© Gnatyuk S., Sydorenko V., Duksenko O. Modern approaches to critical infrastructure objects detection and identification // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 269-275.

СУЧАСНІ ПІДХОДИ ДО ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ НАЙБІЛЬШ ВАЖЛИВИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сергій Гнатюк, Вікторія Сидоренко, Оксана Дуксенко

Національний авіаційний університет, Україна

ГНАТЮК Сергій Олександрович, к.т.н.

Рік і місце народження: 1985 рік, м. Нетішин, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2012 року, голова Наукового товариства студентів, аспірантів, докторантів та молодих вчених з 2015 року.
Наукові інтереси: інформаційна безпека, квантова криптографія, управління інцидентами інформаційної безпеки, захист критичної інформаційної інфраструктури держави.
Публікації: більше 190 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, патенти та авторські свідоцтва.
E-mail: s.gnatyuk@nau.edu.ua

СИДОРЕНКО Вікторія Миколаївна

Рік і місце народження: 1990 рік, м. Попасна, Луганська область, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: аспірант кафедри безпеки інформаційних технологій з 2013 року.
Наукові інтереси: інформаційна безпека, захист критичної інформаційної інфраструктури держави.
Публікації: 10 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: v.sydorenko@ukr.net

ДУКСЕНКО Оксана Петрівна

Рік і місце народження: 1970 рік, м. Київ, Україна.
Освіта: Київський міжнародний університет цивільної авіації, 1995 рік; Національний авіаційний університет, 2015 рік.
Посада: викладач Промислово-економічного коледжу з 2013 року.
Наукові інтереси: інформаційна безпека, криптографічний захист інформації, уразливості інформаційних систем.
Публікації: 6 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: oksana-duks@yandex.ru

Анотація. *Сучасні тенденції розвитку інформаційних технологій спричинили феноменальну залежність суспільства від послуг, які надають різноманітні галузі інфраструктури. Нині, якість та доступність таких послуг є одним з головних показників розвитку інфраструктури держави, а забезпечення їх захисту та стабільного функціонування є найважливішою і обов'язковою складовою національної безпеки розвинених держав. Збільшення концентрації засобів та ресурсів для захисту електронних інфраструктур різних типів зумовило необхідність ранжування інфраструктурних об'єктів, виділення найважливіших з них та появи поняття критична інфраструктура. З огляду на це, у роботі проведено багатокритеріальний аналіз підходів до виявлення критично важливих об'єктів для оцінювання їх можливостей щодо виявлення та ідентифікації найбільш важливих об'єктів критичної інформаційної інфраструктури. Встановлено, що найбільш ефективними для інформаційної*

інфраструктури є підходи, що базуються на теорії графів та імітаційному моделюванні, проте більшість існуючих підходів не враховують повної множини параметрів та інформаційної складової – це зумовлює необхідність розроблення універсального методу ідентифікації об'єктів критичної інформаційної інфраструктури.

Ключові слова: *інформаційна безпека держави, критична інфраструктура, ідентифікація, оцінювання рівня критичності, критична інформаційна інфраструктура, захист об'єктів критичної інформаційної інфраструктури.*

Вступ

Однією з найважливіших складових сучасної інформаційної війни є можливість проведення інформаційних операцій. У загальному плані ці операції пов'язані з наданням інформації здатної вплинути на процес прийняття рішень супротивника. У більш глобальному плані їх мета – переконати противника діяти таким чином, який відповідає власним цілям і завданням, завоювати і тримати під контролем комунікаційні системи та мережі опонентів, одночасно захищаючи і зберігаючи контроль над власними системами. Кожна структура має свої уразливості у вигляді критично важливих вузлів і об'єктів, посилань і платформ, незалежно від того, чи є вона комунікаційною, організаційною або біологічною мережею. Об'єднання критично важливих об'єктів в одну велику складну систему, порівняно нещодавно, дістало назву *критична інфраструктура* [1].

Транспортні та енергетичні мережі, нафто- та газопроводи, урядові та військові об'єкти є життєво важливими компонентами діяльності сучасного суспільства. Останнім часом актуальним стало питання безпеки зазначених об'єктів і забезпечення захисту критичної інфраструктури у цілому.

Аналіз існуючих досліджень і постановка завдання

Критична інфраструктура будь-якої держави − це велика складна система стратегічного масштабу, яка є сукупністю значної кількості елементів різного типу, об'єднаних зв'язками різної природи і яка володіє загальною властивістю (призначенням, функцією), відмінною від властивостей окремих елементів усієї сукупності [2, 3]. Необмежена кількість об'єктів і параметрів системи, які постійно варіюються, та важко прогнозована поведінка об'єктів з великою кількістю взаємозв'язків є основними причинами труднощів виявлення об'єктів критичної інфраструктури держави. Для забезпечення захисту найбільш важливих об'єктів критичної інформаційної інфраструктури (КІІ) необхідно, перш за все, ідентифікувати ці об'єкти за певними критеріями чи критичними параметрами (рис. 1).

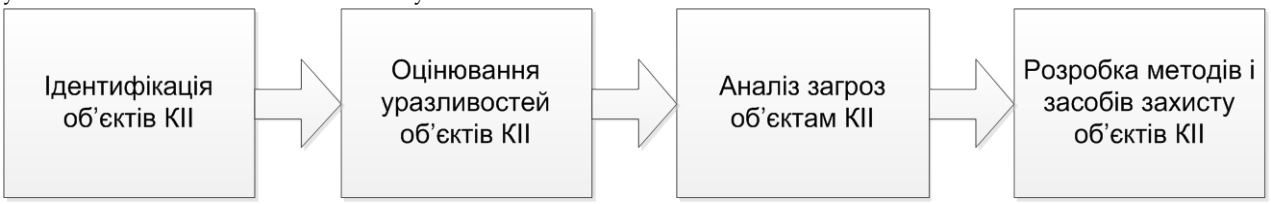

Рис.1. Етапи захисту критичної інформаційної інфраструктури

Як уже зазначалось, поняття «критична інфраструктура» почали активно вживати не так давно – у другій половині 90-х років минулого сторіччя, здебільшого відносно розподілених великомасштабних інформаційних систем (центрів обробки даних, об'єднаних комунікаційних мереж тощо). Більшість розвинених держав самостійно робили спроби дати визначення критичної інфраструктури, розробити підходи до її ідентифікації та державні стратегії захисту. У роботі [4] проведено аналітичне дослідження нормативно-правової бази розвинених держав світу щодо різних варіацій ключових понять у галузі захисту КІІ (критична інфраструктура, КІІ, захист критичної інфраструктури, КІІ).

Що стосується підходів до ідентифікації КІІ, з огляду на роботи [5-7], на сьогодні в розвинених державах відомо незначну кількість методів і моделей, що можуть забезпечити керівникам відповідних ланок управління можливість приймати обґрунтоване і правильне рішення щодо захисту критичних інфраструктур. Проте, не дослідженим і відкритим залишається питання доцільності й ефективності застосування цих методів для виявлення саме об'єктів КІІ.

З огляду на це, **метою роботи** є аналіз відомих підходів до виявлення критично важливих об'єктів інфраструктури для оцінювання їх можливостей щодо ідентифікації найбільш важливих об'єктів критичної інформаційної інфраструктури.

Основна частина дослідження

1. Теорія К. Клаузевіца для мережевих архітектур

Сутність підходу. Основна ідея цієї теорії полягає у пошуку «центральної точки» системи противника, де сконцентровані його ключові сили і потужності.

Опис підходу. Теорія центрів тяжіння К. Клаузевіца досі залишається невід'ємним елементом при розробці сучасних концепцій і відіграє важливу роль в ході підготовки і ведення воєнних операцій. Німецький військовий теоретик і історик К. Клаузевіц створив теорію, яка полягала в тому, що центр ваги − це деяка «центральна точка» або місце, де концентруються найпотужніші сили збройних сил і держави, навколо яких все інше обертається [6]. Тобто центр ваги – це доцентрова

сила, що зв'язує воєдино розрізнені компоненти і, застосувавши комплексний підхід для вивчення зв'язків, що пов'язують розрізнені частини в одне ціле, можна знайти і центр ваги супротивника. І, якщо є можливість направити спеціальний потік енергії (у залежності від типу протистояння) в центральну частину такої системи, то вся вона може бути знищена або виведена з ладу.

На думку К. Клаузевіца найбільш цінний і важливий об'єкт всієї системи обов'язково володіє низкою атрибутів:

– *критичні можливості* − здатності (міць) об'єкта, які роблять його ключовим у контексті певного сценарію, ситуації або завдання;

– *критичні потреби* − умови, засоби, ресурси, методи або способи дії, що дозволяють об'єкту досягати критичних можливостей;

– *критична уразливість* − найбільш уразлива потреба або складовий елемент, виведення з ладу якого не дозволить об'єктам досягти критичних можливостей або виконати поставлене завдання.

На сьогодні у науковій літературі відсутнє формалізоване математичне представлення теорії К. Клаузевіца, проте це можна зробити з переліку основних атрибутів критичної інфраструктури: $K_{ЦВ} = (K_М + K_П + K_У)$, де $K_{ЦВ}$ – критичний центр ваги, $K_М$ – критичні можливості, $K_П$ – критичні потреби, $K_У$ – критична уразливість.

Проте, таке представлення не дає реального значення для знаходження центрів ваги, адже зі збільшенням одного з показників критичності – збільшується і загальний критерій центру ваги. Для більш точного розрахунку необхідно враховувати вагові коефіцієнти для параметрів $K_М, K_П, K_У$, що можуть відрізнятися для різних критичних інфраструктур (різних галузей).

Переваги підходу. Дана теорія дозволяє не тільки розробляти методи виявлення критично важливих об'єктів (центрів тяжіння) інфраструктури супротивника, але і визначати можливі заходи і способи впливу на них.

Недоліки підходу. Результати теорії базуються на припущенні реального місцезнаходження критично важливих об'єктів (центрів тяжіння), тому вони є приблизними і потребують додаткових розрахунків для більш точного оцінювання.

2. Теорія самоорганізуючих мереж А. Барабаши

Сутність підходу. Суть теорії полягає в тому, що будь-яка неструктурована (пуассонівська) мережа під впливом набору загальновідомих правил і законів, в першу чергу економічного і соціального характеру, через певний час (після деякого числа ітерацій) приймає відповідну структуру, без будь-якого зовнішнього впливу, організовуючись навколо найбільш цінних або важливих вузлів.

Опис підходу. А. Барабаши математично довів, що великі мережеві структури (наприклад, Інтернет, соціальні мережі та ін.), що здавалися раніше неструктурованими, тобто випадковими, насправді мають складну внутрішню організацію і є самоорганізуючими з кількома ключовими «хабами», або центрами тяжіння. Центри ваги, в кожному секторі критичної інфраструктури, формуються відповідно до економічних законів, законів соціального розвитку, еволюції та інших правил, що дозволяють з неструктурованих об'єктів формувати самоорганізуючі мережі [6].

Згідно роботи [8] приєднання кожного нового учасника до існуючої мережі відбувається не випадковим чином, тобто в рамках моделі Random Attachment (випадкового приєднання), а деяким особливим шляхом, описаним за допомогою Моделі Preferential Attachment (переважного приєднання). Суть останньої моделі полягає в тому, що різні вузли мають різне число зв'язків і новий вузол з більшою ймовірністю приєднується до найбільш розгалуженого вузла, тому ймовірність зустрітися з ним в просторі Інтернет набагато вища, ніж у менш розгалуженого вузла. Динаміка розвитку мереж описується принципом «багатий стає ще багатшим» (Rich-Get-Richer Phenomen): більш успішні співтовариства ще більше розгалужуються і ще більш консолідують свої зусилля.

Переваги підходу. Самоорганізуюча мережа володіє характеристиками, відмінними від характеристик звичних систем. Статистичні характеристики мережі підлягають не загальному закону нормального розподілу, а степеневому закону розподілу. Якісна відмінність цих законів полягає в тому, що ймовірність великих відхилень виявляється значно вищою. Іншими словами, на частку невеликої кількості вузлів доводиться переважна кількість зв'язків. Крім того, боротьба за зв'язки не є антагоністичною і вузли з великим числом зв'язків можуть мирно співіснувати з менш розгалуженими вузлами. Така система є надзвичайно життєздатною. Як показують експерименти, випадкове вилучення до 80% вузлів дозволяє системі вижити за умови збереження невеликої кількості вузлів [8].

Недоліки підходу. Такий підхід не є гнучким і потребує більш чіткої формалізації для забезпечення необхідного рівня об'єктивності.

3. Теорія графів

Сутність підходу. Суть теорії полягає в тому, що критична інфраструктура може бути представлена у вигляді зваженого орієнтованого графа, вершини якого − об'єкти, а ребра − зв'язки між ними.

Опис підходу. У роботі [9] розглянуто мережу представлену у вигляді графу, яка складається з 10 вершин і 13 ліній зв'язності (рис. 2), де відомі напрямки потоків інформації (рис. 3).

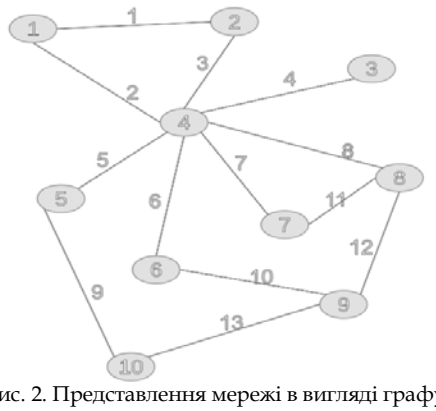

Рис. 2. Представлення мережі в вигляді графу

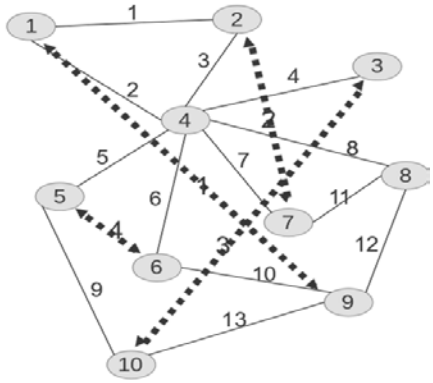

Рис. 3. Напрямки потоків інформації в мережі

Необхідно визначити за графом основні і резервні маршрути передачі інформації за кожним з інформаційних напрямків (рис. 4), де основний маршрут − прямий шлях графом системи зв'язку між абонентами інформаційного напряму, а резервний маршрут − обхідний шлях графом системи зв'язку між абонентами інформаційного напряму з найменшим числом посередників.

Рис. 4. Основні і резервні маршрути передачі інформації

Після цього, до кожного з інформаційних сегментів застосовується критерій належності до критично важливих, який полягає в тому, що вихід з ладу конкретного інформаційного сегмента може призвести до відсутності зв'язності за забезпечуваним ним основним інформаційним напрямком, то він вважається критично важливим інформаційним сегментом аналізованої мережі. У цьому випадку застосування критерію належності показало, що вершина 4 є найбільш критичним сегментом мережі, і при виході її з ладу майже всі інформаційні напрямки понесуть втрати, навіть практично незалежному інформаційному напрямку 4 необхідно буде збільшити плече доставки інформації в 2 рази.

Переваги підходу. Теорія дозволяє наочно представити комплексні взаємозв'язки між об'єктами і розробити математичні вирази для опису рівня взаємодії і взаємозалежності.

Недоліки підходу. Для дослідження інфраструктури необхідно знати не тільки кількість вхідних в ній об'єктів, але і їх взаємозв'язки та взаємовплив. Тільки у такому випадку система може бути представлена у вигляді зваженого орієнтованого графа.

4. Модель пріоритетності активів

Сутність підходу. Суть полягає в розрахунку індексу ризикованості об'єкта, що залежить від рейтингу об'єкта за шкалою категорії чинників та значущості цього чинника [6].

Недоліки підходу. Основний недолік полягає в тому, що дослідження, як правило, здійснювалися без урахування зв'язності об'єктів, що входять до моделі. У той же час, без обліку і аналізу мережевої складової кожного сектора критичної інфраструктури (економічного, фінансового, енергетичного) дуже проблематично забезпечити достатню адекватність моделі об'єкту дослідження.

5. Ідентифікація об'єктів критичної інфраструктури на основі категорію вання

Сутність підходу. Ідентифікація небезпечних об'єктів інфраструктури є першим етапом їх категоріювання. На цьому етапі за допомогою методик оцінки уразливостей за всіма видами потенційного збитку, розроблених для кожного типу об'єктів, визначається значення інтегрального критерію $K_{інт}$, яке порівнюється зі значенням «неприпустимої шкоди» $K_н$:

$$K_{інт} = K_л + K_{екон} + K_{бал} + K_{екол},$$

де $K_л$ − фінансовий збиток, який визначається чисельністю загиблих і постраждалих людей у разі реалізації атаки на об'єкт, $K_{екон}$ − фінансовий збиток у результаті виведення з ладу найбільш уразливих елементів об'єкта, $K_{бал}$ − балансова вартість споруди (або вартість відновлення), $K_{екол}$ − вартісне вираження очікуваного екологічного збитку в разі реалізації терористичної атаки на об'єкт. Для ідентифікації небезпечних об'єктів потрібно визначити поняття «неприпустимий збиток» ($K_н$), тобто той нижній рівень збитку, після досягнення якого об'єкт повинен бути віднесений до розряду небезпечних (критичних) [10]. Процес ідентифікації закінчується складанням переліку небезпечних об'єктів – до нього потрапляють всі об'єкти для яких виконується умова $K_{інт} \geq K_н$, після чого вони підлягають подальшому категоріюванню.

Далі обчислюється реальний критерій потенційного збитку:

$$K^r_{інт} = K_{інт} P_c N_л = (K_л + K_{екон} + K_{бал} + K_{екол}) P_c N_л,$$

де P_c − показник рівня терористичної небезпеки, коефіцієнт, що враховує ймовірність здійснення протягом року терористичного акту на території c-того регіону; $N_л$ − коефіцієнт, що враховує негативні політичні наслідки терористичної чи кримінальної атаки на об'єкт. Критерій $K_{інт}$ визначає у вартісному вираженні рівень ризику терористичної атаки на незахищений об'єкт інфраструктури в конкретному регіоні.

Переваги підходу. Запропонований підхід до ідентифікації небезпечних об'єктів інфраструктури універсальний, не вимагає спеціальної адаптації для кожного виду інфраструктури і дозволяє скласти єдиний реєстр небезпечних об'єктів інфраструктури держави, де кожному об'єкту буде співставлена величина інтегрального потенційного збитку $K_{інт}$.

Недоліки підходу. Важливим аспектом проблеми категоріювання є вибір раціонального числа категорій небезпечних об'єктів інфраструктури. Потрібно для кожної інфраструктури визначити оптимальне число категорій небезпечних об'єктів за критерієм «ефективність − вартість». Суть проблеми полягає в наступному. Очевидно, що вартість системи захисту небезпечного об'єкта прямо пропорційна ступеню його потенційної небезпеки, іншими словами, чим об'єкт потенційно небезпечніший, тим більше складної і дорогої системи захисту він вимагає. Якщо число категорій мале (наприклад, три), то для великої кількості об'єктів кожної категорії загальна для цієї категорії вартість систем захисту буде надлишковою, тобто кошти будуть витрачені нераціонально. Для більш раціонального розподілу коштів необхідне збільшення числа категорій, таким чином, щоб надмірність вартості захисту для всіх об'єктів конкретної категорії була б мінімально допустимою [10].

6. Імітаційне моделювання

Імітаційне моделювання засноване на програмному відтворенні розгорнутого в часі процесу функціонування системи стає реальним інструментом для розуміння і повноцінного дослідження критичної інфраструктури. Метою імітаційного моделювання є створення імітаційної моделі об'єктів критичної інфраструктури і проведення імітаційного експерименту над ними. Це дасть змогу вивчити закони їх функціонування і поведінки з урахуванням заданих обмежень і цільових функцій в умовах імітації та дозволить визначити взаємозв'язки між об'єктами, а також виявляти найбільш уразливі з них. Згідно [11] основою імітаційної моделі для об'єктів критичної інфраструктури є:

– розробка моделі системи на основі часткових імітаційних моделей (модулів) підсистем, об'єднаних своїми взаємодіями в єдине ціле;

– вибір інформативних (інтеграційних) характеристик об'єкта, способів їх здобуття і аналізу;

– побудова моделі впливу зовнішнього середовища на систему у вигляді сукупності імітаційних моделей зовнішніх впливаючих чинників;

– вибір способу дослідження імітаційної моделі відповідно до методів планування імітаційних експериментів.

Основними методами імітаційного моделювання інфраструктур є: аналітичний метод, метод статичного моделювання і комбінований метод (аналітико-статистичний) метод, але вибір будь-якого з них залежить від специфіки досліджуваної інфраструктури та завдань дослідження.

6.1. Система моделювання критичних інфраструктур

Сутність підходу. Система Critical Infrastructure Interdependency Modeling (CIMS) [12] є дискретним моделюванням подій, що моделює та імітує інфраструктури і взаємозалежності, які існують між ними на рівні, відповідному ситуації. Система CIMS була розроблена для вивчення взаємозв'язку між мережами інфраструктури, а точніше мінливості поведінки системи, яка проявляється коли один або декілька вузлів в системі вийшли з ладу. Шляхом простого натискання клавіші вона дозволяє оперативно змінювати стан досліджуваної системи, швидко адаптуючись до мінливої обстановки. Також, система забезпечує високу наочну та інтерактивну середу для спостереження каскадних ефектів і наслідків впливу на інфраструктуру. Завдяки такій візуалізації досягається більш глибоке розуміння мінливої поведінки системи.

Переваги підходу. Модель CIMS є системою імітаційного моделювання, що поєднує дані геопросторової інформації та чотиривимірний (просторово-часовий) ефект. Дозволяє оперативно змінювати стан досліджуваної системи, а саме: обирати та безпосередньо управляти конкретним об'єктом критичної інфраструктури; вводити додаткову подію безпосередньо під час роботи моделі; створювати подієвий сценарій для ініціювання аварійних подій через заданий проміжок часу [6]. Візуалізація послідовна і оновлюється відповідно до моделювання, щоб виявити мінливу або передбачувану поведінку системи, що проявляється у результаті взаємозалежності між вузлами. Це дає можливість легко та швидко оцінити взаємовідносини між мережами інфраструктури та їх наслідки, полегшуючи процес прийняття рішень.

Недоліки підходу. Система CIMS є дискретним моделюванням подій і не представляється в реальному часі. Результати імітаційного моделювання часто обмежені через можливості інформаційного, математичного, технічного забезпечення реалізації моделі.

6.2. Імітаційна модель «Афіна»

Сутність підходу. Модель «Афіна» – програмний інструмент, розроблений для аналізу великих складних систем стратегічного масштабу (включаючи політичний, військовий, економічний та інформаційний сектори), а також для виявлення взаємозалежностей і взаємопов'язаних елементів.

Опис підходу. У цьому програмному інструменті використовується метод Барлоу (Barlow Method) для визначення горизонтальної зв'язності елементів з ваговими коефіцієнтами, метод Вардена (Warden Method) – для розтину вертикальної взаємозалежності та ін. За твердженням американських фахівців, інтегроване застосування цих методів дозволило розробити математичний апарат для дослідження об'єктів будь-якого масштабу (секторів інфраструктури, міст, країн і регіонів) з метою виявлення їх уразливих сегментів (по аналогії з центрами тяжіння К. Клаузевіца) і видачі за ними подальших вказівок [6].

Переваги підходу. У цій моделі передбачено графічний інтерфейс з можливістю відображення виявлених об'єктів, зв'язків між ними і визначення ступеня їх взаємозалежності. Крім того, модель інтегрована з геоінформаційними системами.

Недоліки підходу. Результати імітаційного моделювання часто обмежені через можливості реалізації моделі (аналогічно попередньому підходу). Отримані результати, як правило, не використовуються як готові управлінські рішення, а

розглядаються як своєрідні консультуючі (дорадчі) засоби для наступних раціональних дій менеджера в процесі управління.

Аналіз підходів за базовими критеріями

Таким чином, сьогодні відомо достатню кількість підходів до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури, проте для оцінки доцільності й ефективності їх застосування для виявлення саме об'єктів КІІ необхідно їх проаналізувати за такими базовими критеріями (табл. 1): *1) ясність формалізації* (чіткість і зрозумілість математичних розрахунків); *2) простота реалізації* (відсутність надскладних процедур); *3) гнучкість та універсальність* (можливість зміни певних параметрів за необхідності і застосування у різних галузях діяльності людини); *4) точність* (високий ступінь наближення істинного значення певного параметра); *5) оперативність* (здатність коректно і швидко виконувати розрахунки); *6) інформаційна складова* (врахування особливостей побудови інформаційних систем та мереж, архітектури кіберпростору [13]); *7) об'єктивність* (можливість повністю незалежного оцінювання).

Таблиця 1

Аналіз підходів до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури за базовими критеріями

№ з/п	Назва підходу	Базові критерії						
		1	*2*	*3*	*4*	*5*	*6*	*7*
1.	Теорія К. Клаузевіца для мережевих архітектур	+	-	-	-	-	-	-
2.	Теорія самоорганізуючих мереж А. Барабаши	+	+	-	+	-	-	-
3.	Теорія графів	+	-	+	+	-	-	+
4.	Модель пріоритетності активів	-	+	-	-	-	-	-
5.	Ідентифікація на основі категоріювання	+	-	+	+	-	-	-
6.1	Система моделювання критичних інфраструктур	+	-	+	+	+	-	+
6.2	Імітаційна модель «Афіна»	+	-	+	+	+	-	+

Багатокритеріальний аналіз зазначених підходів показав (див. табл. 1), що найбільш вдалими (з точки зору застосування для КІІ) є підходи, що базуються на теорії графів та імітаційному моделюванні (система моделювання критичних інфраструктур та імітаційна модель «Афіна»), які як і багато інших підходів базуються на теорії графів. Крім того, широко використовуються знання теорії самоорганізованих мереж математика А. Барабаши та ідентифікація об'єктів критичної інфраструктури на основі категоріювання – деякі аспекти цих підходів теж можуть бути використані для об'єктів КІІ. Проте, варто також зазначити, що загальні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури в основному орієнтовані на економічні, екологічні, техногенні та інші системи безпеки держави, не враховують повної множини параметрів і особливостей інформаційних інфраструктур.

Висновки

Таким чином, в даній роботі проведено багатокритеріальний аналіз підходів до виявлення критично важливих об'єктів інфраструктури для оцінювання їх можливостей щодо виявлення та ідентифікації найбільш важливих об'єктів КІІ. Для цього було використано такі базові критерії: ясність формалізації, простота реалізації, гнучкість та універсальність, точність, оперативність, інформаційна складова та об'єктивність. Встановлено, що відомі підходи орієнтовані, як правило, на економічні, екологічні, техногенні та інші системи безпеки держави, переважна їх більшість не враховує повної множини параметрів і особливостей КІІ (інформаційної складової). Крім того, за результатами аналізу стало зрозуміло, що для КІІ ймовірно найбільш ефективними є підходи, що базуються на теорії графів та імітаційному моделюванні.

У подальших дослідженнях, з урахуванням результатів цієї роботи, планується розроблення універсального методу ідентифікації об'єктів критичної інфраструктури, що буде враховувати особливості інформаційної складової і дозволить оцінювати рівень критичності елементів КІІ.

Література

[1] Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д.С. Бірюков, С.І. Кондратов. — К. : НІСД, 2012. — 96 с.

[2] Keating C, Rogers R., Unal R., Dryer D., Safford R., Peterson W., Rabadi G. System of Systems Engineerings // Engineering Management Journal, Vol. 15, № 3, 2003. — p. 36-45.

[3] Jackson M.C. Systems Methodology for the Management Sciences // New York: Plenum, 1991. — 81 p.

[4] Лядовська В.М. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів / В.М. Лядовська, М.О. Рябий, С.О. Гнатюк // Зв'язок. — 2014. — №4. — С. 3-7.

[5] Clausewitz C.-V.. On War // Swedish translation by Mertensson, Buhme och Johansson. Stockholm, Sweden: Bonnier Fakta Bokfurlag. 1991. — p. 1832.

[6] Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // Зарубежное военное обозрение. — 2012. — №1. − С. 19-30.

[7] Курносов Ю.В., Конотопов П.Ю. Аналитика. Методология, технология и организация информационно-аналитической работы. —М., 2004. — 135 с.

[8] Пугачева Е.Г. Идеи теории сложных систем и их применение в экономике // Проблеми системного підходу в економіці: Збірник наукових праць: Вип. 31. — К.: НАУ, 2009. — С. 36-45.

[9] КВИС — критически важные информационные сегменты [Электр. ресурс]. — Режим доступа: http://security-corp.org/administration/network_technologies/4580-kvis-kriticheski-vazhnye-informacionnye-segmenty.html.

[10] Стиславский А.Б. Построение методологии обеспечения транспортной безопасности на основе категорирования // Вісник Національного університету водного господарства та природокористування. — Рівне: НУВГП, Зб. наук.пр. — Ч.2. — № 3 (47), 2009. — С. 155-165.

[11] Братушка С.М. Імітаційне моделювання як інструмент дослідження складних економічних систем / С. М. Братушка // Наук. вісн. НЛТУ України. — 2009. — № 8. — С. 22-28.

[12] Dudenhoeffer D., Permann M., Manic M. CIMS: a framework for infrastructure interdependency modeling and analysis // Proceedings of the Winter Simulation Conference WSC 2006, Monterey,California, USA. — p. 478-485.

[13] Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. — Том 19, №2. — 2013. — С. 118-129.

УДК 004.056.5 (045)

Гнатюк С.А., Сидоренко В.М., Дуксенко О.П. Современные подходы к выявлению и идентификации наиболее важных объектов критической инфраструктуры

Аннотация. *Современные тенденции развития информационных технологий вызвали феноменальную зависимость общества от услуг, которые предоставляют различные области инфраструктуры. Сейчас, качество и доступность таких услуг является одним из главных показателей развития инфраструктуры государства, а обеспечение их защиты и стабильного функционирования является важной и обязательной составляющей национальной безопасности развитых стран. Увеличение концентрации средств и ресурсов для защиты электронных инфраструктур различных типов обусловило необходимость ранжирования инфраструктурных объектов, выделения важнейших из них и появлению понятия критическая инфраструктура. Учитывая это, в работе проведено многокритериальный анализ подходов к выявлению критически важных объектов для оценки их возможностей по выявлению и идентификации наиболее важных объектов критической информационной инфраструктуры. Установлено, что наиболее эффективными для информационной инфраструктуры являются подходы, основанные на теории графов и имитационном моделировании, однако большинство существующих подходов не учитывают полного множества параметров и информационной составляющей – это обуславливает необходимость разработки универсального метода идентификации объектов критической информационной инфраструктуры.*

Ключевые слова: *информационная безопасность государства, критическая инфраструктура, идентификация, оценка уровня критичности, критическая информационная инфраструктура, защита объектов критической информационной инфраструктуры.*

Gnatyuk S., Sydorenko V., Duksenko O. Modern approaches to critical infrastructure objects detection and identification

Abstract. *Modern trends in information technologies led phenomenal dependence on public services, which provide by different spheres of infrastructure. Today, quality and accessibility of services is one of the main indicators of the state infrastructure level, and ensure their security and stable operation is an essential and indispensable part of the national security of developed countries. Increased concentrations of tools and resources to secure various types of electronic infrastructure necessitated ranking of infrastructure facilities, the allocation of the most important ones and the emergence of the concept of critical infrastructure. In view of this, in the paper the multi criteria analysis of approaches was carried out to identify critical facilities to assess their capacity to detect and identify the most important objects of critical information infrastructure. It was established that the most effective information infrastructure approaches are based on graph theory and simulation, but most existing approaches do not take into account the full set of parameters and information component. That's why the development of a universal method for critical information infrastructure identification is necessary.*

Key words: *information security of the state, critical infrastructure, identification, criticality level evaluation, critical information infrastructure, critical information infrastructure protection.*

Отримано *16 вересня 2015 року*, затверджено редколегією *12 жовтня 2015 року*