В законодавстві більшості країн колишнього СРСР (Російська Федерація, Республіка Білорусь, Республіка Казахстан, Туркменістан, Киргизька Республіка) нормативна термінологія інституту державної таємниці в питанні забезпечення безпеки спирається на захист державної таємниці. Правовий інститут державної таємниці в законодавстві України має самобутні риси і в термінологічному плані спирається не на захист, а на охорону державної таємниці. Тим самим, на мій погляд, підкреслюється головна ідея правового інституту державної таємниці в Україні – забезпечення реалізації прав окремих осіб стосовно інформаційних об'єктів, що становлять державну таємницю. Коли в законодавчій термінології акцент робиться на захист, то це, на мій погляд, свідчить перш за все про намагання законодавця ввести в правове поле виконавчий механізм протидії деяким загрозам об'єкту правової охорони і тим самим побічно підкреслити значимість цих загроз у житті суспільства або щодо його безпеки.

Запропоноване тлумачення понять "захист" і "охорона", визначення однойменних термінів в сфері забезпечення безпеки інформаційного об'єкта дозволить розрізняти їх зміст і може бути використано під час розробки науково-теоретичного підґрунтя правового регулювання в сфері забезпечення безпеки об'єктів, а також для подальшого вдосконалення тлумачення понять "охорона" та "захист" у різноманітних сферах суспільних відносин.

Література: ***1.*** *ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.* ***2.*** *ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006. – 56 с.* ***3.*** *ISO/IEC 17799:2005 Information technology – Security technologies – Code of practice for information security management. – ISO/IEC, 2005. – 115 p.* ***4.*** *Закон України "Про державну таємницю" // Відомості Верховної Ради України, 1994, № 16. – ст. 93.* ***5.*** *Закон України "Про Службу безпеки України" // Відомості Верховної Ради України, 1992, № 27. – ст. 382.* ***6.*** *Закон України "Про контррозвідувальну діяльність" // Відомості Верховної Ради України, 2003, № 12. – ст. 89.* ***7.*** *Закон України "Про розвідувальні органи України" // Відомості Верховної Ради України, 2001, № 19. – ст. 94.* ***8.*** *Закон України "Про Національний архівний фонд та архівні установи" // Відомості Верховної Ради України, 1994, № 15. – ст. 96.* ***9.*** *Закон України "Про охорону земель" // Відомості Верховної Ради України, 2003, № 39. – ст. 349.* ***10.*** *Закон України "Про державний кордон України" // Відомості Верховної Ради України, 1992, № 2. – ст. 5.* ***11.*** *Закон України "Про охорону культурної спадщини" // Відомості Верховної Ради України, 2000, № 39. – ст. 333.* ***12.*** *Закон України "Про благоустрій населених пунктів" // Відомості Верховної Ради України, 2005, № 49. – ст. 517.* ***13.*** *Правила організації охорони повітряних суден та об'єктів на авіапідприємствах цивільної авіації України. – Затверджено наказом Державної служби України з нагляду за забезпеченням безпеки авіації від 30.03.2005 № 230.* ***14.*** *Лісовий кодекс України // Відомості Верховної Ради України, 1994, № 17. – ст. 99.* ***15.*** *Тлумачний словник української мови: Понад 12500 статей (близько 40000 слів) / За ред. д-ра філологічних наук проф. В. С. Калашника. – 2-ге вид., випр. і доп. – Х.: Прапор, 2004. – 992 с.* ***16.*** *Шлапаченко В. М. Контррозвідувальна діяльність органів Служби безпеки України – основна складова системи збереження державної таємниці // Збірник наукових праць Національної академії Служби безпеки України, 2003, № 8. – С. 82-85.* ***17.*** *Ожегов С. И. Словарь русского языка. – М.: Государственное издательство иностранных и национальных словарей, 1961. – 900 с.* ***18.*** *Архипов О. Є., Бородавко І. Т., Ворожко В. П. Оцінювання ефективності системи охорони державної таємниці: Монографія. – К.: Наук.-вид. відділ Національної академії Служби безпеки України, 2007. – 63 с.*

УДК 681.5;321;322:621.391;395

ПЕРКОЛЯЦІЙНІ МОДЕЛІ ПРОТИДІЇ ФУНКЦІОНУВАННЮ НЕСАНКЦІОНОВАНОЇ НАНОСЕНСОРНОЇ МЕРЕЖІ

Ірина Кононович

Інститут комп'ютерних технологій Одеської державної академії холоду

Анотація: **Формулюється й аналізується задача організації протидії функціонуванню несанкціонованої розподіленої мережі наносенсорів із самоорганізацією. Розробляється математична модель системи протидії із залученням методів теорії перколяції. Інтерпретуються результати комп'ютерного моделювання.**

Summary: **The task of organization of counteraction to functioning of the unauthorized distributed network of nanosensors with self organization is formulated and is analyzed. The mathematical model of the system of counteraction with bringing in of methods of theory of percolation is developed. The results of computer design are interpreted.**

Ключові слова: **Інформаційна безпека, наноелектроніка, сенсори, сенсорні мережі, теорія перколяції, самоорганізація, моделювання.**

І Вступ

Дана робота стосується сфери досліджень інформаційної безпеки об'єктів інформаційної діяльності в умовах розвитку нанотехнологій та самоорганізації мереж збору й обробки інформації.

Розглядаються й аналізуються проблеми організації протидії функціонуванню мереж наносенсорів, які виконують функції несанкціонованого контролю, управління, збору й обробки інформації.

Стану проблеми інформаційної безпеки за умов розвитку нанотехніки, наноелектроніки, нанокомп'ютерів та інформаційних наносистем присвячена значна кількість робіт у засобах масової інформації й наукових виданнях. Одними з перших в Україні цю проблему освітили харківські вчені [1, с 263 - 272]. *Нанотехнологія* – це наука й технологія управління речовиною у масштабі нанометрів, тобто на рівні молекул і атомів, та технологія виробництва, орієнтованого на дешеве отримання пристроїв та речовин із наперед заданою атомарною структурою. Наноіндустрія створює принципово нову матеріальну базу, нові можливості в телекомунікаціях – нові транзистори, в медицині – нові ліки та обладнання, в енергетиці – нові сонячні батареї, в збройних силах – нові види озброєння, в боротьбі з тероризмом – нові пристрої спостереження, в екології – нові очисні споруди, вона матиме вирішальний вплив на світову енергосистему, економіку, політику, соціальну сферу. Нанотехнології можуть стати причиною серйозних конфліктів, зокрема, збройних та викликати протистояння в сфері інформаційної безпеки на всіх рівнях від національного до технічного і навіть персонального. Вже створюються машини, здатні виконувати необхідні операції з атомами. Закладаються основи атомної та молекулярної збірки та само збірки для використання у електроніці, телекомунікаціях, оптиці, робототехніці. Пройшло випробування в Афганістані системи Smart dust («розумний» пил) військового призначення. Ведуться роботи зі створення «малопотужної» ядерної зброї з використанням елементів нанотехнологій, нано- та пікосупутників. При нанотехнологіях контроль практично неможливий, у крайньому разі, поки що проблематичний [2].

Бурхливий розвиток нанотехнологій забезпечується успіхами наноелектроніки та спінтроніки, наномеханіки, нановимірювань тощо [3, 4]. У найближчому майбутньому можуть бути створені наноелектромеханічні системи, в яких може бути реалізовано керований рух нанооб'єктів. Такі нанопристрої, як нанотранзистори, нанодіоди, наномодулятори струму, нанореле й наноосцилятори з частотою роботи до 400 ГГц, вимагають для своєї роботи мізерної енергії.

Сучасні сенсорні мережі впроваджуються в сферах охорони здоров'я, екологічного моніторингу, управління виробничим процесом, автомобільним рухом, при надзвичайних ситуаціях, у сільському господарстві, військовій сфері [5]. Можливі зміни в хімічному синтезі, енергетиці, науці про матеріали, космічних дослідженнях. Стала актуальною проблема створення обчислювальних машин на нанорівні та молекулярних обчислювальних машин [6]. За словами Президента Російської Федерації В. В. Путіна: «Нанотехнологія, безумовно, буде ключовою галуззю для створення надсучасного та над ефективного як наступального, так і оборонного озброєння». В [7] стверджується, що головна перевага наноозброї в тому, що проти нього нема іншого захисту, окрім нанозахисту.

Нанотехнології проходять лише початковий етап свого розвитку. На просунутих етапах можна очікувати створення еволюціонуючих об'єктів, здатних видозмінювати та коригувати свою структуру. Молекулярні машини можуть оцінювати ситуацію, виробляти рішення і діяти у відповідності з ним. Цікавим може бути новий напрям синергетики – штучного життя [8]. Можна синтезувати або модифікувати нанооб'єкти, здатні еволюціонувати і вирішувати свою задачу протягом багатьох поколінь.

Прогнозуються успіхи в створенні мікро-роботів та молекулярних машин. Відмічається інтерес до прикладної задачі створення ансамблю мікро-роботів, які виконують колективні узгоджені дії [9]. Це вже, свого роду, мережа мікро-роботів, коли сенсор замінюється мікро- або нанороботом. Робототехніка зараз є розвинутою областю. При переході на наномасштаби приділяється увага наномашинам та нанорозмірним датчикам. Можливе створення наномашин на зразок виявлених у середині клітини природних «молекулярних двигунів» – природних наномашин [6, 10]. Прогнозується створення гібридних наномеханічних об'єктів на основі біологічних систем та неорганічних пристроїв. При цьому технологія для створення деструктивних нанороботів здається значно простішою, ніж технологія створення ефективного захисту від такої атаки (глобальної нанотехнологічної імунної системи, «активного щита» [1, с. 268; 11]).

Загальною рисою нанотехнологій є високий ступінь інтеграції в багатьох сферах людської діяльності, а значить інформаційною вразливістю та загрозами. Не всі прогнози з даного огляду можуть бути здійснені на практиці, але нові загрози й проблеми безпеки стають ключовими для забезпечення ефективної діяльності особи, суспільства і держави. При цьому саме випереджаюче вирішення задач забезпечення інформаційної безпеки в застосуваннях сенсорних та наносенсорних мереж є актуальним.

Мета роботи: розробка й дослідження моделей протидії функціонуванню наносенсорної мережі збору, передачі й обробки інформації для вироблення стратегії та методів забезпечення інформаційної безпеки об'єктів інформаційної діяльності. Модель названа перколяційною внаслідок застосування методів теорії перколяції для опису властивостей та поведінки системи протидії.

II Класифікація та огляд стану наносенсорних мереж

Розглянемо параметри наносенсорних мереж, які можуть мати відношення до їхнього моделювання.

Наносенсорною мережею будемо називати сенсорну мережу, яка реалізована за допомогою наносенсорних пристроїв. Сенсорними називають розподілені безпроводні мережі, які складаються з маленьких (за розмірами) вузлів (сенсорів), з інтегрованими функціями моніторингу навколишнього середовища, обробки й передавання даних [5]. Сенсорні пристрої складаються з датчиків для контролю і реєстрації параметрів зовнішнього середовища, мікрокомп'ютера, джерела живлення та приймача-передавача. Сенсорні пристрої проводять вимірювання й первинну обробку даних, а також підтримують інформаційний обмін із зовнішніми інформаційними системами. Радіоприймач-передавач має потужність меншу за 10 мВт. Джерело живлення має функціонувати протягом декількох років.

На сьогодні сенсорні мережі класифікують за ознаками мобільності (стаціонарні та рухомі), за організацією (децентралізовані, ієрархічні або гібридні), за середовищем моніторингу (наземні, підземні, морські, повітряні), за параметрами моніторингу та за сферою застосування. В однорідній сенсорній мережі однотипні сенсори виконують розподілену обробку даних. Інформація передається методом комутації пакетів з використанням багаторазових трансляцій. Кожен вузол мережі є маршрутизаторм. Дальність зв'язку одного сенсора складає сотні метрів. Але мережа може забезпечити велике покриття завдяки багаторазовій маршрутизації.

Один чи декілька сенсорів мають доступ до зовнішнього шлюзу і через нього до інших мереж. В ієрархічній мережі різнотипні сенсори передають дані до потужних головних вузлів, які виконують централізовану обробку даних.

Розмірність сучасних сенсорних мереж складає сотні і тисячі залежно від сфери застосування. Розмірність мереж буде безперервно збільшуватись. Швидкість передавання сучасних сенсорів становить 250 кбіт/с, але пропускна здатність має зрости на порядок і більше.

Сенсори створюють мережу методом самоорганізації. При включенні сенсора він автоматично виявляє інші сенсори, з'ясовує свою роль у мережі і пристосовується до обробки потрібної інформації з навколишнього середовища. Розгорнена сенсорна мережа самостійно прокладає маршрути обміну інформацією і, при необхідності, коригує їх згідно зі змінами в мережі. У сенсорній мережі відсутнє центральне керування пристроями. Мережа може адаптуватись до швидко змінюваних параметрів навколишнього середовища.

Розробка методів забезпечення інформаційної безпеки утруднена тим, що наявні технічні та архітектурні рішення не є остаточними. В публікаціях [4] виділено, що будуть розроблятись: архітектура для спільної, розподіленої та обмеженої ресурсом обробки даних, яка об'єднувала б усі технічні вимоги в одній інфраструктурі; методи фільтрації й відбору важливої інформації, зменшення передавання зайвої інформації, узагальнення даних, отриманих із різних джерел, різними засобами зв'язку; методи збільшення пропускної спроможності радіоканалу; методи встановлення наявності сусідніх вузлів, їх напрямків та місцезнаходження; міжмережні інтерфейси для віддаленого доступу до сенсорних мереж з Інтернету.

Також будуть розвиватись методи та засоби забезпечення фізичної та інформаційної безпеки сенсорних мереж, їх надійності та живучості. Слід очікувати, що на канальному рівні будуть застосовані специфічні засоби автентифікації та шифрування, на мережному та транспортному рівні будуть розроблені ефективні і безпечні методи маршрутизації та протоколи.

III Стратегії протидії функціонуванню наносенсорної мережі

У випадку нанотехнологій поставлена мета полягає у розвитку засобів захисту до появи наступальних технологій. Але заданий рівень наступальної технології зазвичай вимагає набагато менше зусиль, ніж технологія, яка може захистити від нього. Це приводить до значної переваги нападаючої сторони. [1, с. 267; 12, с. 17]. Наступ перевершував оборону протягом більшої частини людської історії. Часто захист забезпечувався не обороною, а завдяки балансу загроз нападу. Вказаний фактор спрямовує пошуки на розробку контр-наносенсорної мережі, яка побудована на тих же принципах, що й нападаюча мережа.

Нехай маємо несанкціоновану наносенсорну інформаційну мережу із самоорганізацією. Пересування наносенсорів обмежене лише безпосередньо близькою зоною навколо кожного з них. Кожен наносенсор здійснює інформаційний обмін лише з найближче розташованими сусідніми наносенсорами. Об'єкт

інформаційної діяльності, що захищається, та його контрольована зона повністю покривається центральною частиною несанкціонованої наносенсорної мережі, яка пролягає далеко за межі контрольованої зони. Виявлення як окремого, так і всіх наносенсорів є надто трудоємним завданням. Зв'язок наносенсоної мережі із цільовою системою несанкціонованої обробки інформації здійснюється з периферійних наносенсорів, перехоплення інформаційного обміну яких є проблематичним. Задача, в даному випадку, зводиться до запобігання правильному функціонуванню несанкціонованої наносенсорної мережі як в межах, так і на підступах до контрольованої зони об'єкта.

Можна запропонувати декілька способів протидії функціонуванню несанкціонованої сенсорної мережі.

1. Оточення кожного сенсора контр-сенсорами, які порушили б структуру мережі блокуванням зв'язку сенсора з іншими елементами мережі. Недолік такого способу полягає у необхідності виявлення сенсорів і у великій кількості контр-сенсорів навколо кожного з несанкціонованих сенсорів.

2. «Кругова оборона» об'єкта шляхом створення кільця контр-сенсорів, які ізолюють частину сенсорної мережі, розташовану в контрольованій зоні, або ззовні, безпосередньо поблизу неї. Контр-сенсор може використовувати зашумлення ефіру або перехоплення чи підміну інформаційного обміну між сенсорами, якщо можна вирішити проблеми розшифрування інформації та проблему «свій-чужий». Недолік цього способу полягає у його низькій стійкості. Стійкість кільця контр-сенсорів визначається найменш стійким його елементом. Кільце повинне мати певну товщину для гарантій захищеності об'єкта. Крім того, повністю не виключається можливість роботи сенсорів в середині кільця. В принципі об'єкт має бути накритий сферичною поверхнею, створеною контр-сенсорами.

3. Перспективним може бути спосіб створення стохастичної самоорганізованої контр-мережі, коли контр-сенсори рівномірно розсіюються в зоні та поблизу об'єкта, який захищається. Саме аналізу цього способу протидії присвячується дана робота. Необхідно знайти, при якій концентрації випадково й рівномірно розташованих контр-сенсорів функціонування несанкціонованої сенсорної мережі може буде порушено. Функціонування несанкціонованої сенсорної мережі можна вважати порушеним, якщо кластери контр-сенсорів утворюють безперервні ланцюги між граничними елементами несанкціонованої мережі. У цьому випадку несанкціонована мережа розпадається на незв'язані сегменти і несанкціонований інформаційний обмін не досягає граничних елементів, з яких здійснюється зв'язок з глобальною мережею.

Для аналізу такої задачі можна застосувати методи теорії перколяції (інша назва – теорія протікання, від англійського – percolation). Теорія перколяції займається зв'язністю дуже великого числа елементів при умові, що зв'язок кожного елемента із своїми сусідами носить випадковий характер, але задається цілком певним способом. Одне з основних питань теорії перколяції – при якій концентрації домішуваних елементів виникає ланцюг цих елементів, який з'єднує периферійні точки мережі. Таку критичну концентрацію домішок називають *порогом перколяції* [13], а явища, які описуються теорією протікання, відносяться до так званих «критичних явищ». Фізика усіх критичних явищ має спільні риси в тому, що поблизу критичної точки система якби розпадається на окремі блоки, причому розміри окремих блоків необмежено ростуть при наближенні до критичної точки. Дана задача еквівалентна задачі про домішки в ізоляторах, які перетворюють їх у провідники. При виникненні ланцюга з домішок властивості ізолятора стрибком змінюються, він стає провідником.

В системі інформаційної безпеки можна вирішувати пряму і зворотну задачу. У даному випадку пряма задача: є несанкціонована сенсорна мережа (з чорними вузлами), треба створити контр-мережу (домішуючи білі вузли чи заміщуючи ними чорні вузли) й знайти, при якій концентрації контр-сенсорів буде досягнуто порогу перколяції. Зворотна задача: є захищена сенсорна мережа, треба створити нападаючу несанкціоновану сенсорну мережу і визначити поріг перколяції, при якому долається захисна мережа.

Процеси протікання докладно вивчені для багатьох варіантів решітчастої задачі. Для простоти вивчимо поставлену задачу у двомірному просторі (на площині). Розглянемо нескінченну квадратну решітку, що математично описується нескінченним регулярним графом. Точки перетину ліній (вершини графа) будуть вузлами, де розташовані сенсори несанкціонованої мережі. Самі лінії (ребра графу) є зв'язками, що відображають інформаційний обмін між вузлами. Будемо шукати, яку частку зв'язків, або яку частку вузлів треба блокувати контр-сенсорами, щоб решітка розпалась. Тоді маємо задачу зв'язків, або задачу вузлів. Контр-сенсори утворюють кластери певного розміру. Нижче порогу перколяції є кластери лише скінченного розміру. Вище порогу перколяції утворюються також перколяційні або нескінченні кластери, які з'єднують дві протилежні сторони системи. Середнє число вузлів, які належать нескінченному кластеру, поблизу перколяційного порогу описується показовою функцією

$$S(p) = \left| p - p_c \right|^{-\gamma}, \qquad (1)$$

де p – концентрація (доля) контр-сенсорів;

p_c – поріг перколяції;
γ – критичний показник.

На рис. 1 показано фрагмент квадратної матриці. Світлими кружками показані вузли несанкціонованої сенсорної мережі. Лініями між вузлами показані зв'язки між сусідніми сенсорами. Чорним кружком показаний контр-сенсор. Для спрощення, сусідні сенсори вважаються зв'язаними по вертикалі й горизонталі, але не по діагоналі. Якщо наявність контр-сервера у даній комірці приводить до розриву одного зв'язку між вузлами, то за термінологією теорії перколяції маємо задачу зв'язків. А якщо наявність контр-сервера приводить до блокування роботи вузла, то маємо задачу вузлів. Вибір типу задачі залежить від характеру взаємодії контр-сенсорів з несанкціонованими сенсорами; вибір може бути проведено, коли будуть відомі їх конкретні тактико-технічні характеристики.

IV Алгоритми та результати моделювання

Багато задач теорії перколяції вирішено аналітичними методами. Але основними методами в теорії перколяції є вивчення процесів шляхом моделювання методом Монте-Карло, зокрема алгоритм багаторазового маркування кластерів Хошена–Копельмана [14, с. 109 - 112]. Розглянемо роботу алгоритму на прикладі задачі розриву зв'язків на квадратній решітці.

Ідея алгоритму полягає в тому, що всім занятим (розірваним) зв'язкам решітки присвоюються різні кластерні мітки. Моделювати решітку буде масив a розміром $L \times L$. До масиву додамо рядок з номером 0 та стовбець з номером 0, які заповнені нулями. Створимо, також, масив кластерних міток c. Початкові значення елементів цього масиву співпадають з їх номерами. Якщо при змінах значення елемента масиву стало менше його номера, таку кластерну мітку називають неправильною.

Нехай зв'язки решітки розірвані з ймовірністю p. Будемо генерувати випадкові числа ξ, рівномірно розподілені на інтервалі [0, 1]. Якщо генероване число $\xi \le p$, то поточному елементові масиву a присвоюємо значення 1, інакше – 0. Починаємо переглядати послідовно всі елементи масиву, починаючи з елементу $a[1, 1]$. Нульовий стовпчик пропускаємо. Можливі такі ситуації.

1. Якщо значення поточного елемента масиву дорівнює 0, то переходимо до наступного елемента.

2. Якщо поточне значення дорівнює 1, то здійснюємо наступну перевірку:

- якщо сусід зліва $a[i, j - 1]$ та сусід зверху $a[i - 1, j]$ мають значення 0, то приймаємо робочу гіпотезу, що даний елемент входить до нового кластера і присвоюємо поточному елементові номер чергової кластерної мітки; чи є цей кластер новим – буде перевірено після перегляду усього масиву;

- якщо сусід зверху має значення щ, а сусід зліва не дорівнює нулю, то поточний елемент та її сусід зліва належать одному й тому ж кластеру; поточному елементові присвоюємо номер кластерної мітки сусіда зліва;

- якщо сусід зверху має значення, відмінне від нуля, а сусід зліва має нульове значення, то поточний елемент та її сусід зверху належить одному й тому ж кластеру; на цьому кроці перевіряємо правильність кластерної мітки; якщо кластерна мітка неправильна, то було злиття кластерів; тому поточному елементу слід присвоїти номер правильної кластерної мітки сусіда зверху;

- якщо сусід зверху та сусід зліва мають ненульові значення, то всі три елемента належать до одного кластера; поточному елементові присвоюємо найменший з номерів правильних кластерних міток сусіда зверху та сусіда зліва; коригуємо масив кластерних міток; для цього в елемент масиву c, який відповідає більшій з кластерних міток, заносимо номер правильної кластерної мітки.

Отримане при моделюванні значення порогу перколяції для решітки скінчених розмірів екстраполюють до нескінченності. Результат одного з прогонів моделі представлено на рис. 2. Для квадратної решітки розмірами 200 x 200 показано кластер контр-сенсорів, що утворився при досягненні поточного кластерного порогу перколяції величиною 0, 45. Видно, що кластер приводить до розпаду системи на незв'язані частини.

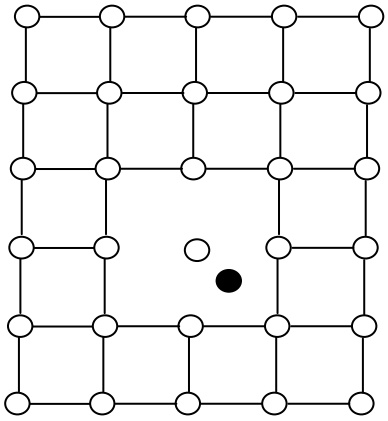

Рисунок 1 – Квадратна решітка як модель сенсорної мережі

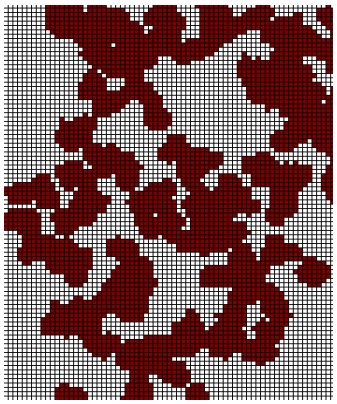

Рисунок 2 – Зразок кластера взаємодіючих контр-сенсорів

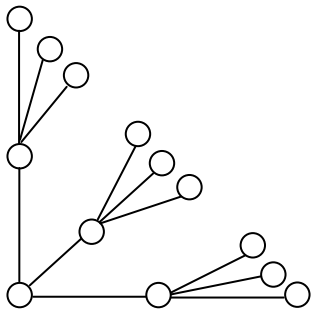

Рисунок 3 – Модель решітки Бете

В результаті моделювання можна побудувати залежність ймовірності виникнення протікання від концентрації. Точка, яка відповідає ймовірності 50%, є порогом перколяції.

V Інтерпретація відомих результатів моделювання

Окремі задачі теорії перколяції вирішено аналітичними методами, більшість їх – натурним чи математичним моделюванням. Скористуємось результатами, викладеними в класичній [13] та інших роботах, інтерпретуючи їх до проблеми вивчення поведінки контр-сенсорних мереж.

1. Одна з натурних моделей задачі вузлів була створена Ватсоном та Лисом [13, с. 9] за допомогою екрануючої металевої сітки розмірами 137 х 137 = 18769 вузлів. Сітка включалась у електричний ланцюг і вимірювався її електричний опір. Далі окремі вузли блокувались (вибрані випадковим чином вузли сітки вирізались) і вивчалась залежність електричного опору сітки від долі блокованих вузлів x. Доля блокованих вузлів є відношенням числа блокованих вузлів до загального числу вузлів. Значення x, при якому перерізується останній шлях від одного краю сітки до іншого й електричний опір зростає до нескінченості є порогом протікання, який позначимо як x_c. Було знайдено, що $x_c = 0{,}69 \pm 0{,}01$.

У нашому випадку це означає, що якщо один контр-сенсор блокує один випадковий несанкціонований сенсор, то несанкціонована мережа починає розпадатись, коли математичне очікування долі блокованих вузлів $x > 0{,}69$. При збільшенні розмірів мережі випадкова величина

$$x_c = \lim_{N \to \infty} x_c(N), \tag{2}$$

де N – розмір сітки, стає достовірною.

2. Задача електропровідності екранної сітки була узагальнена для випадку тривимірного кубу [13, с. 56]. У кубічній решітці кожен вузол зв'язаний із шістьма сусідніми вузлами. Критична концентрація блокованих вузлів, при якій виникає нескінченний кластер контр-серверів є одночасно порогом протікання. Для простої кубічної решітки знайдено , що $x_c = 0{,}31$.

3. Задача зв'язків вирішувалась як задача насадження фруктового саду для випадків квадратної (К), трикутної (Т) та шестикутної (Ш) решіток [13, с. 87 – 102]. Зв'язок між деревами трактувався так, що вони вважаються зв'язаними, якщо одне дерево захворіло, то обов'язково заражує сусіднє. Два довільних вузла вважаються зв'язаними, якщо між ними є цілий нерозірваний зв'язок, або вони зв'язані ланцюгом нерозірваних зв'язків між сусідніми вузлами. Сукупність зв'язаних вузлів називають кластером. В нашому випадку, кластером буде сукупність зв'язків між сенсорами, роботу яких заблоковано. Важливою властивістю кластера є те, що його контр-сенсори блокують всі зв'язки кластера і не блокують жодного за його межами. В задачі зв'язків пороги протікання $x_{зв}$ відрізняється від порогу протікання $x_в$ задачі вузлів. В задачі вузлів блокується відразу вузол з усіма його зв'язками, а в задачі зв'язків блокуються лише один і зв'язків вузла.

Задача зв'язків на квадратній решітці має аналітичне рішення: величина порогу протікання $x_{зв}(K) = 0{,}5$. Доведено, що для будь-якої решітки, не лише плоскої, порогові значення для задачі зв'язків не більше ніж для задачі вузлів, $1 - x_в \le 1 - x_{зв}$. Це означає, що блокуючи вузли легше заблокувати несанкціоновану сенсорну мережу, ніж розриваючи зв'язки.

4. За допомогою цікавого методу покриваючих та включаючих решіток було доведено, що величина порогу протікання залежить від типу решіток, як показано в таблиці.

Тип решітки	Величина порогу протікання	
	в задачі вузлів – $x_в$	в задачі зв'язків – $x_{зв}$
Трикутна	0,3473	0,5
Квадратна	0,5	0,59
Шестикутна	0,6527	0,70

Величина порогу протікання в задачі вузлів для квадратної та шестикутної решітки визначені за допомогою моделювання, остhttp://www.expert.ru/printissues/expert/2007/42/polchasa_mitoza/анні обчислені аналітично [13, с. 112].

5. Існують параметри задачі протікання, інваріантні типу решітки та справедливі для задач, заданих не на решітках. В задачах зв'язків таким параметром є добуток zx, де x – доля не блокованих зв'язків, а z – число найближчих сусідів кожного з вузлів. Цей добуток є універсальним, з похибкою до 10%, показником наявності протікання. Для плоских решіток справедлива формула [13, с. 126] $zx_{зв} = 2$, а для об'ємних решіток формула $zx_{зв} = 1{,}5$. Фізичний сенс універсальності добутку $zx_{зв}$ полягає в тому, що це середнє число цілих зв'язків на вузол у задачі зв'язків, потрібних для виникнення протікання. Поріг протікання значно менше залежить від інших властивостей решіток, приміром, від числа інших сусідів по віддаленості від даного вузла.

У задачі вузлів універсальним є інший параметр: протікання виникає, коли доля простору, зайнята не блокованими вузлами, перевищує деякий критичний параметр, який не залежить від типу решітки. Зайнятий простір навколо кожного з вузлів є куля, радіус якої дорівнює половині відстані між сусідніми вузлами, так, що ці кулі торкаються одна одної. Доля простору, яку займають кулі навколо блокованих вузлів, називають *коефіцієнтом заповнення – f*. Коефіцієнт заповнення дорівнює долі об'єму, який зайнятий кулями, побудованими навколо кожного з вузлів решітки та радіусом, що дорівнює половині відстані до найближчого сусіда. На порозі протікання, незалежно від типу решітки, величина $f\,x_в$ є однаковою для всіх типів решіток з точністю порядку 10 – 15%. Справедливі формули $f\,x_в \approx 0{,}5$ для плоских решіток і $f\,x_в \approx 0{,}16$ для об'ємних решіток [13, с. 131].

Остання формула підтверджена натурним моделюванням. Металеві та пластикові кульки засипаються невпорядковано у банку і вимірюється електропровідність. Протікання по металевим кулькам, що торкаються один одного, виникає, коли об'єм, який займають металеві кульки стає приблизно рівним 0,16 від повного об'єму. Цей результат слабо змінюється, якщо кульки мають різний радіус.

Для моделі несанкціонованої тримірної просторової сенсорної мережі це означає, що для блокування її роботи необхідно заблокувати не менше ніж 84% всіх сенсорів.

6. Вузли можуть мати зв'язки не тільки з сусідніми, а і з не сусідніми вузлами. Коли число вузлів, з якими зв'язано даний вузол, стає великим, задача вузлів стає задачею, яку називають задачею вузлів. Задача сфер відноситься до не решіточних задач. Випадкові елементи цієї задачі задані не на вузлах решітки. На площині задача формулюється наступним чином. Нехай на площині накреслені кола з однаковим радіусом, центри яких розподілені на площині хаотично й в середньому рівномірно. Координати центрів кіл є випадковими числами, рівномірно розподіленими в інтервалі від нуля до L, де L – це розмір системи. Кола можуть скільки завгодно перекривати один одного. Середнє число центрів кіл, яке припадає на одиницю площі є N, тобто N – є концентрацією центрів кіл. Кола вважаються зв'язаними, якщо центр одного кола належить іншому колу. Далекі один від одного кола можуть бути зв'язані через ланцюг таких охоплюючих кіл. Задача – знайти критичне значення концентрації N, при якому виникає протікання по охоплюючим колам, тобто виникають шляхи, які проходять через всю систему і складаються з охоплюючих кіл: виникає нескінченний кластер зв'язаних одне з одним кіл. Доведено, що наявність протікання залежить від середнього числа центрів кіл, які знаходяться в середині одного кола, $B = \pi NR^2$. Знайдено, що критичне значення B_c при якому виникає протікання, дорівнює $B_c = 4{,}1 \pm 0{,}4$ для плоскої задачі сфер і $B_c = 2{,}7 \pm 0{,}1$ для тривимірної задачі сфер [13, с. 141]. Таким чином, в задачі протидії несанкціонованій сенсорній мережі, знаючи радіус дії сенсора, можна знайти потрібну кількість контр-сенсорів. Слід наголосити, що результати вирішення такої задачі дуже слабо залежать від форми охоплюючої фігури.

7. Менш вивченою є поведінка параметрів систем безпосередньо поблизу порогу перколяції. Зокрема, функція $P(x)$ – ймовірність того, що деякий вузол належить до нескінченного кластера, на сьогодні невідома ні для плоских, ні для тривимірних задач. Наприклад, така функція могла б характеризувати, наскільки швидко несанкціонована мережа розпадається після досягнення порогу перколяції. Винятком є, так звана,

решітка Бете, показана вище на рис. 3 для випадку $q = 3$. Модель є графом типу «дерево», яке розгалужується в усі сторони. Для такої моделі знайдено алгебраїчне рівняння [13, с. 203]

$$\left[1 - P(x)\right]^q x + P(x) - x = 0. \tag{3}$$

При $q = 3$ маємо рішення

$$P(x) = \begin{cases} 0 & при \quad 0 < x < 0{,}5 \\ 2 - 1/x & при \quad 0{,}5 < x < 1 \end{cases}. \tag{4}$$

У загальному випадку порогом протікання буде $x_c = 1/q$. Аналогічним чином визначаються умови підтримання ланцюгової реакції ділення урану. Можна дійти якісного висновку, що поблизу порогу перколяції функція $P(x)$ зростає досить круто. Аналогічні висновки можна знайти при розгляді радіусів кореляції нескінченного кластера та гіпотези подібності [13, с. 222; с. 226].

VI Висновки

В роботі проведено огляд стану наносенсорних мереж, запропоновані методи протидії функціонуванню несанкціонованих наносенсорних мереж збору, передавання та обробки інформації, описана та проаналізована модель протидії, надані інтерпретації результатів моделювання перколяційних задач для опису поведінки сенсорних мереж.

Напрямком подальших досліджень можуть бути моделювання процесу перколяції на стохастичній мережі та вивчення поведінки моделей як статичних, так і динамічних сенсорних мереж з метою вироблення практичних рекомендацій для прямої задачі – протидії функціонуванню несанкціонованої мережі, та зворотної задачі – забезпечення високої готовності захисної мережі.

Література: ***1.*** *Поповский В. В., Персиков А. В. Защита информации в телекоммуникационных системах: Учебник: в 2 т. – Харьков: ООО «Компания СМИТ», 2006, М1. Т2 – 292 с.* ***2.*** *Ананян М. А. Наноиндустрия – вектор развития. http://spkurdyumov.narod.ru/ananyan77.htm – С. 9.* ***3.*** *Кононович И. В. Задачи энергетической и энергоинформационной безопасности общества и человека. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., 2007, – № 2(15), –39 – 46.* ***4.*** *Самардак А., Огнев А. Спинтроника: от «микро» к «нано» // Компьютера, № 5, 2006. (http://offline.computerra.ru/2006/625/251473). – С. 10.* ***5.*** *Міночкін А. І., Романюк В. А., Жук О. В. Перспективи розвитку сенсорних мереж // Зв'язок. – 2008. – № 1. – С. 16 - 21.* ***6.*** *Нанотехнология в ближайшем десятилетии. Прогноз направления исследований. /Под ред. М.К. Роко, Р.С. Уильямса и П. Аливисатоса. Пер. с англ. - М.: Мир, 2002 - 292с.* ***7.*** *http://www.newsru.com/russia/18apr2007/nanoputin.html.* ***8.*** *Бурцев М. С. Исследование новый типов самоорганизации и возникновения поведенческих стратегий. Автореферат диссертации на соискание ученой степени кандидата физико-математических наук. М. 2005 - ИПМ им. М. В. Келдыша РАН.* ***9.*** *Малинецкий Г. Г., Митин Н. А., Науменко С. А. Нанобиология и синергетика. Проблемы и идеи (Часть 2). Препринт № 2005_81. Москва 2008 – С. 23.* ***10.*** *Платонов А. К. Проблемы и перспективы робототехники. // Будущее прикладной математики. Лекции для молодых исследователей. М., УРСС, 2004, с. 315-342.* ***11.*** *Ник Бостром - Ph.D., is Director of Oxford University's new Future of Humanity Institute. Угрозы существования человечества. Анализ сценариев вымирания. (http://spkurdyumov.narod.ru/Bostrom1.htm).* ***12.*** *Юдковский Э. Искусственный интеллект как позитивный и негативный фактор глобального риска. Singulare Institute for Artificial Intelligence Palo Alto. // Перевод – Турчин А.В. 2006. – 20 с. (http://spkurdyumov.narod.ru/Yudkovskiy12.htm)* ***13.*** *Эфрос А. Л. Физика и геометрия беспорядка. (Библиотечка «Квант», вып. 19). – М.: Наука, гл. редакция физ.-мат. литературы, 1982. – С. 260.* ***14.*** *Тарасевич Ю. Ю. Математическое и компьютерное моделирование. Вводный курс: Учебное пособие – М.: Едиториал УРСС. 2004. – 152 с.*