Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“ Дослідження та програмна реалізація моделей розповсюдження інформації в соціальних мережах ”

Виконав здобувач вищої освіти
ІІ курсу, групи КН-24М
ОПП «Комп’ютерні науки»
спеціальності 122 «Комп’ютерні науки»
_____ Федосенко Е.Д.
«____» _____ 2025 р.

Керівник проекту
кандидат технічних наук
_____ Улічев О.С.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Федосенко Е.Д. Дослідження та програмна реалізація моделей розповсюдження інформації в соціальних мережах. 122 Комп'ютерні науки. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для моделювання розповсюдження інформаційних впливів в соціальних мережах.

Предметом дослідження є соціальні мережі у широкому розумінні даного терміну – СМ як безліч суб'єктів, які мають між собою канали взаємозв'язку та прибувають у динамічному процесі інформаційної взаємодії. Предметом дослідження також є методи моделювання соціальних мереж і моделі поширення в них інформаційних впливів.

Об'єктом дослідження – є методи і стратегії поширення інформаційних впливів на соц. мережах та стійкість мереж до таких впливів.

Мета дослідження роботи – визначити фактори та характеристики мережі, а також способи вибору вузлів для атак у мережі, які сприяли б збільшенню швидкості поширення.

Результат роботи – програмна реалізація системи моделювання розповсюдження інформаційних впливів з параметризацією стратегії дій генератора та можливістю задавати конфігурацію мережі.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі VisualStudio C#.

Ключові слова: соціальна мережа, інформаційні впливи, поведінкові стратегії, моделювання.

ABSTRACT

Fedosenko E.D. Research and software implementation of information dissemination models in social networks. 122 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed that is intended for modeling the spread of information influences in social networks.

The subject of the study is social networks in the broad sense of the term - SM as a set of subjects that have communication channels between themselves and are involved in a dynamic process of information interaction. The subject of the study is also methods for modeling social networks and models for the spread of information influences in them.

The object of the study is methods and strategies for the spread of information influences in social networks and the resistance of networks to such influences.

The purpose of the study is to determine the factors and characteristics of the network, as well as methods for selecting nodes for attacks in the network that would contribute to increasing the speed of spread.

The result of the work is a software implementation of a system for modeling the spread of information influences with parameterization of the generator's action strategy and the ability to specify the network configuration.

In the process of working on the software model, an analysis of existing hardware and software tools was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with software tools are provided.

The program can be used on a PC with Windows 10/11 OS.

The program was developed in the VisualStudio C# environment.

Keywords: social network, information influences, behavioral strategies, modeling.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

СМ	–	Соціальна мережа
ОС	–	Операційна система
ІВ	–	Інформаційний вплив
ІПВ	–	Інформаційно-психологічний вплив
Сегмент мережі	–	Відокремлена частина мережі з структ. особливостями
Active	–	Активність вузла
Reputation	–	Репутація (довіра до вузла)
Opposite	–	Спротив вузла
Involvement	–	Залученість вузла до ідеї
ABS	–	Activity-Based Costing

ВСТУП

Актуальність теми. Суттєвий розвиток соціальних мереж провокував їх широке застосування для інформаційних впливів на суспільство. Впливи можуть мати різний характер: від реклами товарів та послуг, до пропаганди та навіювання потрібних наративів. І якщо соціальні мережі, як рекламний інструмент, є предметом маркетології, то використання останніх для інформаційних впливів з метою пропаганди та інструменту інформаційних війн є безпосередньо питанням безпеки держави. Актуальність дослідження визначається зростаючим впливом соціальних мереж на свідомість людей та активне їх використання в інформаційному протистоянні, зокрема і під час гібридної війни, яку веде Росія проти України.

Істотне глобальне розширення мережі Інтернет та різке зростання кількості користувачів різних соціальних сервісів останнім часом абсолютно стерло територіальні кордони в інформаційному обміні, а також суттєво збільшилась швидкість розповсюдження інформації. Будь-яка інформація, що потрапила до мережі, моментально стає надбанням світової громадськості. Ці процеси практично неможливо контролювати, з погляду обмежень доступу, сепарування аудиторії та подібних підходів. Зважаючи на це, актуальними стають методи інформаційного протистояння – при появі «небажаної» новини чи інформаційного посилу необхідно вжити заходів не щодо її видалення чи блокування (оскільки це дуже важко чи практично неможливо), а постаратися нівелювати її вплив, переконати аудиторію в протилежному, розсіяти увагу. При цьому «небажаність» визначається кожним активним суб'єктом індивідуально і сама інформаційна суть тут не має жодної ролі. "Небажана" для одного суб'єкта може бути дуже "бажаною" для іншого.

Для багатьох користувачів Інтернету соціальні мережі стають одним із основних джерел інформації та поточних новин. Разом про те дані Інтернет-

ресурси стають зручним середовищем поширення інформаційно-психологічних впливів на звичайних користувачів під час проведення інформаційних кампаній, тобто. пости та коментарі в соціальних мережах все частіше використовуються для маніпулювання громадською думкою, зокрема як для просування товарів/послуг/контенту [37] методами вірусного маркетингу, так і під час інформаційних воєн та протистоянь на різних рівнях: організації, корпорації, політичні партії, держави. Для поширення інформаційних впливів можуть використовуватися як справжні, так і фейкові акаунти, для масованих атак створюються цілі бот-ферми. Для розуміння масштабу явища слід зазначити, що за даними Facebook за період з жовтня 2018 по березень 2020 на даному веб-ресурсі було видалено в сукупності 4,5 млрд фейкових акаунтів [38]. І цей процес не має завершення, він відбувається постійно в тих чи інших масштабах, залежно від значущості та чисельності конкретної мережі.

Актуальними завданнями є як підходи активного впливу, так і методи оцінки та протистояння таким впливам. Фактично, певною мірою, це те саме. Адже поширення діаметрально протилежного посилу (інформаційної ідеї) можна розглядати як протистояння та захисний механізм від негативного інформаційного впливу. В кінці 2019 на початку 2020 року можна було спостерігати ситуацію протистояння прихильників та противників вакцинації проти COVID-19, протистояння дуже багатогранне та має різне інформаційне забарвлення. У цьому дослідженні ми розглядаємо це протистояння лише як приклад, не намагаючись обґрунтувати чи аргументувати одну з протилежних думок. Проте, вакцинування є однією з можливих ефективних шляхів протистояння епідемії (приймемо умовно цей факт). Отже – в інтересах держави та суспільства є поширення інформації, інформаційний мотиваційний вплив на громадян, який націлений на те, щоб максимальна кількість громадян вакцинувалася в короткий термін. Цей приклад показує, яким важливим може бути не лише кінцевий факт інформаційного впливу, а й швидкість поширення інформації.

Таким чином, дослідження поширення інформаційно-психологічних впливів у мережах та забезпечення інформаційної безпеки на цих ресурсах є актуальним завданням.

Соціальні мережі (СМ) стали важливим джерелом інформації для користувачів Інтернету [1-3]. Вони забезпечують платформи для міжособистісної та масової комунікації, пошуку інформації, перегляду новин і багатьох інших функцій. Однак, з іншого боку, соціальні мережі стали сприятливим середовищем для поширення інформаційних впливів (ІВ) і маніпуляцій громадською думкою, що створює серйозні загрози як для окремих користувачів, так і для суспільства та держави в цілому [4-8]. Сьогодні однією з основних загроз є вплив через засоби масової інформації та соціальні медіа. На відміну від інформаційно-кібернетичних (технічних) впливів, які орієнтовані на інформаційні ресурси, ІВ спрямовані на свідомість і підсвідомість людей. Їхня мета — формувати певні ідеї, погляди, переконання, а також спонукати до конкретних дій або бездіяльності, одночасно викликаючи у людей як позитивні, так і негативні емоції, почуття та навіть спричиняючи масові емоційні реакції.

З погляду стрімкої глобалізації інформаційних процесів, глобалізації світового інформаційного простору та інформаційної експансії з боку інших держав актуальним стає завдання аналізу та прогнозування процесів в інформаційному просторі, а також розробка методологічних основ забезпечення інформаційної безпеки та методів протидії деструктивним діям. Одним із найважливіших завдань є запобігання негативним інформаційним впливам на індивідуальну, групову та суспільну свідомість, захист від ворожої чи недружньої пропаганди, створення технологій дослідження, захисту та контрзахисту людини, суспільства та держави негативних наслідків інформаційно-психологічного впливу.

Сучасні наукові роботи, спрямовані на дослідження ІВ у соціальних мережах в умовах інформаційного протиборства (роботи вчених Д. Губанов, А.

Сазонов, В. Горбулін, А. Пую, А. Додонов, Г. Почепцов, С. Розторгуєв) розглядають два напрямки:

– методи інформаційних атак: формування, поширення та використання ІВ.

– методи протидії: виявлення, прогнозування наслідків та захист від ІВ.

Оскільки СМ є одним із каналів поширення ІВ, актуальне завдання дослідження процесу поширення таких впливів СМ для розробки методів прогнозування наслідків та методів захисту. СМ і їх процеси нині активно досліджуються різними вченими, проте розвиток СМ значно випереджає темпи наукових досліджень.

Зважаючи на велике поширення інформаційних протидій, тема дослідження має пряме відношення до спеціальності «Інформаційна безпека». У соціальних мережах, як і в Інтернеті в цілому, користувачі можуть зустрічатися з такими видами інформаційних загроз:

1) загрози порушення конфіденційності, доступності та цілісності інформації;

2) загрози наявності інформаційно-психологічних впливів, порушення достовірності, повноти, об'єктивності, адекватності, корисності.

Загрози обох груп є об'єктами, на які мають бути спрямовані методи протистояння та зусилля спеціалістів у сфері інформаційної безпеки.

Дослідження інформаційних атак на СМ шляхом їх моделювання дозволить розробити та реалізувати превентивні та контрзаходи для запобігання негативним психо-інформаційним впливам (ПІВ) на індивідуальну, групову та громадську свідомість, захист від ворожої чи недружньої пропаганди. Також це дозволяє розробляти науково-методичні засади та технології захисту людини, суспільства та держави від негативних наслідків ВВ.

Роботи вчених, створені задля дослідження процесів поширення ІВ (не технічних) в СМ, можна розділити такі основні групи:

1) застосовують збір та аналіз даних з відкритих частин веб-ресурсів СМ, парсинг та аналіз даних (Н. Лабуш, Т. Батура, Є. Князєва Є., Б. Хоган).

2) використовують математичне та програмне моделювання СМ та процесів у них, застосування теорії комплексних мереж (А. Барабаші, Р. Альберт, Б. Боллобаш, О. Ріордан, П. Ердьош, А. Реньї, П. Баклі, Д. Остхус, Дж. Чаєс, К. Боргс, М. Грановв. Горковенко, І. Гончаров, Б. Торопов).

3) досліджують інформаційні атаки та ІВ на СМ (В. Горбулін, А. Пую, Г. Почепцов, С. Розторгуєв).

Сучасні СМ використовують різні методи протидії парсингу інформації щодо їх веб-ресурсів, зокрема, зростає обсяг закритої частини інформації, а на збирання відкритої інформації створюють значні тимчасові затримки. З останнього дедалі актуальнішою стає друга група методів. Імітаційні моделі СМ дозволяють проводити дослідження процесів, що протікають в них, без значних тимчасових і фінансових витрат і без доступу до даних, які відкриті тільки власникам веб-ресурсів.

Останнім часом розроблено безліч підходів та моделей, кожна з яких має свої переваги та недоліки. Проведений аналіз показав, що переважна більшість моделей та методів не враховують індивідуальні характеристики вузла соціальної мережі (вузол – користувач СМ), а саме поведінка окремого вузла, стратегію поширення інформації, яку обирає вузол у процесі ІВ тощо. Враховуючи зазначене, розробка методів та засобів моделювання та реалізації різних стратегій поширення ІВ у сегментах СМ є актуальним завданням, що має теоретичне та практичне значення.

Предметом дослідження є соціальні мережі у широкому розумінні даного терміну – СМ як безліч суб'єктів, які мають між собою канали взаємозв'язку та прибувають у динамічному процесі інформаційної взаємодії. Предметом дослідження також є методи моделювання соціальних мереж і моделі поширення в них інформаційних впливів.

Об'єктом дослідження – є методи і стратегії поширення інформаційних впливів на соц. мережах та стійкість мереж до таких впливів.

Мета дослідження роботи – визначити фактори та характеристики мережі, а також способи вибору вузлів для атак у мережі, які сприяли б збільшенню швидкості поширення. З іншого боку – визначення вищезгаданих факторів та їхнього впливу на інформаційні процеси дозволяє підвищувати стійкість мережі до інформаційних впливів.

Мета роботи визначає необхідність вирішення наступних **основних завдань**:

1. Дослідити методи генерації мереж та моделі поширення інформаційних впливів у соціальних.

2. Розробити математичну модель поширення інформаційних впливів у сегменті соціальної мережі з урахуванням особистісних характеристик вузлів мережі, що дозволяє на основі аналізу запропонованих характеристик застосувати різні поведінкові стратегії суб'єктами інформаційного впливу.

3. Удосконалити метод генерації сегмента соціальної мережі з можливістю моделювання різних наперед визначених варіантів структури сегмента мережі (топологій).

4. Провести експериментальні дослідження на програмній моделі, перевірити ефективність запропонованих методів з точки зору швидкості поширення інформаційних впливів у сегменті соціальної мережі, визначити фактори та структурні особливості мережі, що мають вплив на досліджувані процеси.

Магістерська робота має елементи наукової новизни. Так математичну модель, яку розглядають у роботі, запропоновано вперше. Також у роботі вперше запроваджується та формалізується поняття поведінкових стратегій, як алгоритмів вибору цільових вузлів для інформаційної атаки. Пропонований підхід до генерації сегмента мережі, хоч і не є абсолютно новим, має низку авторських удосконалень та модифікацій. Реалізована на основі запропонованої математичної моделі програмна модель може бути використана як інструмент подальших досліджень даного напрямку.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Інформація завжди відігравала ключову роль у розвитку людського суспільства. Саме завдяки їй людство отримувало та зберігало досвід попередніх поколінь, формувало знання та культурні традиції. На сучасному етапі соціального розвитку визначальним чинником стає інформатизація – процес активного впровадження та використання інформаційних технологій у всіх сферах життя. Володіння інформацією сьогодні означає доступ до нових моделей управління, впливу на суспільні процеси та формування нових соціальних структур.

Розвиток систем зв’язку, зокрема глобальних мереж передачі даних, спричинив повне нівелювання територіальних обмежень в обміні інформацією. Особливе місце в цьому процесі займають соціальні мережі, які стали одним із головних каналів комунікації між людьми. Їхня популярність і доступність перетворили соціальні мережі на важливий соціально-комунікаційний інструмент, що впливає на суспільну думку, політичні процеси, медіасферу та навіть міжнародні відносини.

У даному дослідженні соціальні мережі розглядаються не лише як засоби комунікації, а й як платформи для проведення інформаційних атак, маніпулювання свідомістю користувачів, нав’язування певних ідеологічних установок або поведінкових моделей. Оскільки соціальна мережа становить об’єкт моделювання, першочергово необхідно визначити саме поняття «соціальна мережа», її структуру та особливості функціонування.

Соціальні мережі – це популярний інтернет-сервіс, що дозволяє користувачам створювати віртуальні спільноти, обмінюватися інформацією, підтримувати зв'язки та організовувати комунікаційну діяльність. За сучасними

даними, близько 90% інтернет-користувачів активно взаємодіють із соціальними мережами.

Соціальна мережа (Social Service Network) – це інтернет-платформа, яка надає зареєстрованим користувачам можливість створювати власні профілі, поширювати персональну інформацію, обмінюватися контентом, спілкуватися та формувати соціальні зв'язки. Завдяки технологіям Web 2.0 основний обсяг контенту формують самі користувачі, що забезпечує мережам високий рівень динамічності та інтерактивності[1].

З погляду теорії соціальних структур, соціальна мережа – це система, що складається з вузлів (якими можуть бути окремі люди, організації або групи людей) та зв'язків між ними, якими є інформаційні або комунікаційні взаємодії[9].

Популярність соціальних мереж пояснюється широкими можливостями, які вони надають користувачу[2,3]:

– спілкування в режимі реального часу (текстові повідомлення, голосові та відеодзвінки);

– оперативний обмін інформацією та доступ до різноманітного контенту;

– зручні інструменти пошуку, фільтрації та групування інформації;

– створення спільнот за інтересами, просування ідей чи ініціатив.

Завдяки цим можливостям соціальні мережі використовуються не лише для приватного спілкування, а й як:

– засоби масової комунікації;

– інструменти політичної боротьби та агітації;

– майданчик для організації громадських рухів і соціальних кампаній;

– середовище для проведення інформаційних та медійних операцій.

Особливо вагомим є використання соціальних мереж у сучасних інформаційних конфліктах. Сьогодні інформаційна війна може починатися задовго до реальних військових дій, а вплив у соціальних медіа часто визначає суспільні настрої та політичну стабільність.

Зростання популярності соціальних мереж підтверджує постійне збільшення їхньої аудиторії. Наприклад, кількість зареєстрованих користувачів у мережі Facebook перевищує 1 мільярд, Twitter і Google+ налічують понад 200 мільйонів користувачів, а LinkedIn – понад 100 мільйонів[10].

1.2 Область застосування

Методи дослідження соціальних мереж здебільшого базуються на підходах, що застосовуються при аналізі мережевих структур у широкому значенні цього поняття. Соціальні мережі мають впорядковану структуру та характеризуються взаємодіями між елементами (вузлами), що загалом відповідає загальним принципам мережевого моделювання. У найбільш узагальненому вигляді соціальну мережу можна подати у вигляді графа:

$$G(V,E), \tag{1}$$

де V - множина вузлів, якими виступають користувачі соціальної мережі, а E - множина ребер, що відповідають контактам або каналам інформаційної взаємодії між цими користувачами.

Таким чином, кожен користувач у графі є вузлом, а ребра представляють комунікаційні або інформаційні зв’язки. Соціальну мережу можна розглядати як соціальну структуру, що відображає реальні взаємодії людей, але водночас вона постає і як технічна реалізація цієї структури на основі інтернет-технологій. Використання цифрових платформ дозволяє збільшувати кількість можливих зв’язків, прискорювати обмін інформацією та розширювати межі взаємодії, не змінюючи при цьому фундаментальних закономірностей формування мережевих структур.

Поняття мережі у вигляді графа вперше було запропоноване Л. Ейлером у задачі про кенігсберзькі мости. Надалі графові структури стали універсальним інструментом моделювання складних взаємозв'язків у різних системах.

Сфера застосування мережевого аналізу є надзвичайно широкою та охоплює різні галузі:

1. Економіка та управління: дослідження внутрішніх і зовнішніх зв'язків організацій, побудова ринкових взаємодій, формування стратегій реклами та просування, аналіз поведінки споживачів і мереж соціальної підтримки.

2. Соціологія: вивчення соціальних груп, взаємодія професійних спільнот, аналіз розвитку наукових колаборацій, дослідження культурних та історичних зв'язків.

3. Медицина та біологія: моделювання поширення інфекцій, аналіз взаємодій в екосистемах, дослідження підтримуючих мереж у психотерапевтичній практиці.

4. Криміналістика та безпека: аналіз мереж незаконного обігу наркотиків, організованих злочинних груп, терористичних осередків та каналів координації їхньої діяльності.

Методи аналізу соціальних мереж ґрунтуються на інструментах теорії графів, інформаційних підходах та статистичних методах. За загальноприйнятою класифікацією М. Доверна виділяють чотири основні напрями аналізу соціальних мереж: структурний, ресурсний, нормативний та динамічний.

- **Структурний підхід** зосереджується на конфігурації мережі: взаємному положенні вузлів, щільності зв'язків, центральності окремих учасників, наявності груп або спільнот. Основним завданням є виявлення найбільш впливових вузлів та ключових структурних елементів.
- **Ресурсний підхід** аналізує можливості учасників мережі використовувати доступні ресурси (інформаційні, соціальні, статусні, фінансові) для досягнення власних цілей. Центральним ресурсом є інформація, яка має властивість невичерпності: її передача не зменшує її кількості у джерела.

- **Нормативний підхід** досліджує систему правил, норм і санкцій, що регулюють поведінку користувачів у мережі, а також рівень довіри між ними. Таким чином аналізується вплив соціальних ролей та культурних установок на мережеву взаємодію.
- **Динамічний підхід** вивчає, як мережа змінюється з часом: які зв'язки формуються або зникають, як виникають нові кластери, як зовнішні фактори можуть впливати на структуру мережі. Цей підхід активно використовує методи моделювання та візуалізації для прогнозування можливих сценаріїв розвитку мережі.

У комплексі ці підходи дозволяють отримати повну картину функціонування соціальної мережі, механізмів її розвитку, впливу окремих учасників на систему та поширення інформації у ній.

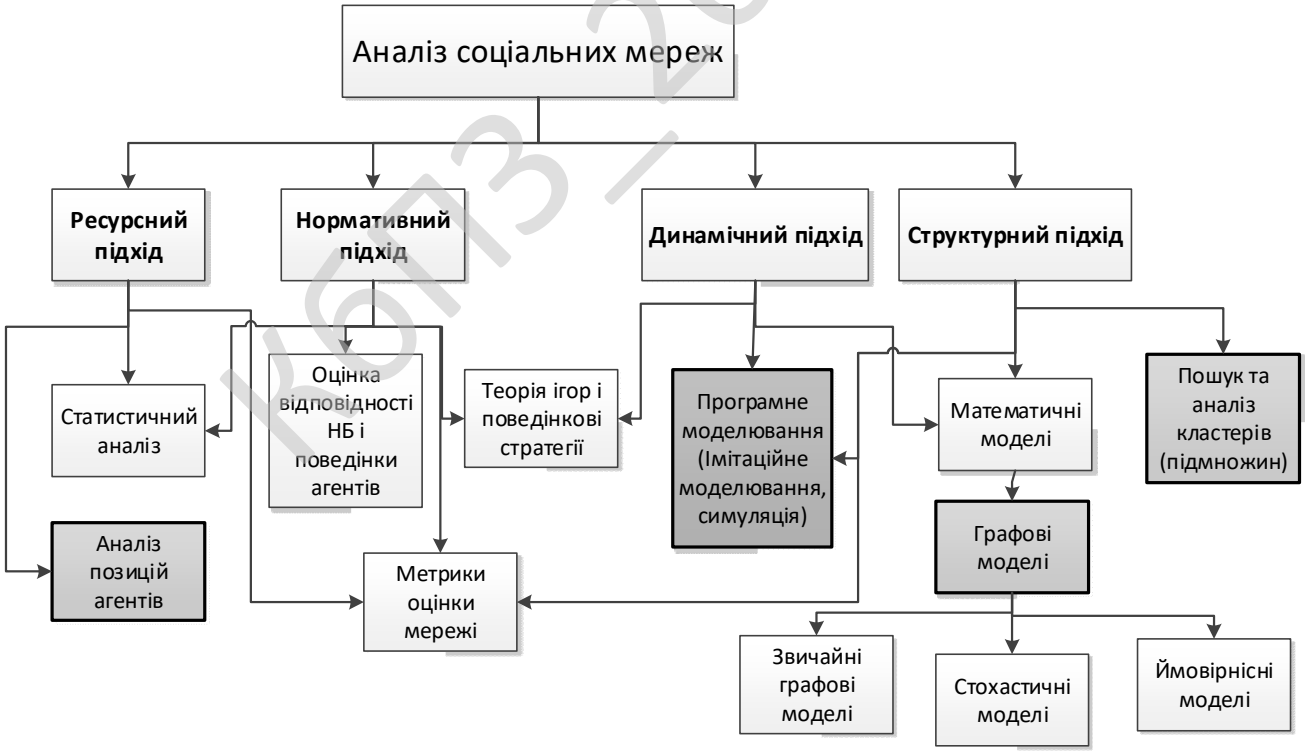

Рисунок 1.1 – Підходи і методи аналізу соціальних мереж

Процес спілкування та функціонування особистих сторінок користувачів має низку особливостей:

- сторінки мають низький ранг у алгоритмах ранжування сторінок, що утруднює пошук цих сторінок;

- велика кількість сторінок угруповань не ранжують глобальні пошукові системи;

- отримати доступ до інформації у дискусіях соціальних мереж може лише зареєстрований користувач соціальних мереж, а у закритих дискусіях – лише учасник дискусії;

- значна частина відвідувачів потрапляє на сайт за безпосередньою рекомендацією інших користувачів;

- взаємопов'язаність сторінок дискусій;

- збереження дискусій неактуальної тематичної спрямованості;

- анонімність чи спотворення даних себе самими користувачами соціальних мереж.

Вищезазначені особливості інформаційного обміну та функціонування окремих спільнот у СС дозволяють використовувати СС як інструмент інформаційного впливу. Соціальні мережі створюють нові загрози, оскільки дуже складно, інколи й неможливо контролювати їх у повному обсязі[31].

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Враховуючи тематику дослідження, важливо розглянути основні класи та представників моделей, створених для опису процесів інформаційного впливу та розповсюдження повідомлень у соціальних мережах. Використання моделей дає змогу проводити аналітичні експерименти, спостерігати динаміку поширення контенту та оцінювати поведінкові реакції користувачів. Саме тому ці підходи є значущими у різних прикладних сферах. Наприклад, маркетологи застосовують моделі для прогнозування успішності рекламних кампаній та просування товарів, бізнес-аналітики використовують їх для оцінки поведінки споживачів, а політичні консультанти, PR-фахівці та політтехнологи - для оцінки ефективності інформаційного впливу, формування громадської думки та проведення кампаній переконання. Таким чином, моделювання дає змогу виявляти групові та індивідуальні переваги, визначати тренди та приймати стратегічно виважені рішення.

Одною з ключових функцій соціальних мереж є поширення інформаційного контенту, що може включати текстові пости, коментарі, аналітичні матеріали, аудіо- та відеофайли, новинні повідомлення, короткі меседжі тощо. Сукупність такого контенту створює інформаційне середовище соціальної мережі, яке постійно оновлюється.

Наявність значної кількості підходів до аналізу змусила дослідників класифікувати існуючі моделі. У науковій літературі [48] запропоновано виділяти чотири основні напрями підходів: **структурний**, **ресурсний**, **нормативний** та **динамічний**.

У структурному підході користувачі розглядаються як вершини графа, а зв’язки між ними — як ребра. Аналізується форма мережі, інтенсивність контактів, центральність та інші топологічні параметри.

Динамічний підхід фокусується на змінах структури мережі в часі: появі нових учасників, формуванні сталих груп, зміні щільності зв’язків тощо.

Надалі розглянуті моделі переважно належать саме до структурного та динамічного підходів або поєднують їх елементи.

Модель епідемії та похідні моделі

Перші спроби моделювання поширення інформації в мережах ґрунтувалися на аналогії з розповсюдженням інфекційних захворювань. Однією з найвідоміших є модель SIR (Susceptible – Infectious – Removed), запропонована Кермаком і МакКендріком [49]. У ній популяція поділяється на три групи:

S — потенційно сприйнятливі (готові прийняти інформацію),

I — носії (активні поширювачі),

R — ті, що втратили інтерес і більше не поширюють інформацію.

Модель описується системою диференційних рівнянь:

$$\begin{cases} \frac{dS}{dt} = -\frac{\beta IS}{N} \\ \frac{dI}{dt} = \frac{\beta IS}{N} - \gamma I, \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (2.1)$$

де β — середня частота «зараження», γ — швидкість «одужання» (втрата інтересу), N — загальна чисельність групи.

Проте в базовому вигляді модель не враховує зміну кількості учасників мережі в часі, тому згодом її розширили, додавши параметри μ (прибуття нових учасників) та δ (вибуття користувачів).

У 1965 році на основі ідей SIR була запропонована модель Дейлі—Кендалла, відома як «модель поширення чуток». Вона описує три групи:

U — інформовані ініціатори,

V — ті, хто сприйняв і поширює інформацію,

W — ті, хто не сприйняв або втратив інтерес.

$$\frac{\gamma V(V+W)}{N}. \qquad (2.2)$$

Модель враховує ймовірнісний характер впливу та ступінь сприйнятливості інформації.

Моделі на основі клітинних автоматів

У моделях клітинних автоматів кожен агент представлений клітиною, стан якої змінюється відповідно до стану сусідніх клітин:

$$y_j(t+1) = F(y_j(t), O(j), T), \qquad (2.3)$$

де O(j) — множина сусідніх агентів, F — правило переходу станів.

Такі моделі дозволяють враховувати локальні особливості взаємодій, у тому числі ефект «згасання новини» та різний рівень інтересу.

Порогові моделі та моделі незалежних каскадів

На основі поняття порога сформовано так звані порогові моделі. Їхній ключовий принцип полягає в поділі агентів соціальної мережі на дві групи: активних, які вже поширюють інформацію, та неактивних, що лише сприймають інформаційний вплив. У процесі моделювання розглядається ітераційна динаміка: з кожною новою взаємодією агент накопичує певну величину інформаційного впливу. Якщо ця величина досягає або перевищує індивідуальний поріг сприйнятливості, агент переходить у стан активного та починає поширювати інформацію далі. Перехід, як правило, вважається незворотним.

На основі поняття порога сформовано так звані порогові моделі. Їхній ключовий принцип полягає у поділі агентів соціальної мережі на дві групи: активних, які вже поширюють інформацію, та неактивних, що поки лише сприймають інформаційний вплив. У процесі моделювання розглядається

ітераційна динаміка: із кожним новим кроком взаємодії кожен агент накопичує певний рівень інформаційного впливу. Якщо цей рівень досягає або перевищує індивідуальний поріг сприйнятливості, агент переходить у стан активного та починає поширювати інформацію самостійно. Важливо, що перехід до активного стану зазвичай вважається незворотним, тобто агент не повертається назад у неактивну групу.

Якщо механізм накопичення інформаційного впливу описується лінійною функцією, такі моделі виокремлюють у спеціальний підклас – моделі з лінійним порогом. Вони дозволяють порівняно просто оцінити інтенсивність впливу оточення на поведінку окремих учасників мережі.

Нехай мережа представлена графом G=(V,E), де:

- V - множина агентів (вузлів),
- E - множина зв'язків між ними.

Для кожного вузла v∈V визначено:

- θv∈[0,1] - поріг активації,
- N(v)⊆VN(v) - множина сусідів (оточення),

w_{uv} - вага впливу агента u на агента v, причому

$\sum_{u \in N(v)} w_{uv} = 1.$

Тоді агент v стає **активним**, якщо виконується умова:

$$\sum_{u \in N(v)} w_{uv} \cdot A_u(t) \geq \theta_v,$$

(2.4)

Близькою за змістом є модель незалежних каскадів, однак її суттєва відмінність полягає у характері впливу між вузлами мережі. У цій моделі вузол v_i може вплинути на вузол v_j лише один раз і робить це з певною ймовірністю. Повторні впливи активного вузла на атакований вузол не проявляються. Якщо

вплив виявився ефективним, то вузол v_j активується і продовжує поширення інформації далі. Якщо ж спроба виявилася невдалою, повторної взаємодії між цими двома вузлами вже не відбувається. Через таку специфіку модель часто розглядають у межах класу систем взаємодії незалежних частинок.

Якщо механізм накопичення інформації описується лінійною функцією, такі моделі класифікують як моделі з лінійним порогом.

Порівняння моделей

Порівняння моделей ускладняються і вибором критеріїв для порівняння та різною внутрішньою структурою та математичною природою моделей. Зрозуміло той факт, що кожна з моделей має свій напрямок і базується на певних відокремлених із реального процесу компонентах: окремо взяті характеристики та властивості.

Запропонована нижче порівняльна таблиця не розподіляє моделі на «кращі» та «гірші», а лише визначає характеристики, що враховуються моделями.

Таблиця 2.1 – Порівняння розглянутих моделей

Модель	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**	**К8**	**К9**
Модель епідемії	-	-	-	+	-	-	-	+	-
Модель із порогами	+	+	+	-	-	+	-	-	-
Модель незалежних каскаді	+	+/-	-	+	-	+	-	-	-
Клітинні автомати	+	+	+	-	-	+	-	+/-	-
Модель на основі ланцюгів Маркова	+	-	-	+	-	-	-	+	+/-
Теоретико-ігрові моделі	+	+	+/-	+/-	+/-	+	+	-	+/-

Позначення таблиці 2.1: К1 – зміна думки під впливом оточуючих агентів; К2- вплив структурних особливостей кола агента та структури мережі в цілому; К3-різна ступінь схильності агентів до ІВ; К4-наявність імовірнісних параметрів; К5 - облік активності агента; К6-оптимізація ІВ; К7-поведінкові стратегії агентів (ігрова взаємодія); К8 - оцінка ймовірності певного результату та розподіл агентів у певний момент часу; К9 - параметризація особистісних якостей агента.

Порівняння моделей показує, що кожна враховує лише частину значущих характеристик (табл. 2.1). Особливо слабким місцем багатьох класичних моделей є

те, що вони припускають однакову поведінку всіх агентів. Насправді ж кожен користувач має власні інтереси, рівень активності, мотивації та стратегії прийняття рішень. Саме тому найбільш перспективними вважаються теоретико-ігрові моделі, які дозволяють враховувати індивідуальні стратегії та репутаційні взаємодії, хоча їх математична реалізація є складнішою.

У підсумку, жодна з моделей не дає повністю комплексного опису процесу поширення інформації. Найбільш адекватні результати отримуються при комбінуванні різних підходів і врахуванні індивідуальних характеристик агентів, особливо на етапі запуску інформаційної хвилі.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Цей інструмент був вибраний з кількох причин. Одна з яких це платформа, під яку розробляється система. Так як цільова ОС це операційна система Microsoft Windows, немає нічого кращого, ніж взяти інструментарії, який розроблявся спеціально для цієї платформи. Тому що саме розробник операційної системи знає всі її особливості, і ніхто краще за нього не зможе врахувати всі нюанси цієї платформи.

Visual Studio 2021 – входить до лінійки продуктів Visual Studio, яку підтримує та постійно розвиває Microsoft, і призначений для розробки програмного забезпечення, а також інструмент включає низку інструментальних засобів. Цей продукт дозволяє розробляти консольні програми, а також програми з графічним інтерфейсом, однією з особливостей якого є підтримка технології Windows Forms. Крім цього можна розробляти веб-сайти, веб-додатки, веб-служби.

Орієнтовані платформи цього продукту Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, Xbox, Windows Phone .NET Compact Framework та Microsoft Silverlight.

Visual Studio включає редактор вихідного коду з підтримкою технології IntelliSense і можливістю найпростішого рефакторингу коду. Вбудований налагоджувач може працювати як налагоджувач рівня вихідного коду, так і як налагоджувач машинного рівня. Інші вбудовані інструменти включають редактор форм для спрощення створення графічного інтерфейсу програми, веб-редактор, дизайнер класів і дизайнер схеми бази даних.

Visual Studio включає такі компоненти:

– Visual Basic .NET, а до появи - Visual Basic.

– Visual C++.

– Visual C#.

– Visual F# (включено з Visual Studio 2010).

Ми будемо використовувати мову програмування C#.

C# це об'єктно-орієнтована мова програмування. Він був розроблений у 1998 році, групою програмістів та інженерів у компанії Microsoft. Як платформа для додатків використовується .NET Framework.

Сама мова відноситься до сімейства мов, які мають C подібний синтаксис. Найбільш близький він із C++ та Java.

Мова строго типізована, у ній організована підтримка поліморфізму, підтримка операторів, делегати, атрибути, події, властивості, узагальнення типи та методи, ітератори та інше.

Особливістю мови є те, що вона залежить від можливостей CLR. Насамперед це стосується системи типів мови. Завдяки CLR C# має багато можливостей, яких позбавлені деякі мови програмування, наприклад CLR надає складання сміття, що робить програму більш стабільною.

Мова C# розроблявся як базова мова для платформи .NET. Платформа .NET характерна підтримкою проектів з використанням одночасно декількох мов програмування. У той же час C# є основною мовою, на неї орієнтована основна підтримка: розробка нових бібліотек, технічна підтримка, документування[28].

C# має деякі запозичення з мови Java, але їх схожість досить перебільшена. Більш правильним буде висловлювання - мова C# об'єднує в собі зручні конструкції і потужні інструменти багатьох мов, в першу чергу варто згадати C ++, Java, VisualBasic. У той же час багато моментів суттєво спрощені для розробника - не потрібно використовувати явний деструктор, роль покажчиків істотно спрощена в порівнянні з C ++, контроль пам'яті багато в чому автоматизовано [15, 17, 20].

Варіативність середовища, з точки зору типу проектів і мови програмування, представлено на рис. 2.1.

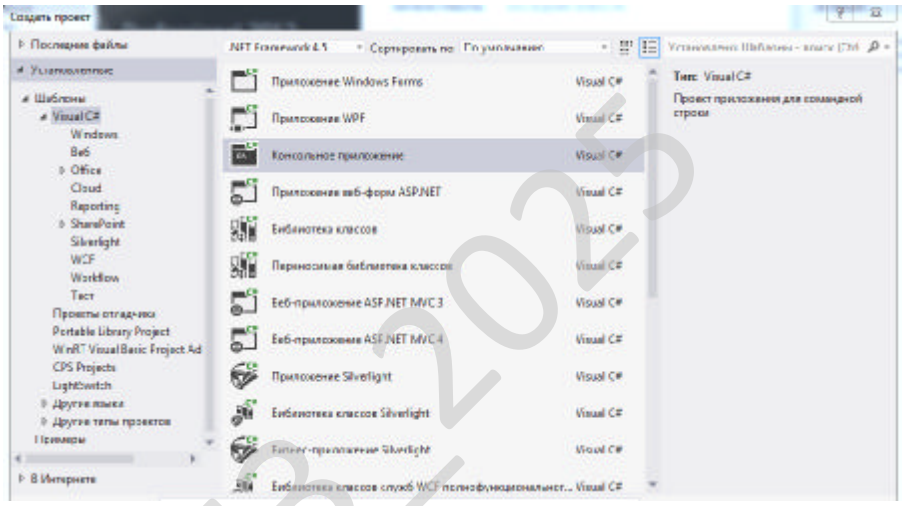

Рисунок 2.1 – Вибір типу проекту та мови програмування

Ось кілька переваг і особливостей мови C# у порівнянні з її найближчими «родичами»:

1. В C# відсутня пряма необхідність у використанні покажчиків, оскільки механізм покажчиків приховано від розробника і застосовується лише побічно.

2. Управління пам'яттю, зокрема видалення невикористовуваних об'єктів і очищення пам'яті, автоматизовано завдяки технології «Збірка сміття». У C# немає операції delete.

3. Мова надає ряд формальних шаблонів і конструкторів для класичних конструкцій, делегатів тощо.

4. Підтримується перевантаження методів, яке спрощене в порівнянні з C++.

5. Є можливість автоматизованого використання анотацій, що дозволяє уточнювати поведінку членів класу.

6. Мова підтримує типізовані запити LINQ, що орієнтовані на різні типи даних, суттєво розширюючи можливості обробки даних.

7. Анонімні типи визначають лише структуру, не накладаючи обмежень на поведінку.

8. Методами розширення можна додавати нові функціональні можливості до існуючих типів.

9. Лямбда-вирази (оператор =>) значно спрощують роботу з делегатами.

10. Можливість ініціалізувати властивості об'єкта безпосередньо при його створенні.

З кожним новим оновленням .NET з'являються нові можливості для мови C#, і остання версія не стала винятком. Варто зазначити, що деякі функції та інструменти, які вже вважаються застарілими з точки зору розробників Microsoft, більше не підтримуються. Це не має критичного значення для нових додатків (для яких існують нові, більш потужні або зручні інструменти), але може створити проблеми для старих проектів, які потребують оновлення та підтримки. Відсутність підтримки застарілих функцій може стати серйозною перешкодою, що потребує значних витрат на адаптацію проекту до нових умов [20].

2.3 Розгорнута постановка завдання

У сучасному суспільстві інформація стала ключовим ресурсом, який визначає розвиток соціальних, економічних та політичних процесів. Соціальні мережі (СС) виконують роль головного каналу обміну інформацією між мільйонами користувачів і водночас стають інструментом впливу на громадську думку, маркетингові стратегії, політичні кампанії та інформаційні протистояння.

Комплексне дослідження цих процесів у поєднанні з програмною реалізацією моделей розповсюдження інформації дозволяє:

- виявляти ключові вузли та групи впливу в соціальних мережах;
- аналізувати динаміку інформаційних потоків;
- оцінювати вплив індивідуальних і групових характеристик агентів на процеси розповсюдження;
- створювати інструменти для стратегічного планування інформаційних кампаній.

Мета і завдання дослідження

Мета дослідження – розробити та реалізувати програмну систему моделювання поширення інформації в соціальних мережах на основі класичних та сучасних моделей, з можливістю порівняння їх ефективності та динаміки розповсюдження.

Для досягнення цієї мети необхідно вирішити такі завдання:

1) Провести аналіз літературних джерел та сучасних підходів до моделювання розповсюдження інформації в соціальних мережах, виділити основні моделі та методи:

- Моделі епідемій (SIR, DK-модель);
- Моделі на основі клітинних автоматів;
- Порогові моделі та моделі незалежних каскадів;
- Теоретико-ігрові моделі та моделі на основі ланцюгів Маркова.

2) Класифікувати моделі за основними критеріями: структурний підхід, ресурсний підхід, нормативний підхід та динамічний підхід.

3) Розробити програмну реалізацію обраних моделей із можливістю:

- налаштовувати параметри агентів та мережі;
- візуалізувати процеси поширення інформації;
- проводити експерименти із різними сценаріями інформаційного впливу;
- збирати статистичні дані для аналізу результатів.

4) Провести порівняльний аналіз ефективності моделей за кількома критеріями: швидкість поширення інформації, охоплення мережі, вплив активності окремих агентів, роль структурних характеристик мережі.

5) Розробити рекомендації щодо використання моделей для прогнозування поширення інформації, оцінки впливу агентів та планування інформаційних кампаній.

Методологія дослідження

Для досягнення поставлених завдань передбачається застосування таких методів:

1. Теоретичні методи – аналіз наукових публікацій, систематизація моделей та їхніх характеристик, класифікація методів моделювання;

2. Математичне моделювання – використання теорії графів, систем диференціальних рівнянь, клітинних автоматів, теорії ймовірностей та статистики;

3. Програмна реалізація – розробка симуляційної системи для моделювання процесів розповсюдження інформації з можливістю візуалізації та зміни параметрів мережі;

4. Емпіричні методи – порівняння результатів моделювання з реальними даними соціальних мереж (Facebook, Twitter, LinkedIn), оцінка адекватності моделей.

Очікувані результати:

Побудова та програмна реалізація моделей розповсюдження інформації у соціальних мережах;

Виявлення найбільш впливових агентів та груп;

Проведення порівняльного аналізу моделей за ключовими критеріями ефективності;

Розробка методичних рекомендацій для використання моделей у маркетингу, політичних кампаніях та інформаційній безпеці.

Постановку завдання дослідження можна конкретизувати в такий спосіб.

В рамках дослідження необхідно реалізувати такі завдання:

- запропонувати методи генерації сегмента мережі;

-математичний формалізований опис вузлів мережі на основі вибраного набору параметрів;

- формалізувати процес інформаційного обміну;

- на основі запропонованих моделей реалізувати програмну симуляцію процесу поширення інформації у мережі;

- провести експерименти щодо виявлення чинників, сприяють/перешкоджаючих підвищенню швидкості поширення інформації;

- запропонувати методи вибору вузлів для інформаційних атак під час реалізації стратегій поширюючи ІВ.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Функціонування системи передбачає 4 основних етапи:

- генерація мережі з заданими параметрами;
- розміщення/вибір позицій генераторів;
- вибір стратегій їх роботи;
- збереження та аналіз результатів експериментів.

Зупинимось на деяких з вище зазначених етапів.

Запропоновано метод створення мережевої структури, який полягає в комбінуванні різних підмножин кластерів з параметризацією. У базовому варіанті передбачається використання трьох типів кластерів: групи, лідерської групи та кліки. Основним параметром при генерації кластерів є кількість вузлів, а додатковим - відсоток вузлів з високим рівнем інформаційного опору, який був введений після проведення експериментів.

Структура мережі складається з набору базових кластерів, параметри яких визначаються під час їх генерації. Для можливості редагування структури та створення мереж з певними характеристиками пропонується додати функціональність для додавання чи видалення вузлів, а також для додавання або вилучення зв'язків. Візуальне розташування вузлів у програмному конструкторі не впливає на саму мережеву структуру, оскільки вона визначається лише наявністю зв'язків між вузлами. Лінійна відстань між вузлами може бути довільною, головне - розмістити їх на екрані так, щоб усі вузли були видимими. Це має лише візуальне значення, не впливаючи на процес обміну інформацією чи результати експериментів. Візуалізація структури допомагає експериментатору краще сприймати мережу, аналізувати її структурні особливості та вносити зміни в ході

експерименту, наприклад, збільшувати щільність зв'язків або додавати вузли з певними характеристиками.

Оскільки вузол є базовим елементом мережі, а програмна модель використовує об'єктно-орієнтований підхід, варто почати з розгляду цього елементу. Вузол в програмній моделі реалізується як окремий клас, реалізація якого наведена в розділі 4.

Далі розглянемо метод генерування однієї з кластерів з прикладу лідерської групи. Лідерська група (див. рис. 3.1) характерна наявністю вузла, що має зв'язок з усіма іншими вузлами мережі.

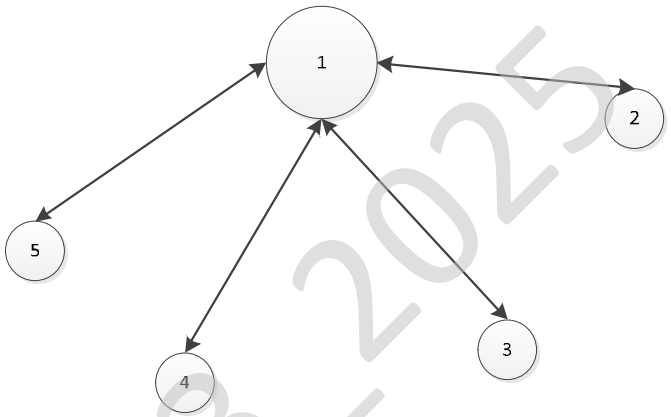

Рисунок 3.1 – Кластер типу «Лідерська група»

Цей метод передбачає кілька складових етапів:

1 Етап. створення масиву точок, що визначають візуальне положення вузлів на екрані;

2 Етап. Створення самих вузлів (визначення індивідуальних параметрів) та додавання їх до загального масиву вузлів мережі;

3 Етап. встановлення структурних особливостей відповідно до обраного типу кластера (створення зв'язків між вузлами);

4 Етап. Внесення змін до матриці суміжності.

Кожен тип кластера в конструкторі має обмеження на кількість вузлів зверху, при встановленні параметрів користувач може встановити значення даного параметра (int countUsers) в запропонованих конструктором мережі межах. Крім

кількості вузлів метод передається центральна точка, визначальна місце розташування кластера на екрані, положення інших вузлів кластера розраховується щодо даної точки. Розташування вузлів на екрані не має жодного впливу на поведінку моделі та реалізовано лише для зручності проведення експериментів.

3.2 Розробка структурної схеми

Об’єм роботи не дозволяє детально описати всі етапи реалізації моделі та її експериментального застосування. Тому в окремих пунктах вирішено висвітлювати лише вибрані етапи.

В попередньому пункті було описано етап генерування структури мережі. Розглянемо структурну схему процесу (рис. 3.2)

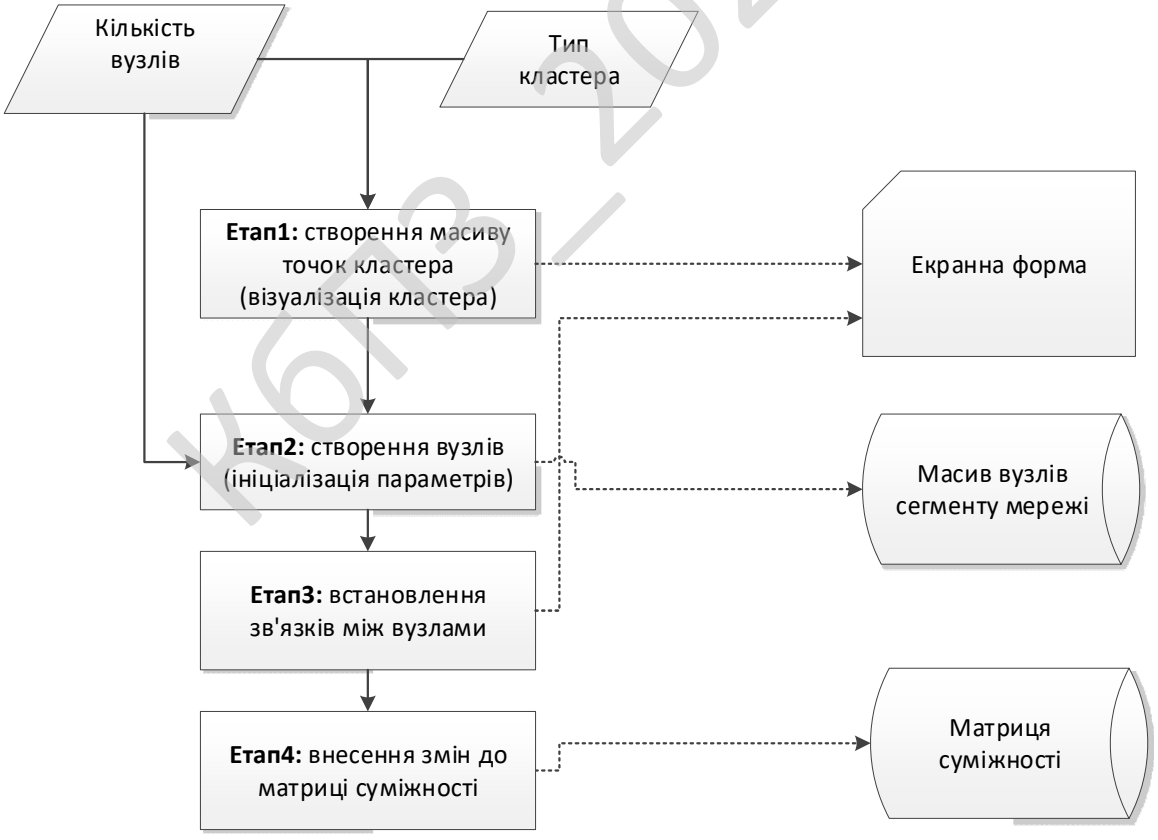

Рисунок 3.2 – Структурна схема генерування мережі

Окремим пунктом є ініціалізація параметрів окремих вузлів мережі, що суттєво буде впливати на кінцевий результат. Для первинної ініціалізації пропонується застосувати наступні формули:

Active_Node(V_i) = rnd(1, CC),

де CC – множина контактів вузла **V_i,**

Reputation_Node(V_i) = rnd(1,90),

Opposite_Node(V_i) = rnd (10,800),

Involvement_Node(V_i) =0.

Для вузла, що є лідером групи, враховуючи вище описані міркування значення параметрів активності, репутації та спротиву дещо вищі, порівняно з іншими вузлами в кластері:

Active_Lider_Node(V_i) = [0.7* КК],

Reputation Lider_Node(V_i) = 100 - rnd(20),

Opposite Lider_Node(V_i) = 500 +random (500),

Involvement Lider_Node(V_i) =0

Лістинг 3.1 – Метод реалізації кластеру типу «Лідерська група»

```
internal void AddLiderGroup(Point point_, int countUsers )
     {
     // Check if the central point is within the permissible limits
     if (point_.Y > 90 && point_.Y < 620)
     {
          //Buffer array of points corresponding to nodes
     Point[] mas_PointBuf = new[]
     {
     //Creating points, initializing offset coordinates
     new Point(0, 0),
     new Point(10, 10),
     new Point(20, 10),};
//Creating an array of points according to the specified number of nodes
     Point[] mas_Point = new Point[countUsers];
//Cycle of assigning a location to each node
     for (int i = 0; i < countUsers; i++)
     {mas_Point[i]=mas_PointBuf[i];}
//Creating a list of cluster nodes
     var us_List = GenarateUser_List(point_, mas_Point, Us_List.Count).ToList();
//Determining a random node to be assigned the role of group leader
     Random random = new Random();
     int leader = random.Next(0, countUsers);
//Setting node characteristics
     for (int i = 0; i < us_List.Count; i++)
          {if (i==leader)
```

```
                {for (int j = 0; j < countUsers; j++)
                     {//If the node is a group leader
                     if (i!=j)
                     {
                     us_List[i].FriendsList.Add(us_List[j]);
                     us_List[j].FriendsList.Add(us_List[i]);
                     us_List[i].Activity = (int) 0.7*countUsers;
                     us_List[i].Opposite = 500 + random(500);
                     us_List[i].Involvement = 0;
                us_List[i].Reputation = 100 - random(20); }
                }
                }
else
     {
int count = random.Next(0, 2);
     for (int j = 0; j < count; j++)
          {
               int user = random.Next(0, countUsers);
               if (i != user && !us_List[i].FriendsList.Any(x=>x.Name==
          us_List[user].Name))
               {
                    us_List[i].FriendsList.Add(us_List[user]);
                    us_List[user].FriendsList.Add(us_List[i]);
                    us_List[i].Activity = random.Next(1,
               us_List[user].FriendsList.countUsers);
                    us_List[i].Opposite = random.Next(10,800);
                    us_List[i].Involvement = 0;
                    us_List[i].Reputation = random.Next(1,90);
               }
               }
          }
     //Making changes to the adjacency matrix
          AddMatrix (us_List[i]);
          }
          //adding the list of cluster nodes to the general list of network nodes
          Us_List.AddRange(us_List);}
     }
```

3.3 Розробка функціональної схеми

Функціональна схема взаємодії компонентів програмного забезпечення з описом інформаційних потоків, складу даних в потоках та послідовності виконання етапів показана на рис. 3.3.

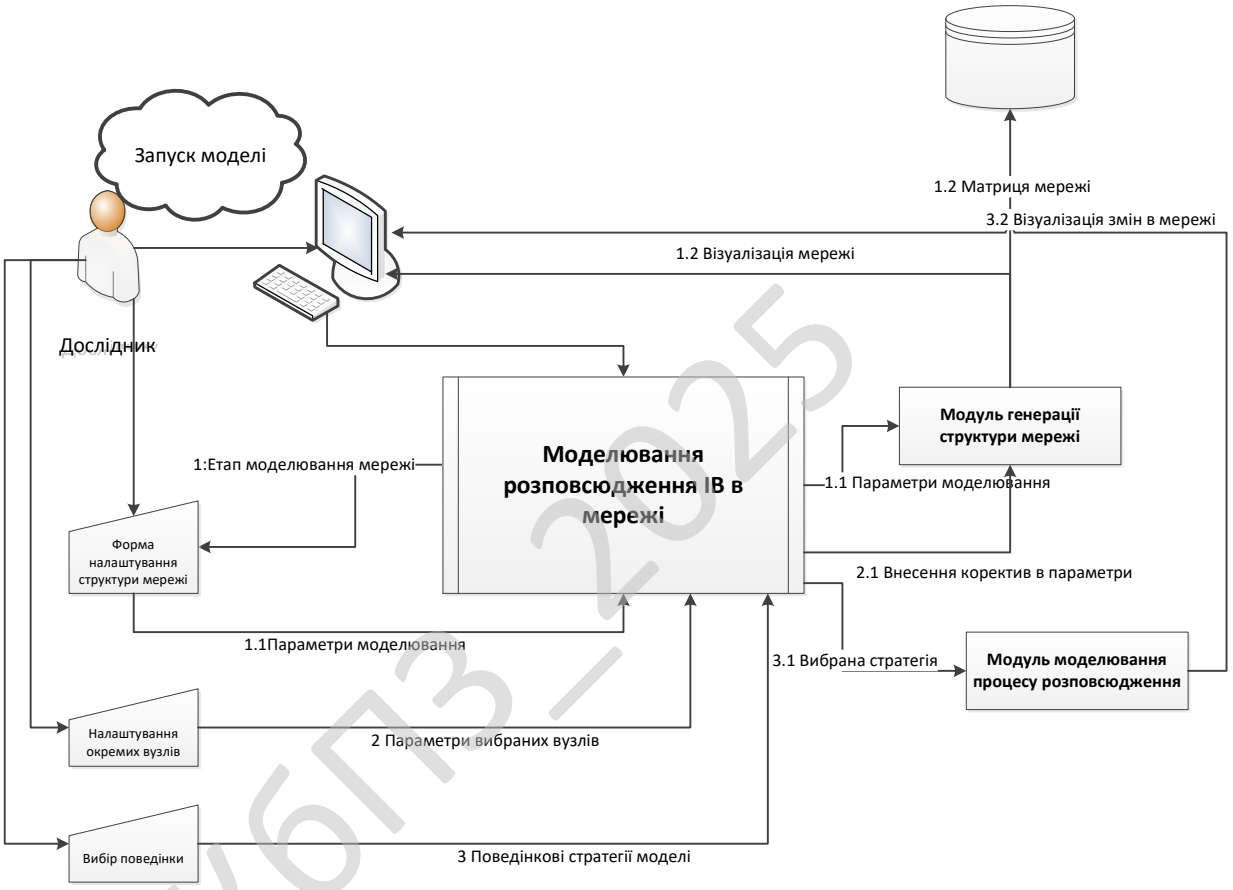

Рисунок 3.3 – Функціональна схема взаємодії з програмною моделлю

Після запуску моделі (програмного застосунку для моделювання) користувач створює структуру мережі. Цей процес базується на використанні кластерних шаблонів. Один з таких шаблонів описано вище.

Далі користувач має змогу внести корективи в згенеровану структуру, додаток дозволяє корегувати окремі вузли, додавати їх або вилучати.

Наступним етапом є вибір положення генератора, що, фактично, теж відноситься до внесення коректив в структуру.

Після завершення коректив структури мережі і вибору позиції генератора впливу обирається поведінкова стратегія, яку має застосовувати генератор в моделі.

Останній етап – безпосередньо моделювання розповсюдження вплив у та опрацювання накопичених даних, що представляються користувачеві у вигляді графіків.

3.4 Розробка діаграми процесів

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування).

В нашому випадку така діаграма буде певною мірою доповнювати та деталізувати функціональну схему в частині взаємодії користувача та програми, а також внутрішньо-модульні обміни даними в середині самої програми.

Діаграма процесів представлена на рис. 3.4

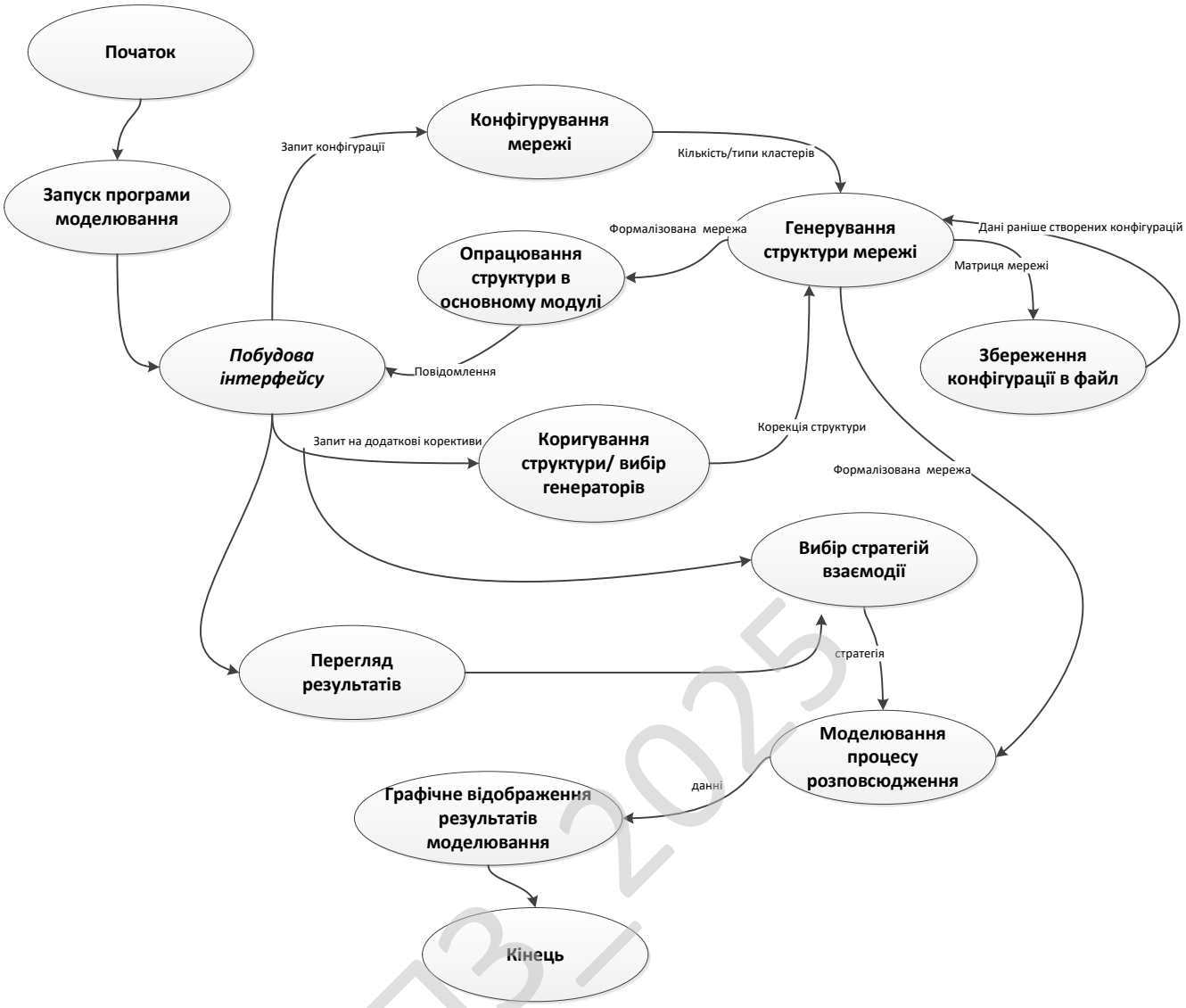

Рисунок 3.4 – Діаграма процесів системи

Як видно з діаграми (рис. 3.4), процеси програми можна розділити на процеси користувача та внутрішні процеси системи.

Внутрішні процеси ініціює користувач. Через наявні інтерфейсні елементи користувач має змогу задавати основні параметри та корегувати окремі елементи моделі. По завершенню процесу моделювання користувач отримує візуалізацію результатів в вигляді графіку, що демонструє швидкість зростання розповсюдження інформаційних впливів по мережах.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Блок-схеми є одним з варіантів ілюстрування алгоритмів. Але вони доречні у випадку структурного програмування. В нашому випадку програмний комплекс реалізовано в об'єктній парадигмі програмування, більше того сценарій залежить від дій користувача і не є повністю детермінованим.

За допомогою блок-схем проілюструємо стратегії, що реалізовані в програмному комплексі для моделювання.

Модель, що реалізується в програмному комплексі, передбачає, що коли вузол приєднується до ідеї, він запозичує у атакуючого вузла й відповідну стратегію поширення. Іншими словами: якщо в мережі діє генератор ідеї з певною стратегією $F1(P_1P_2 \dots P_i, \{Vj_g\})$, всі залучені ним вузли надалі поводяться за тією ж стратегією, тобто наслідують її.

Найпростіший варіант - коли генератор вибирає цілі випадково. Така «безаналізна» поведінкова стратегія (назвемо її «кущ») формалізується так:

$$P_{bush} = \{u_i \in U_g | i = random(|U_g|), |u| \leq Act_g\}, \quad (4.1)$$

тобто з множини доступних контактів U_g випадковим чином обираються вузли, причому їхня кількість не перевищує активність генератора Act_g. Перевага цієї стратегії - відсутність затрат часу на аналіз: зекономлені ресурси перенаправляються на здійснення більшої кількості атак за одиницю часу, що робить її ефективною при масових, швидких кампаніях (див. схему на рис. 4.1).

Рисунок 4.1 – Блок-схема простої стратегії («Кущ»)

Проте існують і складніші багатокритеріальні підходи. Стратегії, які включають аналіз і вибір вузлів за певними ознаками, можуть давати вищу ефективність, але вимагають додаткового часу на обробку інформації. Одна з цілей моделювання - експериментальна оцінка ефективності різних стратегій залежно від структури сегменту мережі та початкового положення генератора.

Найпростіша характеристика для відбору цілей - число зв'язків вузла (у соціальних мережах - кількість друзів). Інтуїтивно, вузли з великою кількістю контактів є більш перспективними для залучення: успішна атака на такий вузол значно розширює канал поширення. Однак вибір «впливових» вузлів потребує часу на аналіз, отже генератору доводиться жертвувати інтенсивністю (зменшувати кількість одночасних діалогів) порівняно зі стратегією «кущ». У рамках цієї аналітичної стратегії атакуючі звернення можуть повторюватися до одного й того ж вузла протягом ітерації - доки накопичена «залученність» не перевищить встановленого порогу, після чого атакований вузол сам перетворюється на генератор і починає поширювати ідею. Зі зростанням числа генераторів у мережі кількість вузлів, обраних для атаки наступними генераторами, також може збільшуватися.

Цю стратегію зручно позначити як «дерево». Формально вона задається так:

$$P_{тев} = \{u_i \in U_g \mid |U_{u_i}| \to max, |u| = 2^{l\_g}, |u| \leq K * Act_g, u_i \notin Gen\}, \quad (4.2)$$

де $u_i \in U_g$ – користувачі в околі генератора; $|U_{u_i}| \to max$ – кількість вузлів-контактів атакованого вузла, що є критерієм вибору вузла для атаки (за принципом максимуму); $|u| = 2^{l\_g}$ – кількість вузлів для атаки залежить від рівня генератора.

Для балансування між «швидкою» (без аналізу) і «цілленною» (з аналізом) стратегіями можна вибрати K=0,5. Атака на вузол триває, доки він не стане генератором ($u_i \notin Gen_{u\_i}$).

Ідея «дерева» полягає в швидкому захопленні вузлів з великою кількістю контактів і побудові підмережі поширення. Зі збільшенням рівня генератора кількість одночасних цілей зростає, що знижує інтенсивність окремого генератора (через розподіл зусиль), але компенсується сумарним ефектом кількох генераторів у мережі. Після першочергового відбору й залучення перспективних вузлів

доцільно перемикатись на стратегію «кущ»: спрямувати зусилля на масове поширення без додаткового аналізу, використовуючи вже відібраний набір контактів як спрямовуючу структуру для подальшого росту (див. рис. 4.2).

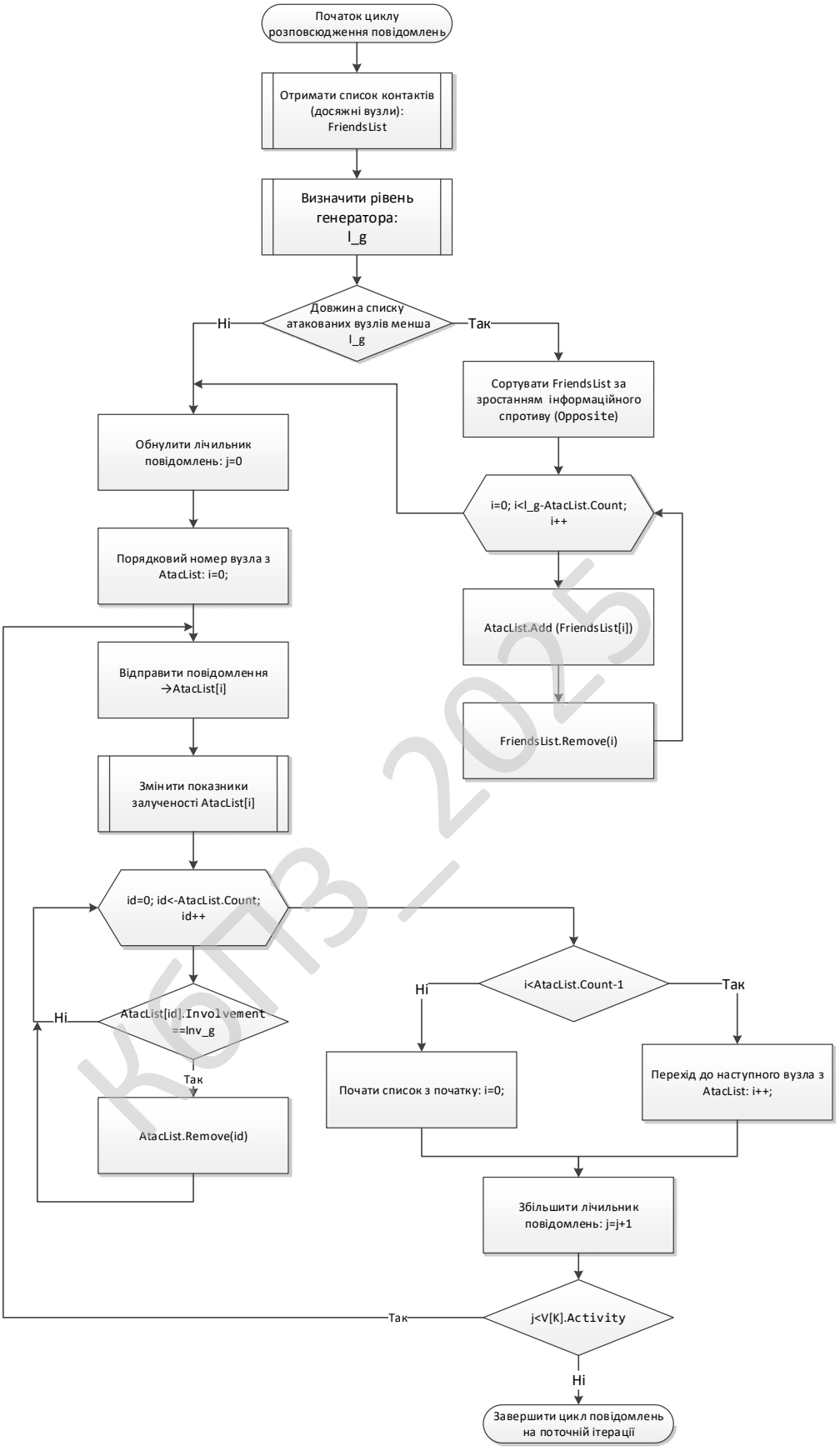

Рисунок 4.2 – Блок-схема стратегії з аналізом

4.2 Захист розробленого програмного забезпечення

Захист розробленого програмного забезпечення здійснюватиметься за допомогою RC6 - симетричного блочного криптографічного алгоритму, який є подальшим розвитком RC5. Алгоритм був створений Роном Рівестом, Меттом Робшау та Реєм Сіднеєм із метою участі в конкурсі на визначення нового стандарту шифрування AES. RC6 увійшов до п’ятірки фіналістів цього конкурсу, а також був поданий до проєктів NESSIE і CRYPTREC. Спочатку алгоритм мав пропрієтарний статус і був запатентований компанією RSA Security, однак термін дії патентів завершився, і сьогодні RC6 перебуває у відкритому доступі. Водночас назва "RC6" залишається зареєстрованою торговою маркою RSA.

Версія алгоритму RC6, подана на конкурс AES, працює з блоками даних обсягом 128 біт і підтримує ключі довжиною 128, 192 та 256 біт. Подібно до RC5, RC6 є параметризованим і може бути налаштований на використання ширшого діапазону розмірів блоків і ключів (від 0 до 2040 біт). Алгоритм зберігає загальну структурну схожість із RC5 та вирізняється простотою реалізації.

Попри те, що RC6 був одним із претендентів на роль нового стандарту AES, його продуктивність на деяких апаратних платформах виявилася нижчою, ніж очікувалося. Це пов’язано з використанням операції множення, яка виконується повільніше на певних типах процесорів. Неочікувано низька ефективність була зафіксована і на системах з архітектурою Intel IA-64. Через це алгоритм втрачає одну з основних своїх переваг — високу швидкість, що стало одним із ключових чинників, які перешкодили його обранню як нового стандарту шифрування.

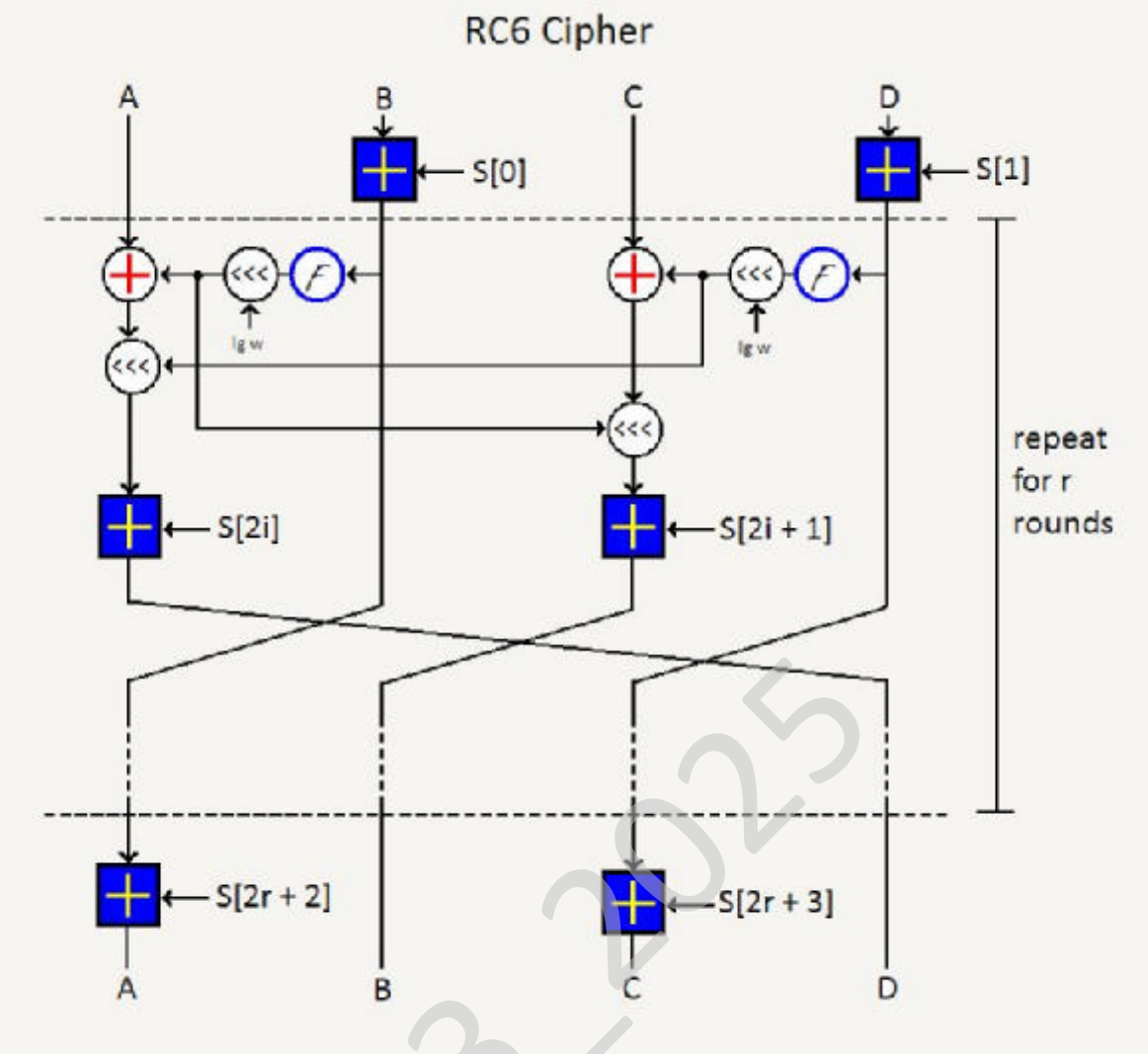

Рисунок 4.3 – Структура RC6

Деталі RC6

Так само, як і RC5, RC6 – повністю параметризована сім'я алгоритмів шифрування. Для специфікації алгоритму з конкретними параметрами, прийнято позначення RC6-w/r/b, де

– W – довжина машинного слова в бітах.

– R – число раундів.

– B – довжина ключа в байтах. Можливі значення 0 .. 255 байт.

Для того щоб відповідати вимогам AES, блочний шифр повинен працювати з 128-бітовими блоками. Так як RC5 – виключно швидкий блочний шифр, розширення його, щоб працювати з 128-бітовими блоками, привело б до

використання двох 64-бітових робочих регістрів. Але архітектура і мови програмування ще не підтримують 64-бітні операції, тому довелося змінити проект так, щоб використовувати чотири 32-бітних регістри замість двох 64-бітних.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

В даному розділі буде представлено опис застосування розробленої програмної моделі та деякі результати отримані в ході моделювання. Розроблювальна система не є прикладною програмую і описувати її впровадження в промислову експлуатацію не можливо.

Для перевірки ефективності запропонованих поведінкових стратегій було проведено серію експериментів на розробленій програмній моделі. Було змодельовано мережу, що складається з кластерів різних типів: груп, лідерських груп, а також додаткових вузлів і зв'язків. Зовнішній вигляд мережі наведено на рис. 5.1. Генератор ідеї було розміщено в розрідженій частині мережі (позначено на рисунку). Загальна кількість вузлів становила 180.

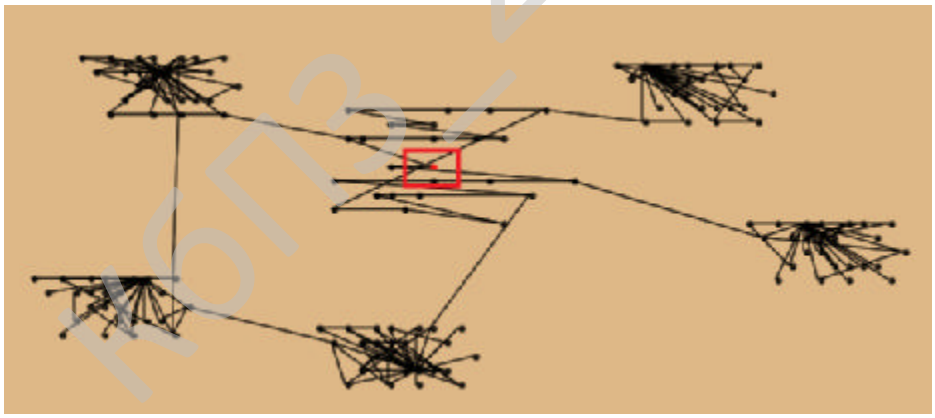

Рисунок 5.1 – Змодельований сегмент мережі для експерименту (150 вузлів)

Результати моделювання із застосуванням різних поведінкових стратегій подано на рис. 5.2, де «1» позначає стратегію **«дерево»**, а «2» — **«кущ»**.

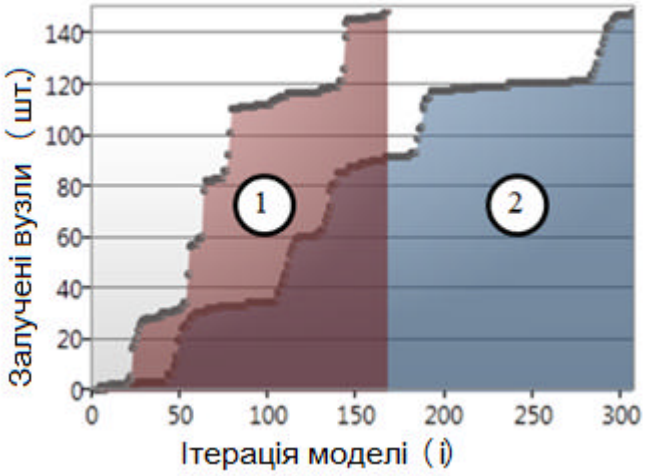

Рисунок 5.2 – Графіки залучення вузлів до ідеї за різними стратегіями генераторів

Як видно з графіків (рис. 5.2), для повного поширення ідеї мережею за стратегією **«дерево»** знадобилося приблизно 160 ітерацій. На тому ж часовому етапі стратегія **«кущ»** забезпечила залучення близько 60% вузлів.

Після збільшення щільності зв'язків у мережі ситуація змінилася. На рис. 5.3 представлено графіки для випадку, коли щільність зв'язків підвищено на 40%, а також додано кілька вузлів-містків між кластерами (загальна кількість вузлів зросла до 200).

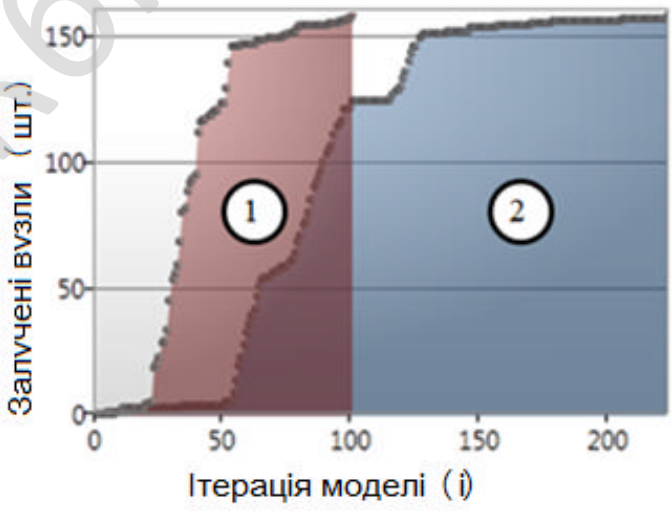

Рисунок 5.3 – Графіки залучення вузлів до ідеї за різними стратегіями генераторів після підвищення щільності зв'язків

Для перевірки гіпотези щодо впливу щільності зв’язків на ефективність стратегій було суттєво збільшено кількість вузлів і зв’язків, а також додано кластери з високою щільністю (кліки). У результаті мережа мала вигляд, показаний на рис. 5.4; кількість вузлів становила 220, при цьому позиція генератора залишилася незмінною.

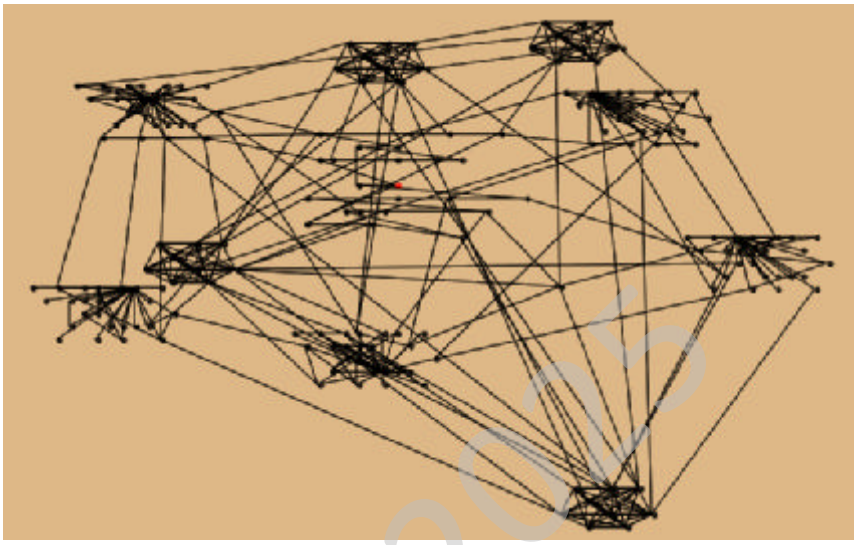

Рисунок 5.4 – Структура сегмента мережі після підвищення рівня щільності

На оновленій мережі обидві стратегії — **«кущ»** і **«дерево»** — продемонстрували майже однакові результати (рис. 5.5). Після сотого кроку моделювання обидві стратегії охопили практично всі вузли. Незначна різниця у швидкості захоплення вузлів пояснюється тим, що стратегія **«кущ»** використовує випадковий вибір цілей, а не аналітичний підхід.

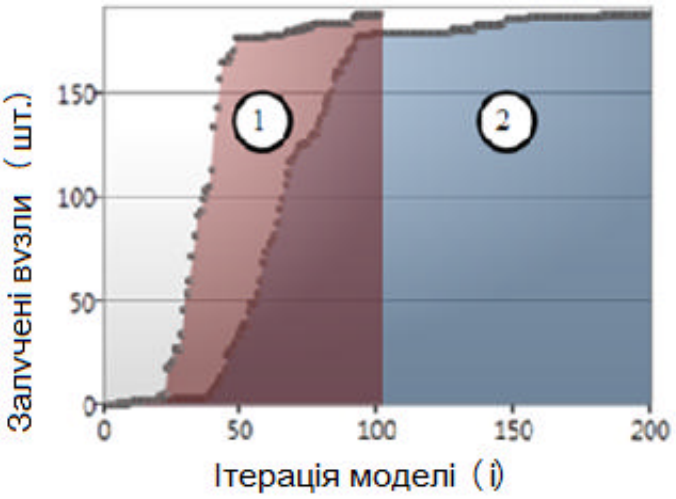

Рисунок 5.5 – Результати експерименту після істотного підвищення щільності зв’язків

У цілому стратегія **«дерево»** показала вищу ефективність, проте в ході експериментів було виявлено певні колізії. Зокрема, на початкових рівнях (1–2) вибір за критерієм максимальної кількості зв’язків може спрямовувати атаки на вузли з високим рівнем інформаційного опору (*Opposite*), що значно збільшує час їх переконання.

Аналіз отриманих результатів дозволяє зробити такі висновки:

- стратегія **«дерево»** має перевагу при середній щільності зв’язків у мережі;
- при низькій щільності (коли кожен вузол має небагато контактів) стратегія **«кущ»** завдяки своїй високій активності може випадково обрати потрібні вузли швидше;
- при високій щільності зв’язків обидві стратегії демонструють подібну ефективність, оскільки зростає кількість альтернативних шляхів поширення ідей, і головним чинником стає активність генератора.

Результати експериментів свідчать про такі закономірності:

1. Модель адекватно реагує на різні типи поведінкових стратегій.

2. Ефективність стратегій із вибором за критерієм зменшується у порівнянні з випадковими стратегіями при зростанні щільності зв’язків.

3. Графік залучення вузлів має ступінчасту структуру.

4. Різке зростання кількості залучених вузлів спостерігається після досягнення рівня 10–15% від загальної кількості.

Отримані результати підтверджують адекватність і достовірність моделі.

Пункти (1) і (2) є логічно передбачуваними, а (3) пояснюється появою генераторів у щільних ділянках мережі. Так, на структурі, що складається з п’яти кластерів із підвищеною щільністю зв’язків, графік (рис. 1) має п’ять чітко виражених сходинок. Після вирівнювання щільності мережі ці сходинки зникають, а темп зростання графіка підвищується (рис. 5.5).

Щодо пункту (4), отримані результати узгоджуються з висновками дослідників Політехнічного університету Ренсселаера [7], які встановили, що приблизно **10% залучених вузлів** здатні визначати інформаційні настрої всієї мережі та формувати вирішальний вплив.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для моделювання розповсюдження інформації в соціальних мережах та інформаційних впливів.

Предметом дослідження є соціальні мережі та методи моделювання соціальних мереж і моделі поширення в них інформаційних впливів.

Об'єктом дослідження є методи і стратегії поширення інформаційних впливів на соц. мережах та стійкість мереж до таких впливів.

Мета дослідження роботи – визначити фактори та характеристики мережі, а також способи вибору вузлів для атак у мережі, які сприяли б збільшенню швидкості поширення. Мета роботи визначає необхідність вирішення наступних **основних завдань**:

1. Дослідити методи генерації мереж та моделі поширення інформаційних впливів у соціальних.

2. Розробити математичну модель поширення інформаційних впливів у сегменті соціальної мережі з урахуванням особистісних характеристик вузлів мережі, що дозволяє на основі аналізу запропонованих характеристик застосувати різні поведінкові стратегії суб'єктами інформаційного впливу.

3. Удосконалити метод генерації сегмента соціальної мережі з можливістю моделювання різних наперед визначених варіантів структури сегмента мережі (топологій).

4. Провести експериментальні дослідження на програмній моделі, перевірити ефективність запропонованих методів з точки зору швидкості поширення інформаційних впливів.

Магістерська робота має елементи наукової новизни. Зокрема:

1) Вперше запропоновано математичну модель інформаційної взаємодії.

2) В роботі набуло подальшого розвитку поняття поведінкових стратегій, для яких запропонована формалізація та алгоритми їх реалізації.

Реалізована на основі запропонованої математичної моделі програмна модель може бути використана як інструмент подальших досліджень даного напрямку.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Постановка завдання для розрахунку

Проводиться оцінка основних характеристик програмного продукту, призначеного для проведення імітаційного моделювання та аналізу бізнес-активності підприємства. Моделювання проводиться у середовищі розробки iThink 9.0.2.

7.2 Обґрунтування функцій програмного продукту

Головна функція F_0 – використання програмного продукту, у який аналітик вносить вхідні дані та будує модель для аналізу та оцінки. Виходячи з конкретної мети, можна виділити наступні основні функції ПП:

F_1 – вибір базових моделей;

F_2 – інтерфейс користувача;

F_3 – робота з вхідними даними.

Кожна з основних функцій може мати декілька варіантів реалізації.

Функція F_1:

а) Метод «Швидкізлети та падіння»;

б) Метод “Just in Time”.

Функція F_2:

а) Інтерфейс користувача з підтримкою перемикачів, графіків та кнопок;

б) Інтерфейс користувача тільки з вікном для введення даних.

Функція F_3:

а) Робота з вхідними даними з підтримкою перемикачів, графіків та кнопок;

б) Робота з вхідними даними тільки з самою моделлю.

Варіанти реалізації основних функцій наведені у морфологічній карті системи (Рисунок 7.1). На основі цієї карти побудовано позитивно-негативну матрицю варіантів основних функцій (таблиця 7.1)

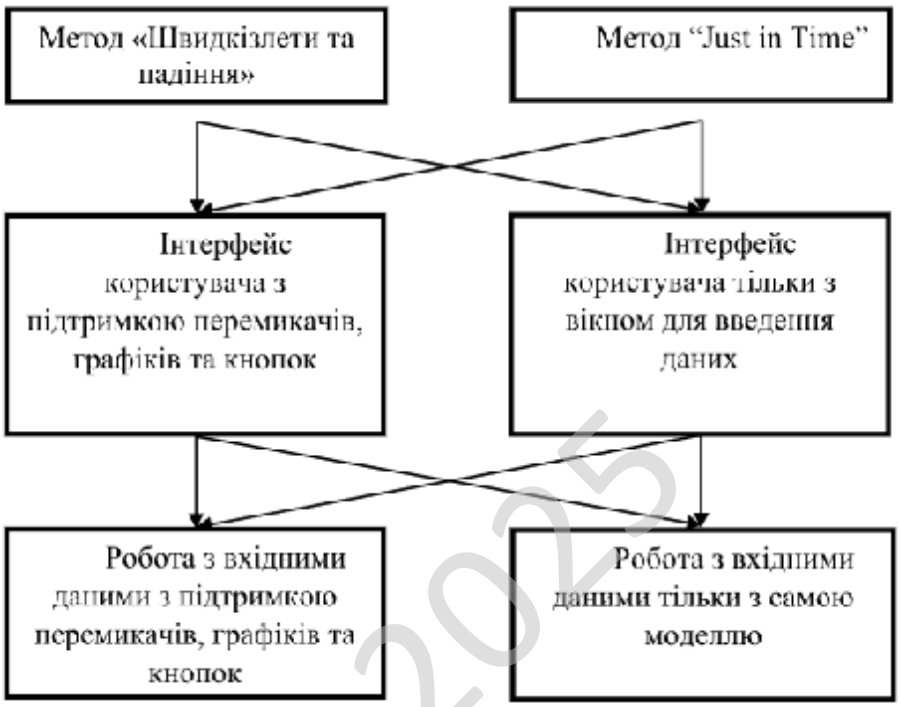

Рисунок 7.1 - Морфологічна карта

Морфологічна карта відображує всі можливі комбінації варіантів реалізації функцій, які складають повну множину варіантів ПП.

Таблиця 7.1 - Позитивно-негативна матриця

Основні функції	Варіанти реалізації	Переваги	Недоліки
F1	*А*	Більш надійний та стабільний метод	Більше витрат на ресурси
	Б	Використовує менше ресурсів компанії	Більша кількість ризиків
F2	*А*	Наглядність	Повторюваність дій
	Б	Швидкий процес	Знання мови програмування
F3	*А*	Простота використання	Важкість створення та передбачення можливих випадків
	Б	Швидкодія	Складність вивчення

Функція *F1:*

Оскільки розрахунки проводяться з великими об’ємами вхідних даних, то точність роботи повинна бути максимальною, тому варіант б) має бути відкинутий.

Функція *F2:*

Обробка даних займає важливе місце при використанні ПП і тому варіант б) має бути відкинутий.

Функція *F3:*

Інтерфейс користувача відіграє важливу роль у даному програмному продукту, тому варіант б) має бути відкинутий.

Таким чином, будемо розглядати такі варіанти використання ПП:

F1а – F2а – F3а

F1а – F2а – F3б

Для оцінювання якості розглянутих функцій обрана система параметрів, описана нижче.

7.3 Обґрунтування системи параметрів

Для того, щоб охарактеризувати програмний продукт, будемо використовувати наступні параметри:

X1 – швидкодія моделі. Пов’язаний з F2;

X2 – кількість необхідних параметрів на введення. Пов’язаний пропорційно з F3;

X3 – час обробки даних. Пов’язаний з F1;

X4 – потенційний об’єм моделі.Пов’язаний з F1 .

X1: Відображає швидкодію операцій залежно від обраного методу.

*X2:*Відображає значення яких змінних потрібно знати перед початком роботи.

*X3:*Відображає час, який витрачається на дії.

*X4:*Показує розмір програми.

Гірші, середні і кращі значення параметрів вибираються на основі вимог замовника й умов, що характеризують експлуатацію ПП як показано у Таблиця 4.2.

Таблиця 7.2 - Основні параметри ПП

Назва Параметра	Умовні позначення	Одиниці виміру	Значення параметра		
			гірші	середні	кращі
Швидкодія моделі	X1	Оп/мс	19	11	2
Кількість необхідних змінних	X2	Шт.	27	19	13
Час обробки даних	X3	мс	800	420	60
Потенційний об’єм моделі	X4	Блоків	50	300	900

За даними таблиці 2 будуються характеристики параметрів – Рисунок 7.2 – Рисунок 7.5.

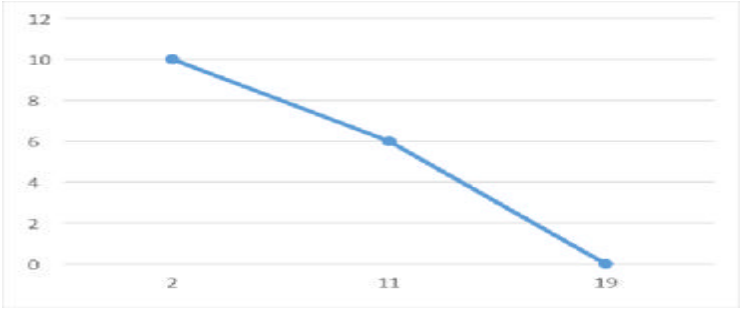

Рисунок 7.2 - X1, швидкодія моделі

Рисунок 7.3 - X2, кількість необхідних змінних

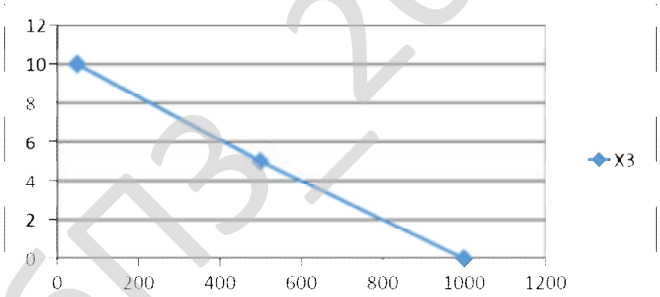

Рисунок 7.4. - X3, час обробки даних

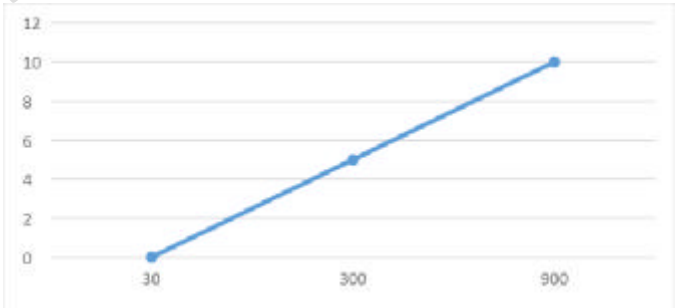

Рисунок 7.5 - X4, потенційний об’єм моделі

Визначення коефіцієнтів значимості передбачає:

– визначення рівня значимості шляхом присвоєння різних рангів;

– перевірку придатності експертних оцінок для використання;

– визначення оцінки попарного пріоритету параметрів;

– обробку результатів та визначення коефіцієнту значимості.

Результати експертного ранжування наведені у таблиці 7.3.

Таблиця 7.3 - Результати ранжування параметрів

Позначення параметра	Назва параметра	Одиниці виміру	Ранг параметра за оцінкою експерта							Сума рангів R_i	Відхилення Δ_i	Δ_i^2
			1	2	3	4	5	6	7			
X1	Швидкодія моделі	Оп/мс	3	3	4	4	3	3	3	23	5,5	30,25
X2	Кількість необхідних змінних	Шт.	4	4	3	3	4	4	4	26	8,5	72,25
X3	Час обробки даних	мс	2	1	2	1	2	2	2	12	-5,5	30,25
X4	Потенційний об’єм моделі	Блоків	1	2	1	2	1	1	1	9	-8,5	72,25
	Разом		10	10	10	10	10	10	10	70	0	205

Порахуємо коефіцієнт узгодженості:

$$W = \frac{12S}{N^2(n^3 - n)} = \frac{12 \cdot 205}{7^2(4^3 - 4)} = 0{,}84 > W_k = 0{,}67$$

За найбільший ранг приймемо 4, за найменший – 1.

Скориставшись результатами ранжирування, проведемо попарне порівняння всіх параметрів і результати заносимо у таблицю 7.4.

Таблиця 7.4 - Попарне порівняння параметрів

Параметри	Експерти							Кінцева оцінка	Числове значення
	1	2	3	4	5	6	7		
X1 і X2	<	<	>	>	<	<	<	<	0.5
X1 і X3	>	>	>	>	>	>	>	>	1.5
X1 і X4	>	>	>	>	>	>	>	>	1.5

Продовження таблиці 7.4									
X2 і X3	>	>	>	>	>	>	>	>	1.5
X2 і X4	>	>	>	>	>	>	>	>	1.5
X3 і X4	>	<	>	<	>	>	>	>	1.5

$$a_{ij} = \{1.5 \text{ при } X_i > X_j \; 0.5 \text{ при } X_i < X_j \; .$$

Для кожного параметра зробимо розрахунок вагомості $K_{вi}$.

Таблиця 7.5 - Розрахунок вагомості параметрів

Параметри x_i	Параметри x_j				Перша ітер.		Друга ітер.		Третя ітер	
	X1	X2	X3	X4	b	K	b	K	b	K
X1	1,0	0,5	1,5	1,5	4.5	0,281	16,25	0,275	59,125	0,274
X2	1,5	1,0	1,5	1,5	5,5	0,344	21,25	0,360	77,875	0,361
X3	0,5	0,5	1,0	1.5	3.5	0,219	12,25	0,208	44,875	0,207
X4	0,5	0,5	0,5	1,0	2.5	0,156	9,25	0,157	34,125	0,158
Всього:					16	1	59	1	2165	1

Таблиця 7.6 - Розрахунок показників рівня якості основних функцій ПП

Основні функції	Варіант реалізації функції	Абсолютне значення параметра	Бальна оцінка параметра	Коефіцієнт вагомості параметра	Коефіцієнт рівня якості
F1(X1)	А	11	5	0,264	1,32
F2(X2)	А	19	5	0,21	1,1
F3(X3,X4)	А	450 80	5 1,3	0,264	1,32 0,342
	Б	350 120	6,5 2	0,264	1,716 0,528

За даними з таблиці 6 визначаємо рівень якості кожного з варіантів:

$$K_{K1} = 2,32 + 1,32 + 0,342 = 4,08$$

$$K_{K2} = 2,32 + 1,716 + 0,528 = 4,565$$

Як видно з розрахунків, кращим є 2 варіант, для якого коефіцієнт технічного рівня має найбільше значення.

7.4 Економічний аналіз вартості розробки ПЗ

Для визначення вартості використання ПП спочатку проведемо розрахунок трудомісткості.

Всі варіанти включають в себе два окремих завдання:

1. Встановлення програмного продукту;

2. Використання програмного продукту;

Варіант 1 містить ще одне завдання: 3. Навчання аналітика за допомогою вбудованих методів.

Варіант 2: 4. Використання аудіо-додатків до моделей.

Завдання 1 за ступенем новизни відноситься до групи А, завдання 2 – до групи Б. За складністю алгоритми, які використовуються в завданні 1 належать до групи 1; а в завданні 2 – до групи 3.

Для реалізації завдання 1 використовується довідкова інформація, а завдання 2 використовує інформацію у вигляді даних.

Для першого та четвертого завдання, виходячи із норм часу для завдань розрахункового характеру степеню новизни А та групи складності алгоритму 1, трудомісткість дорівнює: T_P =90 людино-днів. $K_П$ = 1,5. $K_{СК}$ = 1. $K_{СТ}$ = 0,8. Тоді, за формулою 5.1, загальна трудомісткість програмування першого завдання дорівнює:

$$T_1 = 90 \cdot 1{,}5 \cdot 0{,}8 = 108 \text{ людино-днів.}$$

Для другого та третього завдання (використовується алгоритм третьої групи складності, степінь новизни Б), тобто T_P =30 людино-днів, $K_П$ =0,7, $K_{СК}$ = 1, $K_{СТ}$ =0,8:

$$T_2 = 30 \cdot 0{,}7 \cdot 0{,}8 = 16{,}8 \text{ людино-днів.}$$

Складаємо трудомісткість відповідних завдань для кожного з обраних варіантів реалізації програми, щоб отримати їх трудомісткість:

$T_I = (108 + 16,8 + 16,8) \cdot 8 = 1132,8$ людино-годин;

$T_{II} = (108 + 16,8 + 108) \cdot 8 = 1862,4$ людино-годин;

Найбільш високу трудомісткість має варіант II.

В розробці беруть участь два аналітика з окладом 19000 грн., один програміст з окладом 14000 грн. Визначимо зарплату за годину за формулою:

$$\text{СЧ} = \frac{9500 + 9500 + 7000}{3 \cdot 21 \cdot 8} = 51,5 \text{ грн.}$$

Зарплата розробників за варіантами становить:

I. $C_{ЗП} = 51,5 \cdot 1171,2 \cdot 1,2 = 72380,16$ грн.

II. $C_{ЗП} = 51,5 \cdot 1188,08 \cdot 1,2 = 73423,344$ грн.

Відрахування на єдиний соціальний внесок становить 22%:

I. $C_{ВІД} = C_{ЗП} \cdot 0,22 = 72380,16*0,22 = 15923,63$ грн.

II. $C_{ВІД} = C_{ЗП} \cdot 0,22 = 73423,344 *0,22 = 16153,13$ грн.

Так як одна ЕОМ обслуговує одного аналітика з окладом 9500 грн., з коефіцієнтом зайнятості 0,41 то для однієї машини отримаємо:

$$C_Г = 12 \cdot М \cdot K_З = 12 \cdot 9500 \cdot 0,41 = 46740 \text{ грн.}$$

З урахуванням додаткової заробітної плати:

$$C_{ЗП} = C_Г \cdot (1 + K_З) = 46740 \cdot (1 + 0,41) = 65903,4 \text{ грн.}$$

Відрахування на єдиний соціальний внесок:

$$C_{ВІД} = C_{ЗП} \cdot 0,22 = 65903,4 * 0,22 = 14498,74 \text{ грн.}$$

Амортизаційні відрахування розраховуємо при амортизації 25% та вартості ЕОМ – 22000 грн.

$$C_А = K_{ТМ} \cdot K_А \cdot Ц_{ПР} = 1,15 \cdot 0,25 \cdot 22000 = 6325 \text{ грн.},$$

Витрати на ремонт та профілактику розраховуємо як:

$$C_Р = K_{ТМ} \cdot Ц_{ПР} \cdot K_Р = 1,15 \cdot 22000 \cdot 0,05 = 1265 \text{ грн.},$$

Ефективний годинний фонд часу ПК за рік розраховуємо за формулою:

$T_{ЕФ} = (Д_К – Д_В – Д_С – Д_Р) \cdot t_З \cdot K_В = (365 – 104 – 8 – 16) \cdot 8 \cdot 0,9 = 1706,4$ годин.

Витрати на оплату електроенергії розраховуємо за формулою:

$C_{ЕЛ} = T_{ЕФ} \cdot N_C \cdot K_З \cdot Ц_{ЕН} = 1132 \cdot 0,156 \cdot 0,61 \cdot 1,53 = 164,81$ грн.,

Накладні витрати розраховуємо за формулою:

$$C_Н = Ц_{ПР} \cdot 0,67 = 22000 \cdot 0,67 = 14740 \text{ грн.}$$

Тоді, річні експлуатаційні витрати будуть:

$C_{ЕКС} = 65903,4 + 14498,74 + 6325 + 1706,4 + 371,81 + 14740 = 103545,35$ грн.

Собівартість однієї машино-години ЕОМ дорівнюватиме:

$$C_{М\text{-}Г} = C_{ЕКС} / T_{ЕФ} = 103545,35 / 1706,4 = 60,68 \text{ грн/час.}$$

Витрати на оплату машинного часу, в залежності від обраного варіанта реалізації, складає:

I. $C_М = 60,68 * 1171,2 = 71068,416$ грн.;

II. $C_М = 60,68 * 1188,08 = 72092,694$ грн.;

Накладні витрати складають 67% від заробітної плати:

I. $C_Н = 71068,416 * 0,67 = 47615,83$ грн.;

II. $C_Н = 72092,694 * 0,67 = 48302,105$ грн.;

Отже, вартість розробки ПП за варіантами становить:

I. $C_{ПП} = 72380,16 + 15923,63 + 71068,416 + 47615,83 = 206988,036$ грн.;

II. $C_{ПП} = 73423,344 + 16153,13 + 72092,694 + 48302,105 = 209971,273$ грн.;

Отже розрахунки вартості розробки показують, що оціночна вартість розробки ПЗ буде на рівні 210000 грн.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Комп’ютер – невід’ємна складова сучасного життя. За допомогою обчислювальної техніки вирішують складні робочі задачі, ведуться наукові дослідження, створюються архітектурні креслення і твори мистецтва. Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп’ютерної техніки. Незважаючи на видиму безпеку та розвитку сучасних технологій, при роботі за комп'ютером є ряд чинників, які можу вплинути на здоров'я людини. Через масовий характер робіт, що виконуються працівниками за допомогою комп’ютера, законодавством України чітко врегульовано норми та вимоги до використання комп’ютерної техніки на підприємстві, безпосередньо й охорона праці на підприємстві при роботі за комп’ютером.

Законом України “Про охорону праці” [1] регламентуються загальні положення державної політики в галузі охорони праці, а реалізуються ці положення, зокрема, Вимогами щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями, затверджені наказом Мінсоцполітики від 14.02.2018р. № 207, зареєстровані в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 [2].

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ.

У розділі даної магістерської роботи висвітлюються основні питання охорони праці працівників, робота яких пов’язана з роботою за комп’ютером, планування робочого приміщення, де працюють користувачі ПК; параметри мікроклімату, освітленість робочих місць та виробничих приміщень; шумові завади.

Правильна організація і раціональне устаткування робочого місця можливість ефективно і з як найменшими витратами праці виконувати свої функції, плідно спілкуватися співробітниками і підлеглими, підтримувати високу працездатність і робочий настрій. Велике значення має раціональна конструкція і розташовує елементів робочого місця, що важливе для підтримки оптимальної робочої пози людини-оператора, а також необхідно дотримувати правильний режим праці і відпочинку.

Що стосується питання охорони праці людини необхідно вирішувати на всіх стадіях трудового процесу незалежно від виду професійної діяльності.

Забезпечення безпечних і здорових умов праці в значній мірі залежить від правильної оцінки небезпечних, шкідливих виробничих факторів. Однакові по складності зміни в організмі людини можуть бути викликані різними причинами. Це можуть бути фактори виробничого середовища, надмірне фізичне і розумове навантаження, нервово-емоційна напруга, а також різне сполучення цих причин.

Робота працівників пов’язана з роботою за комп’ютером, тому актуальною є розгляд саме умов праці та стану охорони праці працівників які постійно працюють з комп’ютерною технікою.

Завдання даного розділу полягає у тому, щоб розробити якісний програмний продукт необхідно організувати безпеку на робочому місці програміста. Під час проектування безпеки робочому місці з ПК необхідно домагатися високої якості та надійності технічного забезпечення, але й створювати комфортні параметри довкілля для розробників.

8.2 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 8.1.

Таблиця 8.1 – Розміри приміщення

Найменування	Значення, м
Ширина	5,4
Довжина	6
Висота	2,75

Таблиця 8.2 – Площа та обсяг приміщення, на одного працюючого·

Геометрична характеристика	Одиниця виміру	Нормативне значення *	Фактичне значення
Площа, S	$м^2$	не менше 6.0	8,1
Обсяг, V	$м^3$	не менше 20.0	24,3

* Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин) [2].

У зазначеному приміщенні працюють 4 людей. За даними, які наведено у табл. 8.1, та табл. 8.2, можна зробити висновок, що площа та об’єм приміщення у розрахунку на одно робоче місце програміста не відповідають нормативним вимогам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [2], але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5] та НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин»). Таним чином можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

Температура повітря в приміщенні визначається впливом температури зовнішнього повітря і тепловою енергією, яка виділяється всередині приміщення. Джерелами виділення теплоти в даному приміщенні є електроустаткування, освітлювальні прилади, а також люди. У світлий час доби джерелом надлишкового тепла є сонячна радіація. Згідно Постанови № 42 від 01.12.1999 Головного державного санітарного лікаря України, робота, виконувана в даному приміщенні, відноситься до категорії Іа. В цьому випадку людина витрачає енергії до 120 ккал у годину. Вологість повітря в приміщенні визначається впливом багатьох факторів, серед яких: вологість атмосферного повітря, виділення вологи людьми (при диханні та випарами з поверхні шкіри).

Мікроклімат повітряного середовища в приміщенні характеризується запиленістю та загазованістю повітря. Мікроклімат приміщення визначається діючим на організм людини поєднанням, вологості, температури, швидкості руху повітря та інтенсивності теплового випромінювання. Аналіз мікроклімату складається з визначення зазначених вище факторів і порівняння результатів із встановленими нормами.

У таблиці 8.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і розглянутого приміщення. У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Таблиця 8.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Вологість,%	Швидкість повітря, м/с	Температура,°С	Вологість%	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	22-23	40-55	0,1
Тепла	23-25	50-70	0,1	24-25	50-65	0,11

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року. В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

У приміщенні знаходяться наступні джерела шуму: принтер HP 1100, електродвигуни вентиляторів ЕОМ.

Одним з найважливіших факторів, які впливають на ефективність трудової діяльності людини, та попереджають травматизм і професійні захворювання програмістів є освітлення на робочому місці.

З 2019 року діють Державні будівельні норми україни “Природне і штучне освітлення” – ДБН В.2.5-28:2018 [1], у яких прописані вимоги до використання всіх освітлювальних приладів, у т.ч. світлодіодних.

Працю працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [1], можна віднести до роботи з малою точністю (найменший розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В).

Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [1],

Крім того все поле зору повинне бути освітлено достатньо рівномірно – ця основна гігієнічна вимога. Так як яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

8.3 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог. Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов'язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

Для підвищення ефективності системи управління охорони праці дуже важлива роль належить формуванню і розвитку інформаційної культури фахівців IT-технологій

8.4 Розрахункова частина

Для захисного штучного заземлення застосовуються вертикальні електроди: металевий куток 45х45х5 мм, довжиною L=2.5 м, та горизонтальний електрод – металева полоса з перетином 40х4 мм. Напруга – 220/380 В. Розрахункова схема розташування заземлюючих електродів – у ряд (рис. 8.1).

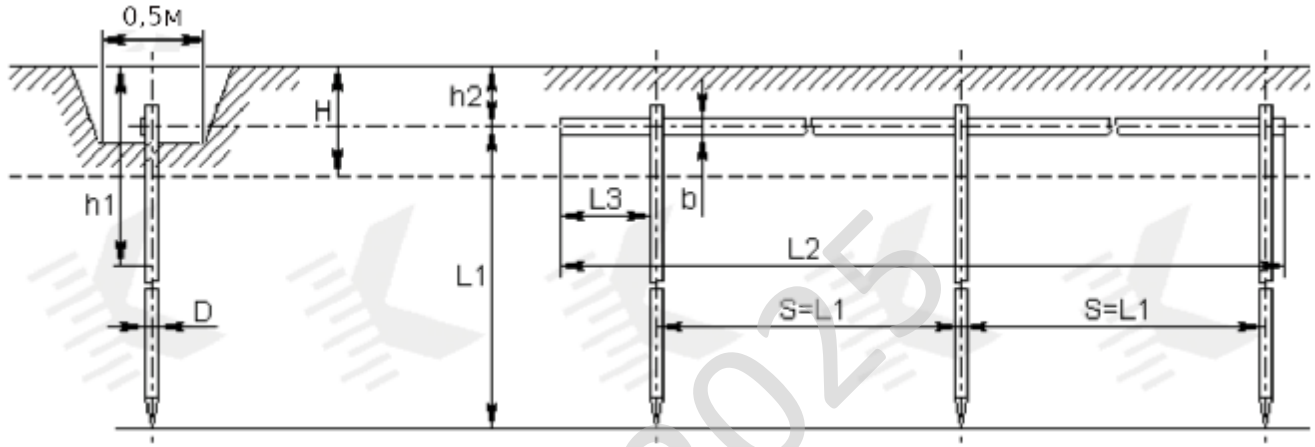

Рисунок 8.1 – Схема штучного заземлення.

Розрахунок проводиться за допустимим опором розтіканню струму заземлювача.

Початкові дані для розрахунку захисного заземлення:

– тип верхнього шару грунта – чорнозем, нижнього шару грунта – глина (питомий опір ρ_2 = 40 Ом·м);

– умовна товщина верхнього шару грунта: H=0.5 м;

– відстань між вертикальними заземлювачами (електродами) A=3 м;

– глибина закладення горизонтального контура заземлення t=0.8 м;

– опір заземлювача, який нормується: $R_{ЗН}$ = 4 Ом.

Необхідно визначити необхідну кількість вертикальних заземлювачів та довжину полоси (горизонтального заземлювача).

Виконаємо розрахунок захисного заземлення.

Відстань від центра вертикального заземлювача до поверхні землі:

$$T=t+L/2=0,8+2.5/2=2.05 \text{ м.}$$

Розрахунковий питомий опір грунта (з врахуванням того, що фактично вся конструкція заземлювача розташовується у нижньому шарі грунту):

$$\rho = \psi \cdot \rho_2 = 1.36 \cdot 40 = 54.4 \text{ Ом·м.}$$

де $\psi = 1.36$ – табличне значення коефіцієнта сезонності для відповідної климатичной зони у багатошаровому грунті [6];

$\rho = 40$ Ом·м. – табличне значення питомого опору нижнього шару грунту (глина) [11].

Еквівалентний діаметр вертикального електрода (кутка) [11]:

$$D_в=0.95 \cdot К= 0.95 \cdot 45 = 0.043 \text{ м.}$$

де К= 45 мм – розмір металевого кутка (заданий).

Відношення A/L=3/2.5=1.2.

Опір розтіканню електричного струму одного електрода вертикального заземлювача з урахуванням заглиблення заземлювача [11]:

$$R_О=0.366 \cdot (\rho/L) \cdot [\lg(2L/D_в)+(1/2)\lg((4 \cdot T+L)/(4 \cdot T-L))] =$$

$$=0.366 \cdot (54.5/2.5) \cdot [(\lg(2 \cdot 2.5/0.0475)+(1/2) \cdot \lg((4 \cdot 2.3+2.5)/(4 \cdot 2.3-2.5))]=17.55 \text{ Ом.}$$

Визначаємо коефіцієнт екранування вертикальних електродів Кев=0.8 при орієнтовній кількості вертикальних електродів, яке дорівнює 4 [11].

Визначаємо необхідну кількість вертикальних заземлювачів (без врахування горизонтального заземлювача), при $R_{ЗН} = 4$ Ом

$$N=R_О /(Кев \cdot R_{ЗН})= 17.55 / (0.8 \cdot 4)=5.48 \approx 6 \text{ шт.}$$

Визначаємо довжину з'єднуючої полоси:

$$L_П =1.05 \cdot A \cdot N = 1.05 \cdot 2.5 \cdot 5.48 = 17.28 \approx 18 \text{ м.}$$

Опір розтіканню електричного струму з'єднуючої полоси з урахуванням кліматичного коефіцієнта питомого опору грунту $K_П$ [11]:

$$R_П = 0.366 \cdot (\rho_2 \cdot K_П/L_П) \cdot \lg(2(L_П \cdot L_П)/(B \cdot t)) =$$

$$=0.366\cdot(40\cdot5/17.28)\cdot\lg((2\cdot17.28^2)/(0.04\cdot0.8))=18 \text{ Ом}.$$

де $K_П = 5$ – табличне значення кліматичного коефіцієнта питомого опору грунта для відповідної кліматичної зони для з'єднуючої полоси [11]:

B = 40 мм. = 0.04 м.- ширина з'єднуючої полоси (задана).

Загальний опір розтіканню електричного струму заземлювача [11]:

$$R = (R_О\cdot R_П)/(R_О\cdot\eta_П + N\cdot R_П\cdot Кев)=$$

$$=(17.55\cdot18)/(17.55\cdot0.75+ 5.48\cdot18\cdot0.8) = 3.43 \text{ Ом}.$$

де $\eta_П = 0.75$ – табличне значення коефіцієнта екранування з'єднуючої полоси [11].

Умова $R \le R_{ЗН}$ виконується, $3.43 \le 4$.

При необхідності можна зменшити кількість електродів заземлювача зменшивши загальний опір розтіканню електричного струму заземлювача методом зменшення питомого опору ґрунта, домішуючи у грунт безпосередньо навколи електродів заземлювача розчини солей NaCl, CaCl, сажу, соду, шлак, коксову дрібницю, або спеціальні суміші.

8.5 Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз приміщення, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок захисного штучного заземлення, як одного з ключових факторів безпеки програміста. Розроблено заходи з охорони праці.

9 ОСНОВНІ ВИСНОВКИ

Темою магістерської роботи стало дослідження щодо оцінки швидкості поширення інформації за умови використання різних стратегій поширення та стійкості мереж до інформаційних впливів.

У процесі виконання дипломної роботи отримано такі результати:

1. Проаналізовано методи та моделі поширення інформаційних впливів у соціальних мережах, аналіз дозволив виявити як комбіновані комплексні моделі, які мають підвищити адекватність та відповідність програмного моделювання реальним процесам, так і моделі, орієнтовані на дослідження конкретних характеристик. Аналіз показав, що переважна більшість моделей та методів не враховують індивідуальні характеристики вузла та поведінку суб'єктів при поширенні інформації, стратегію поширення інформації, яку вибирає вузол у процесі інформаційних впливів.

2. У роботі запропоновано математичну модель поширення інформаційних впливів у сегменті соц. мережі, яка дає можливість застосування різних поведінкових стратегій суб'єктами ІВ на основі аналізу особистісних характеристик вузлів для атаки.

3. У роботі запропоновано підхід до генерації структури сегмента мережі, заснований на комбінації обраних кластерів (групи, лідерські групи, кліки). Підхід дозволяє моделювати структуру мережі з зумовленою структурою та щільністю зв'язків.

4. Проведене експериментальне дослідження програмної моделі, яке дозволило отримати деякі оцінки запропонованих стратегій поширення інформації та порівняти результати їх застосування за різних початкових умов.

В четвертому розділі магістерської роботи запропоновано різні стратегії поведінки генераторів – суб'єктів інформаційного впливу.

Проведено експерименти для порівняння ефективності застосування різних базових стратегій поведінки суб'єктами впливу у соціальних мережах при поширенні інформаційних впливів.

Експерименти доводять адекватність запропонованої моделі. Модель прогнозовано реагує зміну параметрів. Результати, отримані в ході експериментів, про критичну кількість залучених вузлів для стрімкого зростання кількості шанувальників у мережі збігаються з результатами інших дослідників.

Експерименти порівняння результатів швидкості поширення інформації в сегменті за різних початкових умов (щільність зв'язків, кількість вузлів у мережі з високим рівнем інформаційного опору, початкове розміщення генератора) дозволяють зробити такі висновки:

- стратегії «Дерево» показують найкращий рівень стабільності незалежно від вихідного положення генератора.

- стратегія «Кущ» найбільш нестабільна, але показує досить високі результати за сприятливих умов (висока щільність зв'язків у зоні генератора, низький рівень інформаційного опору).

В п’ятому розділі представлено ряд експериментів на реалізованій програмній моделі, результати експериментів візуалізовані за допомогою графіків та діаграм, кожен окремий результат проаналізовано.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Проведено маркетингове та економічне обґрунтування ІТ-проєкту, що дозволило визначити ключові фактори успіху даного проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вебер К.С. Порівняльний аналіз соціальних мереж/К.С. Вебер, А.А. Піменова // Вісник університету. Серія: природничі та технічні науки. - 2022. - № 2 (19). - С. 634 - 636.

2. Пелещішин А.М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / О. М. Пелещишин, Ю.О. Сєров, О.Л. Березко, О.П. Пелещішин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А.М. Пелещишина. – Львів: Видавництво Львівської політехніки, 2012. – 368 с.

3. Сєров Ю.О. Аналіз комунікативних процесів у Веб-спільнотах середовища Веб 2.0 / Ю.О. Сєров, А.М. Пелещішин, К.О. Слобода // Східно-Європейський журнал передових технологій. - 2009. - № 1/2 (37). - С. 38 - 41.

4. Адаськов О.І. Рекомендації щодо проведення інформаційних заходів у мережі Інтернет на користь виконання завдань інформаційно-психологічних операцій / О.І. Адаськов // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - 2014. - Віп. 45. - С. 57 - 67.

5. Муратова Н.Ф. Інтернет-ЗМІ як окремий вид у системі засобів: лексичне та етимологічне позначення поняття // Філологічні науки. Питання теорії та практики, - № 2 (6). - С. 118-120.

6. Панченко Є. Інтеграція Інтернет-ЗМІ та соціальних мереж у Рунеті: Нова публічна сфера чи простір контролю? / Є. Панченко // Digital Icons: Studies in Russian, Eurasian and Central European New Media - 2011. - № 5. - С. 87 - 118.

7. Смирнов А.І. Глобальна безпека в цифрову епоху/ А.І. Смирнов, В.Р. Григор'єв, 2014. - 394 с.

8. Пірцхалава Л.Г., Хорошко В.А., Хохлачова Ю.Є. Шелекст М.Є. Інформаційне протиборство у сучасних умовах: [Монографія] / За редакцією професора В.А. Добре. - К.: ЦП "Компрінт", 2019. - 226 с.

9. Мелешко Є.В., Константинова Л.В., Улічов О.С. Дослідження властивостей інформації та методів її поширення з точки зору інформаційної безпеки у соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 3 (35). - Полтава: ПНТУ ім. Ю. Кондратюка. - 2015. - С. 98-106.

10. Улічев О.С. Дослідження моделей розповсюдження інформації та інформаційних впливів у соціальних мережах // Збірник наукових праць "Системи управління, навігації та зв'язку". Випуск 4 (50). - Полтава: ПНТУ ім. Ю. Кондратюка. - 2018. - С. 147-151.

11. Улічев О.С. Математична модель поширення інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеві машинобудування, автоматизація. – Кропивницький: ЦНТУ, 2018. – Віп. 31. – С. 165-174.

12. Улічев О.С., Мелешко Є.В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах // Збірник наукових праць "Сучасні інформаційні системи". Випуск 2(2). - Харків: ХПІ. - 2018. - С. 35-39.

13. Ulichev O., Meleshko Ye., Sawicki D., Smailova S. Комп'ютер modeling disemination of informational influences in social networks with different strategies of information distributors // Proc. SPIE 11176, Wilga, Poland (ISSN: 0277-786X). - 2019. - Number article: 111761T. (SCOPUS).

14. Ulichev O., Meleshko Y., Khokh V. Комп'ютерна методика методу соціальної мережі структури для дослідження дисемінації процесів інформаційних influences // Scientific and Practical Cyber Security Journal (SPCSJ) 4(3). - Georgia, Tbilisi, 2019. - P. 34-47.

15. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження робастності рекомендаційних систем із колаборативною фільтрацією до інформаційних атак // Наукове видання Кібербезпека: освіта, наука, техніка.– Київ: КУБГ, 2019. Т.1 № 5. – С. 95-104.

16. Мелешко Є.В., Хох В.Д., Улічов О.С. Дослідження відомих моделей атак на рекомендаційні системи з колаборативною фільтрацією // Збірник наукових праць Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – №. 5 (57). - С. 67-71.

17. Ulichev O., Meleshko Y., Smirnov O., Khokh V. Метод методу вибору предметів для інформаційного впливу в соціальних мережах під час інформації campaign заснований на аналітичній hierarchy process // 1st International workshop on cyber hygiene & conflict management Kyiv, Ukraine, 2019 (SCOPUS). [прийнято до публікації]

18. Улічев О.С. Генерування моделі соціальної мережі для дослідження впливу її структури на розповсюдження інформаційних впливів // Збірник тез II Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 20-22 квітня 2017 р. - Кропивницький: ЦНТУ. - 2017. - С. 103-104.

19. Улічев О.С., Мелешко Є.В. Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». м. Кропивницький. 19-20 квітня 2018р. - Кропивницький: ЦНТУ. - 2018. - С. 136-220.

20. Улічев О.С., Мелешко Є.В. Математична модель розповсюдження інформації у сегменті соціальної мережі // Матеріали Двадцятого Міжнародного науково-практичного семинару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 року. – Кропивницький: КЛА НАУ. - 2018. - С. 68-72.

21. Улічев О.С., Мелешко Є.В. Програмна модель розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез VIII Міжнародної науково-технічної конференції «ITSEC», м. Київ, 16-18 травня 2018 року. - Київ: НАУ. - 2018. - С. 34-35.

22. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез Сьомої міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 17-19 травня 2018 р. - Львів: Національний університет "Львівська політехніка". - 2018. - С. 29-30.

23. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез X Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем(SITS'2018)»,21-23 червня 2018 року. – Миколаїв-Коблево: НАУ та МІПРО. – 2018. – С. 77–79.

24. Мелешко Є.В., Шингалов Д.В., Улічев О.С. Дослідження Баєсових мереж довіри як засобів для моделювання динамічних процесів у складних мережах // Збірник тез XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», 20-22 листопада 2019 року. - Дніпро: ДНУ. - 2019. - С. 284-285.

25. Мелешко Є.В., Хох В.Д., Улічов О.С. Методи тестування робастності рекомендаційних систем із колаборативною фільтрацією // Всеукраїнська науково-практична Інтернет-конференція «Перспективні напрямки інформаційних та комп'ютерних систем та мереж, комп'ютерно-інтегровані технології в промисловості, телекомунікаціях, енергетиці та транспорті» 13-14 листопада 2019 р. - м. Кропивницький: ЦНТУ. - 2019. С. 88-89.

26. Мелешко Є.В., Хох В.Д., Улічов О.С. Дослідження методів підвищення робастності рекомендаційних систем до інформаційних атак // Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення

кібербезпеки та захисту інформації», 19 – 22 лютого 2020 р. – м. Київ: Вид-во Європейського університету, 2020. – С. 65-70

27. List of virtual communities with more than 100 million active users [Electronic resourse]. – Mode of access: http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users. – Title from the screen.

28. Verizon 2022 Data Breach Investigations Report [Електронний ресурс]// URL: https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/ (дата звернення: 25.10.2025)

29. Орлов А.Ю. Організація віртуального співтовариства у мережі Інтернет/А.Ю. Орлов / / Інформаційні технології. - 2008. - № 8. - С. 15 - 19.

30. Пелещішин А.М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / О.М. Пелещішин, Ю.О. Сєров, О.Л. Березко, О.П. Пелещішин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А. М. Пелещішина. – Львів: Видавництво Львівської політехніки, 2012. – 368 с.

31. Почепцов Р. Контроль за розумом / Р. Почепцов. – К: ВД Київсько-Могилянська академія, 2012. – 350 с.

32. Рідель В.В. Комп'ютерне моделювання // Методичні вказівки навчальної дисципліни, Одеса, 2017

33. Закон України "Про інформацію" від 2 жовтня 1992 р.: із змінами, внесеними Законом України від 2 грудня 2010 р. : за станом на 1 березня 2015 р. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12/ed20110113. - Назва з екрану.

34. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. із змінами, внесеними Законом України від 21 лютого 2014 р. : за станом на 1 березня 2015 р. / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр. - Назва з екрану.

35. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

36. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.

37. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.

38. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

39. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

40. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.

41. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

42. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of*

Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

43. Губанов Д.А., Калашніков А.О., Новіков Д.А. Теоретико-ігрові моделі інформаційного протистояння в соціальних мережах // Управління великими системами. Випуск 31

44. Губанов Д.А., Новіков Д.А., Чхартішвілі А.Г. Моделі репутації та інформаційного управління у соціальних мережах // Математична теорія ігор та її застосування. 2019. Том 1. Випуск 2. С. 14-37.

45. Seidman S.B., & Foster B.L. (1978). A граф-теоретична загальнеізація клікового концепції. Journal of Mathematical Sociology, 6, - С. 139-154.

46. Moody J., White D.R. (2003). Структуральна cohesion and embeddedness. American Sociological Review, 68 (1), - С. 103-128.

47. Wellman B., Hogan B., Berg K. та ін. (2006). Connected lives: The project. У П. Purcell (Ed.), The networked neighborhood (P. 161-216).

48. Батура Т.В. Моделі та методи аналізу комп'ютерних соціальних мереж//Програмні продукти та системи 2013. № 3 С. 130-137.

49. Kermack W.O., McKendrick A.G. A Contribution to the Mathematical Theory of Epidemics // Proc. з Royal Society A: Mathematical, Physical and Engineering Sciences. 1927. No. 115 (772). 700 p. DOI:10.1098/rspa.1927.0118. JSTOR 94815.

50. Горковенко Д.К. Порівняльний аналіз моделей епідемії та клітинного автомата при моделюванні поширення інформації в соціальних мережах // Науково-технічні відомості. Інформатики. Телекомунікації. Управління. 2017. Т. 10. № 3. С. 103-113. DOI: 10.18721/JCSTCS.10309

51. Kempe D., Kleinberg J., Tardos E. Maximizing Spread of Influence через Social Network / Proceedings of 9-th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2003. – p. 137-146.

52. Erdös P., Rényi A. На ході розвитку графів // Magyar Tudományos Akademia Matematikai Kutato Intezetenek Közlemenyei [Publications of Mathematical Institute of Hungarian Academy of Sciences]. - 1960. - T. 5.

53. Watts DJ; Строгатц, С. Н. (1998). «Collective dynamics of “small-world” networks» (PDF). Nature. 393 (6684): 440-442. Bibcode:1998Natur.393..440W. doi:10.1038/30918. PMID 9623998

54. Barab´asi L.-A., Albert R., Jeong H. Scale-free characteristics of random networks: topology of the world-wide web. Physica, A281, 69-77, 2000

55. Bollobás B., Riordan O. Mathematical results on scale-free random graphs // Handbook of graphs and networks. Weinheim: Wiley-VCH, 2003. P. 1-34

56. Buckley P.G., Osthus D. Popularity засновані на random graph models leading to scale-free degree sequence. Discrete Mathematics, 282:53–63, 2004

57. Bollobás B., Borgs C., Chayes T., Riordan O.M. Directed scale-free graphs. ProceedingSODA '03 Proceedings of the fourteenth annual ACM-SIAM символізм на Discrete algorithms, P. 132–139, 2003

58. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

59. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

60. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

61. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»,* № 2 (307). С. 46-52. 2022.

62. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки.* №4. С. 103-110. 2020.

63. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.

64. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

65. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». *Центральноукраїнський науковий вісник. Технічні науки.* № 2(33). с. 161-172, 2019.

66. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

67. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дрєєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 184-194, 2019.

68. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87.

69. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

70. Смірнов О.А., Котелянець В.В. Стійкі до колізій стохастичні моделі функціонування безпроводових сенсорних мереж. Вісник інженерної академії України, №3, с. 145-152, 2018

71. Смірнов О.А., Смірнов С.А., Дідик А.К. Метод безпечної маршрутизації метаданих у хмарні антивірусні системи. Системи озброєння та військова техніка. – Випуск 2 (46) – Х.: ХУПС – 2016. – С. 146-149.

72. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.

73. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.