad (5)$$

де k_0 - коефіцієнт приведення.

Коефіцієнт незалежності інформаційної системи формується з:

потенціалу, яким управляє система $П_{IC}$;

кількості інформаційних систем, що взаємодіють з даною системою N_{IC}^{vz};

кількості інформаційних систем, які здатні перебрати на себе функції даної системи N_{IC}^{res};

кількості каналів виходу у зовнішнє середовище з системи n_k^{ex} та їх пропускної спроможності C_i^{ex};

ступеня застосування інформаційною системою програмно-технічних засобів ϕ_{ptr}.

Враховуючи дані складові коефіцієнт незалежності системи можна розрахувати

$$Нз = \frac{N_{IC}^{res}}{П_{IC} \cdot N_{IC}^{vz} \cdot n_k^{ex} \cdot \sum_{i=0}^{n_k^{ex}} C_i^{ex} \cdot \phi_{ptr}} k_0^{нз}, \qquad (6)$$

де $k_0^{нз}$ - коефіцієнт приведення.

Висновки. Запропонований підхід може бути використаний для оцінки стану критичності інформаційно-управляючих систем спеціального призначення. Крім того, він дає змогу визначити напрямок зниження ствану критичності інформаційно-управляючих систем. Цілком зрозуміло, що збільшення незалежності та здатності системи до нападу являються найменш перспективними. Саме підвищення здатності системи до захисту, а точніше забезпечення її живучості є найперспективнішим напрямком.

У подальшому передбачається продовжити обґрунтування методології забезпечення живучості інформаційно-управляючих систем спеціального призначення.

1. *Расторгуев С. П.* Информационная война. Проблемы и модели. Экзистенциальная математика: учебное пособие для студентов вузов, обучающихся по специальности в области информационной безопасности / С. П. Расторгуев – М.: Гелиос АРВ, 2006. – 240 с.
2. *Новик И. Б.* Введение в информационный мир / Новик И. Б., Абдуллаев А. Ш. – М.: Наука, 1991. – 89 с.
3. 1. *Ляшенко І. О.* Мережоцентризм у військовій справі / І. О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. К., 2009. – № 2(5). – С. 78 – 81.
4. 2. *Ляшенко І. О.* Еволюція розвитку концепцій ведення збройної боротьби / І. О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. К., 2009. – № 3(6). – С. 91 – 93.
5. 3. *Ляшенко І. О.* Кібернетичний простір - як еволюція розвитку інформаційних технологій / І. О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони. К., 2010. – № 2(8). – С. 14 – 16.
6. 4. *Яковлєв А. В.* Надежность информационных систем / Владимирский гос. университет, Муромский институт (филиал). – Муром, 2004. – 63 с.
7. 5. *Мартынов В. В.* Надежность информационных систем / Изд-во РАУ. – Эр., 2009. – 200 с.
8. 6. *Морозов Ю. Д.* Качество, надежность и эффективность экономических информационных систем / Морозов Ю. Д., Бобков В. П. // Московський гос. университет экономической статистики и інформатики. – М., 1986. – 269 с.
9. 7. *Майерс Г.* Надежность программного обеспечения / Пер. с англ. М.: Мир, 1980. – 360 с.

Поступила 18.9.2013р.

УДК 538.91+538.975+004.922

Н.Н. Крупа, Ю.Б. Скирта

ВЛИЯНИЕ ОТЖИГА НА ФИЗИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПЛЁНОК Ni_2MnGa. АЛГОРИТМ ОБРАБОТКИ ДАННЫХ АТОМНО-СИЛОВОЙ МИКРОСКОПИИ

Приведены результаты влияния отжига плёнок Ni_2MnGa на их структуру, проводимость и магнитные свойства. Описаны алгоритмы обработки изображений поверхности пленок, полученных методом атомно-силовой микроскопии. Показано, что при отжиге пленки из аморфных становятся поликристаллическими и переходят из немагнитного состояния в магнитное мартенситное состояние.

