КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.133144
УДК 004.94:519.21

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Спасітєлєва Світлана Олексіївна
кандидат фізико-математичних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

МАТЕМАТИЧНІ МЕТОДИ В КІБЕРБЕЗПЕЦІ: ГРАФИ ТА ЇХ ЗАСТОСУВАННЯ В ІНФОРМАЦІЙНІЙ ТА КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ

Анотація. Дана стаття присвячена проблемі застосування теорії графів в системах кібербезпеки та носить оглядовий характер. Широке проникнення математичних методів у розробку інформаційних технологій характеризує сучасний етап нашого суспільства. Серед математичних методів, що застосовують в інформаційній та кібернетичній безпеці, велику нішу складають графові технології. Стрункa система спеціальних термінів і позначень теорії графів дозволяє просто і доступно описувати складні і тонкі речі як геометрично, так і алгебраїчно. Граф є математичною моделлю найрізноманітніших об'єктів, явищ і зв'язків між ними. Цим і обґрунтовано вибір та актуальність даного дослідження. В статті викладено основні елементи теорії графів, широку сферу їх впровадження та проведено історичний ракурс розвитку цієї теорії. Аналіз наукових праць дозволив визначити основні напрями застосування властивостей, характеристик графів та графових алгоритмів в інформаційній та кібернетичній безпеці. Серед них виділено дослідження, пов'язані із застосуванням графів в інформаційних системах та у програмуванні; з моделюванням, аналізом та застосуванням графів атак; з криптографічними перетвореннями; з побудовою дерева рішень у задачах прийняття рішень в умовах ризику і невизначеності. Доведено, що уміння оперувати методами графових технологій сприяє розвитку програмних і технічних засобів захисту інформації. Розглянуті підходи до застосування теорії графів в інформаційній та кібернетичній безпеці можуть бути впроваджені під час вивчення дисципліни «Спеціальні методи в системах безпеки: дискретна математика» для студентів спеціальності 125 Кібербезпека, а також при підготовці фахівців у процесі науково-дослідної роботи або курсової чи дипломної роботи. Підвищуючи професійну спрямованість навчання, майбутні кібербезпечники отримують ґрунтовні знання фундаментальних дисциплін.

Ключові слова: математичні методи; кібербезпека; граф; граф атак; графові алгоритми; криптографія.

ВСТУП

Постановка проблеми. Математика, як вважає більшість науковців, – це мова науки. Тому є очевидним: якщо не існує математичного обґрунтування чи обчислення в даному дослідженні, то така діяльність не є науковою. Сучасна кібербезпека сформувалася у самостійний науковий напрям, який має свою специфіку постановок задач та технологій для їхнього дослідження, спираючись та реалізуючи математичні методи для аналізу інформації.

Попередньо у роботі [1] було здійснено огляд наукових досліджень щодо застосування фрактальної теорії в системах кібербезпеки. Продовжуємо серію таких напрацювань, виділивши, як окрему технологію, як засіб, як метод, теорію графів.

Аналіз останніх досліджень і публікацій. Найбільш значущі проблеми аналізу даних пов’язані з відношеннями, а не просто з розміром таблиці дискретних даних. Оскільки дані стають все більш взаємопов’язаними, взаємозалежними, а системи – все більш складнішими, то використання цих відношень стає пріоритетним у аналізі інформації. Графові технології та аналіз графів надають потужний інструмент для роботи з такими даними. У сучасному світі теорія графів є однією з найбільш актуальних та найефективніших серед математичних технологій, бо сфера її застосування міститься у різних областях діяльності людства, зокрема у інформаційній та кібернетичній безпеці. Аналіз наукової літератури (було опрацьовано біля 50 наукових джерел) засвідчує наявність глибокої зацікавленості вчених до проблеми використання графових технологій у кібербезпеці. Розгляд досліджень дав змогу констатувати наступні напрями застосування даної теорії в інформаційній та кібернетичній безпеці:

- в інформаційній системі та у програмуванні [2; 3];
- моделювання, аналіз та застосування графів атак [4 – 12];
- криптографічні перетворення за допомогою теорії графів [13 – 18];
- побудова дерева рішень у задачах прийняття рішень в умовах ризику і невизначеності [20].

Сучасний розвиток інформаційного суспільства безпосередньо пов'язаний з впровадженням інформаційних технологій у всі сфери життя. Збір, обробка і передача величезних обсягів інформації є неможливим процесом без комп’ютерної техніки. Інформація перетворилася в товар, як правило, значної вартості. Тому методи та засоби її захисту мають постійно удосконалюватися та розвиватися. А потенціалом для цього слугують математичні технології. Цим і підтверджується актуальність даного дослідження.

Мета статті. Метою даної статті є узагальнення, аналіз існуючих підходів до використання теорії графів в області захисту інформації та визначення шляхів подальшого використання графових технологій у даній сфері

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Графом називають сукупність об'єктів довільної природи (вершин) і зв'язок (ребер), які з'єднують деякі пари цих об'єктів. Теорія графів відноситься до скінченої геометрії. Стрункa система спеціальних термінів і позначень теорії графів дозволяють просто і

доступно описувати складні і тонкі речі. Особливо важлива наявність наочної графічної інтерпретації поняття графа. З геометричної точки зору граф – це геометрична фігура, яка складається з точок (вершин) і ліній (ребер), які їх з'єднують. З алгебраїчної точки зору графи можна представити спеціальними матрицями суміжності і списками суміжності.

Графи є чудовим засобом візуалізації – перетворення великих і складних видів абстрактної інформації в інтуїтивно-зрозумілу візуальну форму; вони дозволяють змоделювати інформацію у вигляді набору об’єктів і зв'язків між ними.

Засновником теорії графів як самостійного розділу математики вважають видатного швейцарського математика Л. Ейлера, який у 1736 році показово розв’язав "задачу про сім кенігсберзьких мостів". Свій внесок у розвиток теорії графів внесли німецький фізик Г. Кирхгоф, який у 1847 році розробив теорію дерев для вивчення електричних кіл; англійський математик А. Келі у 1858 році розвинув теорію дерев для вивчення практичних задач органічної хімії; угорський математик Д. Кеніг у 1936 році ввів термін «граф» і опублікував першу книгу з теорії графів. Системний виклад специфічних аспектів теорії графів можна знайти, наприклад, в роботах [21 – 23].

В залежності від видів вершин і/або ребер, які містять графи, а також від принципів побудови виділяють орієнтовані і неорієнтовані графи; графи з петлями, змішані графи, порожні графи, мультиграфи, звичайні графи, повні графи, двочасткові графи; регулярні графи; дерева, ейлерові графи, гамільтонові графи, зважені графи та інші. Орієнтованим графам притаманний напрямок. У зважених графах до кожного вузла застосовується поняття відстані і витрат.

До теперішнього часу теорія графів містить достатньо багато дієвих інструментів для вирішення широкого кола прикладних задач, в яких досліджувану складну систему можна розглядати у вигляді графової моделі з окремими компонентами і зв’язками між ними. Це такі задачі, як:

- задача про мінімальне кістякове дерево;
- задача про мінімальний шлях;
- задача про максимальний потік;
- задачі мережевого планування.

Коло питань, що вирішуються теорією графів, і різноманітність залучених для цього моделей і механізмів їх вирішення настільки великі, що вищезгадані прикладні задачі можна сьогодні зустріти в економіці і задачах управління, в конструюванні і дослідженні електричних кіл, в комунікації, соціології, лінгвістиці, психології і в багатьох інших сферах.

Теорія графів набула застосувань у великому діапазоні задач комп’ютерних наук, інформаційних технологій і програмування і як спосіб мислення, і як практична реалізація. Широке застосування теорії графів у комп’ютерних науках й інформаційних технологіях можна пояснити додаванням до вищезазначених означень графа ще одного поняття графа як структури даних. Лінійні структури даних такі як, наприклад, масиви, таблиці, черги зв’язують елементи відношенням «сусідства»; в нелінійних структурах елементи містяться на різних ієрархічних рівнях.

Засоби та ідеї теорії графів знайшли своє застосування в математичному моделюванні систем. Відзначимо тільки деякі найбільш відомі види математичних моделей у вигляді графа:

- дерево рішень використовується в задачах прийняття рішень в умовах ризику і невизначеності;
- дерево гри використовується у теорії ігор для розробки стратегій ігор;

- блок-схема комп'ютерної програми використовується для її розробки і тестування;
- граф структури даних використовується для її розробки і оптимізації;
- граф скінченного автомата використовується для дослідження скінченних автоматів в програмній інженерії;
- системний граф використовується в проектуванні і аналізі систем;
- комп'ютерна мережа використовується в проектуванні і аналізі таких мереж.

Відзначимо, що головною умовою можливості побудови моделі у вигляді графа є дискретність системи або явища, що моделюється.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Рамки статті обмежені описом основних напрямів застосування графових технологій в інформаційній та кібернетичній безпеці.

Застосування графів в інформаційних системах та у програмуванні

Спеціальність 125 Кібербезпека є частиною галузі 12 Інформаційні технології. То є очевидним, що однією з компетенцій майбутнього фахівця інформаційної безпеки є уміння розробляти програмне забезпечення у даній сфері та знати основні елементи інформаційної системи. Тому розглянемо питання щодо застосування графів в інформаційних системах та у програмуванні.

Для розробки та опису схеми інформаційних потоків в інформаційній системі зручно використовувати теорію графів. Будують інформаційну систему як орієнтований граф, який містить скінченну кількість вузлів – це компоненти інформаційної системи, та дуг, які відображають інформаційні потоки, тобто взаємозв'язки між ними. Опис схеми інформаційних потоків можна змоделювати за допомогою маршрутів графа, послідовно перерахувавши: джерело інформації, проміжна апаратура та отримувач інформації, а також вид інформації, яка передається. Суміжність компонентів інформаційної системи буде визначати матриця суміжності, а матриця інцидентності – зв'язки між компонентами та інформаційними потоками. На основі даних цих матриць можна передбачити засоби захисту інформації, наприклад, розмежування доступу до інформації. Ми згодні з авторами, які вважають, що сучасний стан програмування не можна уявити собі без теоретико-графових алгоритмів [2; 3]. Модель програми у вигляді керуючого графа, модель арифметичного виразу у вигляді орієнтованого дерева, синтаксичні дерева, дерева сортування, мережі Петрі і інші теоретико-графові конструкції внесли свій вагомий внесок в розвиток програмування і його автоматизації. Поява суперкомп'ютерів і мереж та проблема, що виникла при цьому щодо ефективної організації паралельних і розподілених обчислень над інформаційними масивами великого обсягу, підтвердили тенденцію використання графів як найбільш ефективного засобу автоматизації програмування [3]. Як відомо, більшість діаграм UML (уніфікована мова моделювання у програмуванні) по суті – графи з вершинами з геометричних фігур. Граф несе, в першу чергу, топологічну інформацію, і розташування його вершин важливо лише для діаграм типу тимчасових послідовностей. Графічні взаємозв'язки представлені плоскими лініями; вони узагальнюють поняття ребер з теорії графів, маючи менше формальний характер, але розвинену семантику. Шляхами служать послідовності відрізків ліній, що з'єднують окремі графічні символи.

Оскільки обсяги інформації, яку бажано візуалізувати, постійно збільшуються та ускладнюються, виникає все більше ситуацій, в яких класичні графові моделі перестають

бути адекватними. У дослідженні [3] зроблено ґрунтовний аналіз теоретико-графових методів та алгоритмів у програмуванні:

- клас алгоритмів на деревах (обхід та генерація дерева, побудова каркасів, структурних дерев, ізоморфізму, уніфікації та перетворення дерев для організації , представлення та синтаксичного аналізу інформації;
- клас алгоритмів на безконтурних графах (DAG) (семантичний аналіз та кодогенерація інформації);
- клас алгоритмів для звідних та регуляризаційних графів (для проведення оптимізаційних та розпаралелювальних перетворень програм).

Моделювання, аналіз та застосування графів атак

Велика кількість наукових досліджень присвячена удосконаленню моделей атак у вигляді графів для задач моніторингу кібербезпеки з метою захисту інформації. Для визначення шляхів атак у комп'ютерних мережах використовують графи атак (дерева атак) [5 – 12].

Графи атак – це метод, за допомогою якого можна досліджувати взаємодію між уразливостями всієї системи. Графи атак можуть приймати інформацію, надану сканером уразливостей, проаналізувати її з метою виявлення наявних блоків захисту.

З іншого боку, граф атак - це орієнтований граф G = G(V,E), на якому досліджується сукупність сценаріїв (шляхів атак), що моделюють нанесення збитків зловмисним агентом інформаційній системі, яка підлягає захисту.

Виділяють наступні види графів атак [4]:

- state enumeration graph (граф перерахування станів) – в таких графах вершинам відповідають трійки (s, d, a), де s – джерело атаки, d – мета атаки, a – елементарна атака (або використання уразливості); дуги позначають переходи з одного стану в інший (рис. 1);
- condition-oriented dependency graph (граф залежностей, орієнтованих на умови) – вершин відповідають результати атак, а дугам – елементарні атаки, що призводять до таких результатів (рис. 2);
- exploit dependency graph (граф залежностей експлойтів або граф умов реалізації можливостей експлойтів) – вершини відповідають результатам атак або елементарним атакам, дуги відображають залежності між вершинами – умови, необхідні для виконання атаки і наслідок атаки (рис. 3).

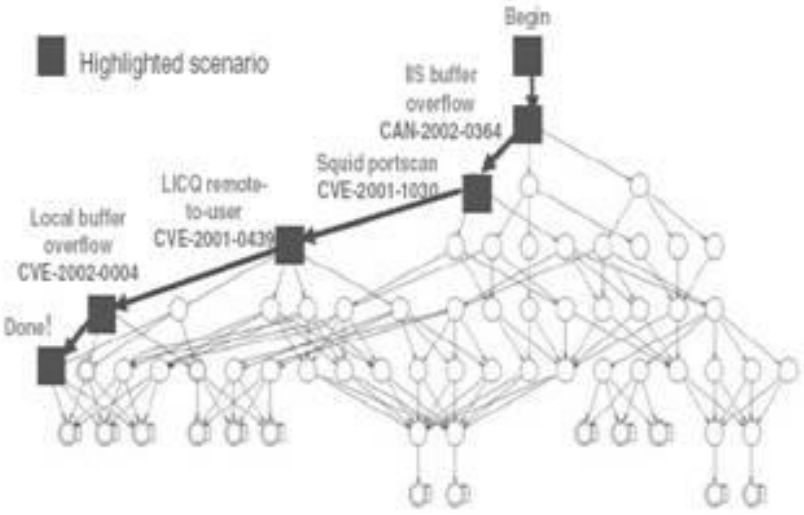

Рис. 1. State enumeration graph

ISSN 2663 - 4023

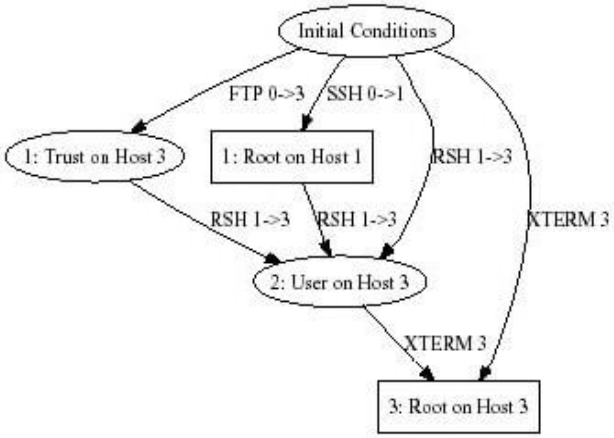

Рис. 2. Condition-oriented dependency graph

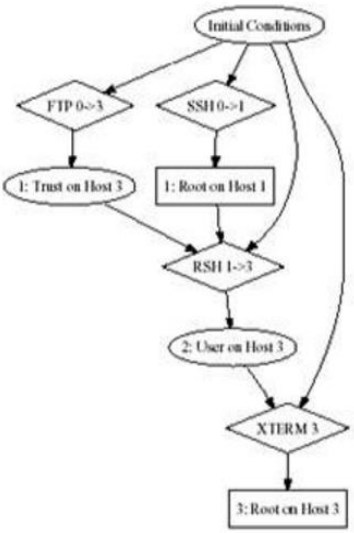

Рис. 3. exploit dependency graph

Такі моделі застосовуються в основному на етапі аудиту безпеки мереж для виявлення слабких місць системи захисту і прогнозування дій порушника. Графи атак також використовуються при розслідуванні комп'ютерних інцидентів, для аналізу ризиків і кореляцій попереджень систем виявлення атак.

У дослідженні [5] вперше вводиться поняття «дерева атаки» формальний метод опису безпеки систем, заснованих на атаках, які можуть бути здійснені проти них. Крім того, в цьому методі B. Schneier пропонує додати витрати на вузли атаки, щоб дозволити розпізнати реалістичні атаки. Дерева атаки забезпечують ще один метод оцінки кіберризиків, який за своєю суттю повинен враховувати супротивника.

Дослідження [6] продовжує вивчення характеристик дерева атак, але під новою назвою атакувальні дерева (ACT), в якому захисні механізми можуть бути застосовані на будь-якому вузлі дерева, а не тільки на рівні листового вузла, здійснено якісний аналіз і ймовірнісний аналіз ризиків.

Автори наукової праці [7] подібно до дерев атак візуально представляють шляхи, які супротивник може пройти через розглянуту систему, у вигляді графа атак.

Досліджується граф атаки, який використовується для оцінки сукупної ймовірності компромісу шляхів через граф. Ймовірність у наведених прикладах полягає в тому, що змодельований розподіл Монте-Карло генерується мінімальною та максимальною оцінкою для кожного використаного експлойту.

Аналіз наукових джерел дозволив визначити різні підходи до побудови та застування графа атак, проте мета у всіх розробок одна – своєчасне виявлення атакуючого в системі і точне прогнозування його цілей може допомогти запобігти серйозної шкоди системі і уникнути великих втрат.

Теорія графів та криптографічні перетворення.

Теорії графів широко застосовується у криптографії (криптології, кодування). На це вказують дослідження у наукових працях, наприклад [13 – 19]. Так, автор у статті [13] визначає зв'язок між теорією графів та криптологією наступним чином: множині перетворень будь-якого ендоморфного шифру відповідає помічений граф, вершинами якого є елементи тексту, що шифрується, а дуги помічають ключем, який використовується. Квадратна таблиця розміру n x n, що визначає табличний шифр, може бути легко перетворена в n-вершинний граф. Властивість транзитивності напівгруп і груп перетворень, пов'язаних з шифром, може мати інтерпретацію як сильна зв’язність відповідного графа. Вивчення протоколів автентифікації типу «запит-відповідь» ґрунтується на графах Келі групи Кокстера.

У дослідженні [15] аналізуються деякі криптографічні алгоритми, засновані на загальних концепціях теорії графів, теорії екстремальних графів і розширених графів.

Алгоритм шифрування-дешифрування за допомогою графів Ейлера було запропоновано у статті [17].

Теорія інформації широко використовує властивості двійкових дерев. Наприклад, якщо потрібно закодувати деяке число повідомлень у вигляді певних послідовностей нулів і одиниць різної довжини. Код вважається найкращим для заданої ймовірності кодових слів, якщо середня довжина слів найменша в порівнянні з іншими розподілами ймовірності. Для вирішення такого завдання Хаффман запропонував алгоритм, в якому, код представляється деревом-графом в рамках теорії пошуку. Для кожної вершини пропонується питання, відповіддю на який може бути або «так», або «ні», що відповідає двом ребрам, які виходять з вершини. Побудова такого дерева завершується після встановлення того, що було потрібно [18]

Застосування теорії графів для побудови дерева рішень

Як відомо, дерево рішень – це спосіб представлення правил в ієрархічній послідовній структурі, де кожному об’єкту відповідає єдиний вузол, який дає рішення. Початок розвитку даної технології поклала праця «Experiments in Induction» в 1966 році (вчені E.B. Hunt, J.Marin, P.J. Stone).

Як стверджують автори [20], сфера застосування дерев рішень на сучасному етапі дуже широка, проте всі завдання, які вирішуються цим апаратом, можуть бути об’єднані в три групи:

- опис даних (дерево рішень дозволяє зберігати інформацію в компактній формі);
- класифікація (дерево рішень дозволяє віднести до відповідно сформованого класу, при цьому основна змінна має носити дискретний характер);

- регресія (дерево рішень дозволяє встановити залежність основної змінної від вхідних змінних, при цьому основна змінна має бути неперервною).

У дослідженні автори для регулювання глибини дерева (цей процес дозволяє зменшити розмір дерева, вирізавши при цьому деякі ділянки з маленькою вагою чи з низькою ймовірністю адекватності рішення) пропонується прямий матричний метод. За допомогою тестування було доведено, що даний метод має переваги над евристичним алгоритмом за рахунок більш низької трудомісткості.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Якісна кібернетична освіта базується передусім на математиці. Теорія графів – розділ математики, що дає змогу формалізувати взаємозв'язки між різноманітними видами інформації, організувати абстрактне їх представлення. Тому її значення та застосування у різних напрямах наукових досліджень, зокрема у сфері інформаційної та кібернетичної безпеки, буде розвиватися і надалі.

Розглянуті підходи до застосування теорії графів в інформаційній та кібернетичній безпеці можуть бути впроваджені під час вивчення дисципліни «Спеціальні методи в системах безпеки: дискретна математика» для студентів спеціальності 125 Кібербезпека, а також при підготовці фахівців у процесі науково-дослідної роботи або курсової чи дипломної роботи. Підвищуючи професійну спрямованість навчання, майбутні кібербезпечники отримують ґрунтовні знання фундаментальних дисциплін.

Вектор подальших досліджень може бути спрямований на огляд інших математичних технологій для розв'язання проблеми захисту інформації з метою зацікавленості студентів у вивченні математичних теорій та методів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). MATHEMATICAL METHODS IN CYBER SECURITY: FRACTALS AND THEIR APPLICATIONS IN INFORMATION AND CYBER SECURITY. *Cybersecurity: Education, Science, Technique*, (5), 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139

2 Battista, G. D., Eades, P., Tamassia, R., & Tollis, I. G. (1994). Algorithms for drawing graphs: an annotated bibliography. *Computational Geometry*, *4*(5), 235–282. https://doi.org/10.1016/0925-7721(94)00014-x

3 Касьянов, В.Н., Евстигнеев, В.А. (2003). *Графы в программировании: обработка, визуализация и применение*. БХВ-Петербург.

4 Danforth M. Models for Threat Assessment in Networks. http://www.cs.ucdavis.edu/research/tech-reports/2006/CSE-2006-13.pdf

5 Schneier, B. (1999). Attack trees, *Dr. Dobb's Journal of Software Tools*.

6 Roy, A., Kim, D. S., & Trivedi, K. S. (2010). Cyber security analysis using attack countermeasure trees. У *the Sixth Annual Workshop*. ACM Press. https://doi.org/10.1145/1852666.1852698

7 Noel, S., Jajodia, S., Wang, L., Singhal., A. (2010). Measuring Security Risk of Networks Using Attack Graphs. *IJNGC, 1*(1), 135–147. https://scholar.google.com.ua/scholar?q=Measuring+Security+Risk+of+Networks+Using+Attack+Graphs&hl=uk&as_sdt=0&as_vis=1&oi=scholart

8 Matthews., I, Mace Newcastle, J., Soudjani, S., Aad van Moorsel. (2020). Systematic Computational Approach. arXiv:2005.06350v1 [cs.CR] 13 May 2020.

9 Ou, X., Boyer, W. F., & McQueen, M. (2006, 1 січня). *(PDF) A scalable approach to attack graph generation*. ResearchGate. https://www.researchgate.net/publication/313772274_A_scalable_approach_to_attack_graph_generation

10 Derbyshire, R., Green, B., & Hutchison, D. (2021). “Talking a Different Language”: Anticipating Adversary Attack Cost for Cyber Risk Assessment. *Computers & Security*, 102163. https://doi.org/10.1016/j.cose.2020.102163
11 Savchenko, V. A., Matsko, O. I., Legominova, S. V., Poltorak, I. S., & Marchenko, V. V. (2019). The Cyberattack Simulation by Graph Theory. *Modern information security*, (4). https://doi.org/10.31673/2409-7292.2019.040611
12 Doynikova, E. V., & Kotenko, I. V. (2018). Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection. *SPIIRAS Proceedings*, *2*(57), 211. https://doi.org/10.15622/sp.57.9
13 Фомичев, В. М. (2010). *Методы дискретной математики в криптологии*. Диалог-МИФИ.
14 Коренева, А. М. (2010). О некоторых результатах систематизации теоретико-графовых моделей, используемых для решения задач криптологии. У *XIV Международная телекоммуникационная конференция студентов и молодых ученых «МОЛОДЕЖЬ И НАУКА»* (с. 239–241). М.: НИЯУ МИФИ.
15 Priyadarsini, P. L. K. (2015). A Survey on some Applications of Graph Theory in Cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(3), 209–217. https://doi.org/10.1080/09720529.2013.878819
16 Ustimenko, V. (2015). On algebraic graph theory and non-bijective multivariate maps in cryptography. *Algebra and Discrete Mathematics, 20* (1), 152–170.
17 Amudha, P., Charles Sagayaraj, A.C., Shantha Sheela, A.C. (2018). An Application of Graph Theory in Cryptography. *International Journal of Pure and Applied Mathematics, 119*(13), 375-383.
18 *Scientific American Article | Huffman Coding*. (б. д.). Huffman Coding | … with a bunch of Family Stuff too. http://www.huffmancoding.com/my-uncle/scientific-american
19 Read, R. C. (1997). Graph Theory and the Amateur Cryptographer. *Computers & Mathematics with Applications*, *34*(11), 121–127. https://doi.org/10.1016/s0898-1221(97)00226-5
20 Куприянов, М.С., Шичкина, Ю.А. (2012). Применение теории графов для разработки прямого метода построения деревьев решений, *Системы. Методы. Технологии, 4*(16), 62-65. https://brstu.ru/static/unit/journal_smt/docs/number16/62-65.pdf
21 Оре, О. (1956). *Графы и их применение*. М.: Мир.
22 Нидхем, М., Ходлер, Э. (2020). *Графовые алгоритмы. Практическая реализация на платформах Apache Spark и Neo4j*. ДМК Пресс.
23 Shrinivas, S.G., Vetrivelet, S., Elango, N.M. (2010). Applications of grapf theory in computer science an overview. *International Journal of Engineering Science and Technology*, *2*(9), 4610-4621.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Svitlana M. Shevchenko
PhD, Associate Professor
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Pavlo M. Skladannyi
PhD,
Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Svitlana O. Spasiteleva
PhD, Associate Professor
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

MATHEMATICAL METHODS IN CIBERNETIC SECURITY: GRAPHS AND THEIR APPLICATION IN INFORMATION AND CYBERNETIC SECURITY

Abstract. This article is devoted to the problem of applying graph theory in cybersecurity systems and is an overview. Widespread penetration of mathematical methods in the development of information technology characterizes the current stage of our society. Among the mathematical methods used in information and cyber security, a large niche is graph technology. A streamlined system of special terms and symbols of graph theory allows you to easily and easily describe complex and subtle things both geometrically and algebraically. A graph is a mathematical model of a wide variety of objects, phenomena, and the relationships between them. This justifies the choice and relevance of this study. The article outlines the main elements of graph theory, the wide scope of their implementation and provides a historical perspective on the development of this theory. The analysis of scientific works allowed to determine the main directions of application of properties, characteristics of graphs and graph algorithms in information and cyber security. Among them are studies related to the use of graphs in information systems and programming; with modeling, analysis and application of attack graphs; with cryptographic transformations; with the construction of a decision tree in decision-making tasks in conditions of risk and uncertainty. It is proved that the ability to operate with the methods of graph technologies contributes to the development of software and hardware for information protection. The considered approaches to the application of graph theory in information and cyber security can be implemented during the study of the discipline "Special methods in security systems: discrete mathematics" for students majoring in 125 Cybersecurity, as well as in training in research or course work or thesis. By increasing the professional orientation of training, future cybersecurity workers gain a thorough knowledge of fundamental disciplines.

Keywords: mathematical methods; cybersecurity; graph; attack graph; graph algorithms; cryptography.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). MATHEMATICAL METHODS IN CYBER SECURITY: FRACTALS AND THEIR APPLICATIONS IN INFORMATION AND CYBER SECURITY. *Cybersecurity: Education, Science, Technique*, (5), 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139

2 Battista, G. D., Eades, P., Tamassia, R., & Tollis, I. G. (1994). Algorithms for drawing graphs: an annotated bibliography. *Computational Geometry*, *4*(5), 235–282. https://doi.org/10.1016/0925-7721(94)00014-x

3 Kasianov, V.N., Evstyhneev, V.A. (2003). Hrafы v prohrammyrovanyy: obrabotka, vyzualyzatsyia y prymenenye. BKhV-Peterburh.

4 Danforth M. Models for Threat Assessment in Networks. http://www.cs.ucdavis.edu/research/tech-reports/2006/CSE-2006-13.pdf

5 Schneier, B. (1999). Attack trees, *Dr. Dobb's Journal of Software Tools*.

6 Roy, A., Kim, D. S., & Trivedi, K. S. (2010). Cyber security analysis using attack countermeasure trees. У *the Sixth Annual Workshop*. ACM Press. https://doi.org/10.1145/1852666.1852698

7 Noel, S., Jajodia, S., Wang, L., Singhal., A. (2010). Measuring Security Risk of Networks Using Attack Graphs. *IJNGC, 1*(1), 135–147. https://scholar.google.com.ua/scholar?q=Measuring+Security+Risk+of+Networks+Using+Attack+Graphs&hl=uk&as_sdt=0&as_vis=1&oi=scholart

8 Matthews., I, Mace Newcastle, J., Soudjani, S., Aad van Moorsel. (2020). Systematic Computational Approach. arXiv:2005.06350v1 [cs.CR] 13 May 2020.

9 Ou, X., Boyer, W. F., & McQueen, M. (2006, 1 січня). *(PDF) A scalable approach to attack graph generation*. ResearchGate. https://www.researchgate.net/publication/313772274_A_scalable_approach_to_attack_graph_generation

10 Derbyshire, R., Green, B., & Hutchison, D. (2021). "Talking a Different Language": Anticipating Adversary Attack Cost for Cyber Risk Assessment. *Computers & Security*, 102163. https://doi.org/10.1016/j.cose.2020.102163

11 Savchenko, V. A., Matsko, O. I., Legominova, S. V., Poltorak, I. S., & Marchenko, V. V. (2019). The Cyberattack Simulation by Graph Theory. *Modern information security*, (4). https://doi.org/10.31673/2409-7292.2019.040611

12 Doynikova, E. V., & Kotenko, I. V. (2018). Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection. *SPIIRAS Proceedings*, *2*(57), 211. https://doi.org/10.15622/sp.57.9

13 Fomychev, V. M. (2010). Metodы dyskretnoi matematyky v kryptolohyy. Dyaloh-MYFY.

14 Koreneva, A. M. (2010). O nekotorыkh rezultatakh systematyzatsyy teoretyko-hrafovыkh modelei, yspolzuemыkh dlia reshenyia zadach kryptolohyy. U XIV Mezhdunarodnaia telekommunykatsyonnaia konferentsyia studentov y molodыkh uchenыkh «MOLODEZh Y NAUKA» (s. 239–241). M.: NYIaU MYFY.

15 Priyadarsini, P. L. K. (2015). A Survey on some Applications of Graph Theory in Cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(3), 209–217. https://doi.org/10.1080/09720529.2013.878819

16 Ustimenko, V. (2015). On algebraic graph theory and non-bijective multivariate maps in cryptography. *Algebra and Discrete Mathematics, 20* (1), 152–170.

17 Amudha, P., Charles Sagayaraj, A.C., Shantha Sheela, A.C. (2018). An Application of Graph Theory in Cryptography. *International Journal of Pure and Applied Mathematics, 119*(13), 375-383.

18 *Scientific American Article | Huffman Coding*. (б. д.). Huffman Coding | … with a bunch of Family Stuff too. http://www.huffmancoding.com/my-uncle/scientific-american

19 Read, R. C. (1997). Graph Theory and the Amateur Cryptographer. *Computers & Mathematics with Applications*, *34*(11), 121–127. https://doi.org/10.1016/s0898-1221(97)00226-5

20 Kupryianov, M.S., Shychkyna, Yu.A. (2012). Prymenenye teoryy hrafov dlia razrabotky priamoho metoda postroenyia derevev reshenyi, Systemы. Metodы. Tekhnolohyy, 4(16), 62-65. https://brstu.ru/static/unit/journal_smt/docs/number16/62-65.pdf

21 Ore, O. (1956). Hrafы y ykh prymenenye. M.: Myr.

22 Nydkhem, M., Khodler, Э. (2020). Hrafovыe alhorytmы. Praktycheskaia realyzatsyia na platformakh Apache Spark y Neo4j. DMK Press.Shrinivas, S.G., Vetrivelet, S., Elango, N.M. (2010). Applications of

grapf theory in computer science an overview. *International Journal of Engineering Science and Technology*, *2*(9), 4610-4621.