ЗМІСТ

ВСТУП 5

РОЗДІЛ 1. СУТНІСТЬ ПРІОРИТЕТНИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ 6
1.1 Узагальнені підходи щодо якості визначення пріоритетних алгоритмів у системі захисту інформації 6
1.2 Класифікаційно-категоріальний характер приорітетних алгоритмів у захисті інформації 10
1.3 Основні принципи оцінювання типових алгоритмів захисту інформації 18

РОЗДІЛ 2. СТРУКТУРНА ОРГАНІЗАЦІЯ ПРІОРИТЕТНИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ 22
2.1 Методи оцінювання кіберстійкості критичної інфраструктури у захисті інформації 22
2.2 Концепція кібервійськ, як програмний захист інформації 24
2.3 Мобільні особливості кібербезпеки щодо штучного інтелекту у повоєнній Україні: Виклики та стратегії 32

РОЗДІЛ 3. ПРИОРІТЕТНІ АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ У ВОЄННИХ ПРАКТИКАХ 40
3.1 Оборона повітряного простору як практичний алгоритм щодо захисту інформації 40
3.2 Основні прийоми дискретного матиматичного моделювання у захисті інформаці 54
3.3 Феноменальні способи математичного моделювання як росповсюдження квантових радіохвиль у Захисті мирного неба України 67
3.3.1 Мегастильники в математичному моделюванні 67
3.3.2 Макростильники в математичному моделюванні 71
3.3.3 Мікростільники в математичному моделюванні 78

3.3.4 Фемтостільники в математичному моделюванні
за умов воєнного часу.....82
3.4 Мобільні особливості кібербезпеки щодо
штучного інтелекту у повоєнній Україні:
виклики та стратегії 85
3.5 Воєнна криптосистема, як якісна практика управління
державною таємницею у захисті інформації 88

ВИСНОВКИ.....101

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....102

ВСТУП

За сучасних умов повномасштабної фази війни в Україні з російською агресією автором виникла нагальна потреба щодо написання означеної монографії. Дана монографія присвячена розгляду пріоритетних алгоритмів щодо воєнного захисту інформації. Адже такий воєнний захист відіграє **актуальну роль** у різноманітних контекстах забезпечення цілісності, конфіденційності та доступності даних.

Метою монографії є системний аналіз сутності, структури та механізму воєнного захисту інформації, що логічно обумовлює державно-стратегічний пріоритет комп'ютерної інженерії.

Так, у першому розділі проаналізовано загальні підходи до визначення якості пріоритетних алгоритмів у системі захисту інформації, а також здійснено класифікаційно-категоріальний характер алгоритмів, що сприяє їх ефективно-діючому розумінню та оптимізації вибору в конкретних ситуаціях. В другому розділі акцентовано на структурну організацію пріоритетних алгоритмів, зокрема на критичну інфраструктуру та мобільні пристрої.

У третьому розділі розглянуто застосування пріоритетних алгоритмів у воєнних практиках, зокрема в обороні повітряного простору та у використанні математичного моделювання для розробки ефективних стратегій захисту.

Таким чином монографія є важливим кроком у розумінні та вдосконаленні алгоритмів захисту інформації, що мають вирішальне значення у забезпеченні безпеки як у цивільній, так і військовій сферах.

Монографія складається з трьох розділів, перший та другий поділяється на три підрозділи, а третій на п`ять.

РОЗДІЛ 1.
СУТНІСТЬ ПРІОРИТЕТНИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Узагальнені підходи щодо якості визначення пріоритетних алгоритмів у системі захисту інформації

У цьому змісті визначемо такий важливий алгоритм у забезпеченні найдійності та ефективності, що до означеної тематики як стеганографія.

Адже Стеганографія – це вчення про приховане передавання інформації шляхом вбудовування секретних даних в інші незвичайні об'єкти або медіафайли, такі як: текстові документи, зображення, аудіофайли чи відеофайли. Це відрізняється від криптографії, яка займається захистом інформації через шифрування. При цьому основною метою стеганографії є таємне передавання інформації без підозрілості чи виявлення її наявності.

Основні причини використання стеганографії включають:

1. Забезпечення конфіденційності: Це дозволяє приховувати наявність повідомлень або даних в інших об'єктах, зменшуючи ризик їхнього виявлення та доступу незаконних користувачів.

2. Передавання конфіденційної інформації: Застосовується у випадках, коли важлива інформація повинна бути передана безпечно без привертання надмірної уваги.

3. Запобігання аналізу даних: Це може заважати спостереженню або аналізу даних, таким чином, ускладнюючи виявлення секретних повідомлень.

Щодо впливу на надійність та ефективність, стеганографія може мати наступні аспекти:

– Надійність: Спроектовані стеганографічні методи мають за мету забезпечити надійність прихованої інформації. Це означає, що така інформація повинна залишатися прихованою навіть при аналізі атаками на дані.

– Ефективність: Стеганографія стає ефективно діючою, коли приховані дані можна вбудувати в об'єкт дії без помітних змін в оригіналі. Адже, чим послаблено помітний ефект має процес вбудовування, тим ефективніше його функціювання.

За допомогою стеганографії можна забезпечити таємне комунікування та захист конфіденційності. Проте, важливо пам'ятати, що цей метод не є абсолютною гарантією безпеки, тому його ефективність може залежати від обраного алгоритму та аналізу, який може бути застосований до прихованих даних. [77, С. 134-138.]

Сучасні тенденції розвитку алгоритмів стеганографіі передбачають:

1. Посилення обчислювальної складності: Розвиток алгоритмів стеганографії містить у собі зростання обчислювальної складності для ускладнення виявлення прихованої інформації.

2. Використання машинного навчання: Машинне навчання стало корисним інструментом для покращення якості та надійності стеганографічних методів, зокрема для генерації більш стійких прихованих повідомлень та унікальних ключів.

3. Використання адаптивних методів: Алгоритми стеганографії стають більш адаптивними до різних умов і типів зображень або медіафайлів.

4. Застосування у сферах безпеки: Стеганографія широко використовується для захисту конфіденційної інформації, такої як: урядові документи або особисті дані, від несанкціонованого доступу.

5. Оцінка стійкості до атак: Дослідження та розробка методів для оцінювання стійкості стеганографічних систем до різних видів атак і аналізу стають актуальними завданнями, що полягає в наступному.

Автором зазначено, що розвиток технологій і методів стеганографії може змінюватися з часом, і для актуальної інформації варто постійно знаходити нові джерела та дослідження в цій галузі. Саме тому запропоновано розглянути сучасні алгоритми стеганографії на прикладах.

1. LSB (Least Significant Bit) стеганографія: Цей метод використовує найменш значущі біти (LSB) покриття (зображення або звук) для приховування бітів іншого файлу. Мінімальні зміни в оригінальному покритті допомагають підтримувати при-

хованість. Алгоритми, які використовують LSB стеганографію, можуть зашифровувати приховані дані для підвищення безпеки. [108, С. 56-63.]

2. Фреквенційна стеганографія: Цей метод використовує зміни в частотному спектрі аудіо- або зображень для приховування даних, що здатний використовувати методи, а саме: зміна амплітуди або частотної фази сигналу. Фреквенційна стеганографія може бути більш стійкою до розширення та компресії, порівняно з LSB методами.

3. Використання текстового формату: Сучасні алгоритми стеганографії можуть використовувати текстові документи, такі як HTML-сторінки або PDF-файли, для приховування інформації. Вони можуть використовувати різні методи, такі як зміна розмірів шрифту, розташування тексту або вставка невидимих символів для кодування даних.

4. Використання різноманітних носіїв: Сучасні алгоритми стеганографії можуть працювати з різними типами носіїв, включаючи зображення, аудіо, відео, текст і навіть мережевий трафік, які спроможні використовувати необхідні приховані комбінації цих носіїв для баз даних.

5. Використання криптографії: Деякі сучасні алгоритми стеганографії комбінують стеганографію з методами шифрування, що робить важчим виявлення інформації та забезпечує додатковий рівень безпеки.

6. Методи множинного приховування: Ці алгоритми використовують багато різних методів приховування для покращення стійкості та надійності стеганографії. Наприклад, один алгоритм може використовувати LSB стеганографію, фреквенційну стеганографію та текстовий формат одночасно. [46, С. 153-154]

Ці сучасні алгоритми стеганографії розвиваються, щоб залишатися кроком перед методами виявлення стеганографії. При цьому важливо пам’ятати, що використання стеганографії для незаконних цілей, таких як: шпигунство або кримінальна діяльність, може бути незаконним і порушувати приватність та безпеку. Виходячи із останнього важливо зазначити, що розвиток алгоритму стеганографії тягне за собою не тільки позитивні моменти у вигляді захисту інформації та збереження конфіденційної

інформації, але і погіршення ситуації із кібератаками на державні установи та інші установи.

Нещодавно ми спостерігали за використанням стеганографії у таких шкідливих програмах і засобах кібершпигунства: Microcin (також відомий як six little monkeys); NetTraveler; Zberp; Enfal (його новий завантажувач називається Zero.T); Shamoon; KinS; ZeusVM; Triton (Fibbit). [135 с. 233–236.]

Чому автори шкідливого програмного забезпечення все активніше використовують стеганографію у своїх розробках? Ми бачимо три основні причини:

1. Це дозволяє їм приховати сам факт завантаження або вивантаження даних, а не лише самі дані.

2. Допомагає обійти системи глибокого пакетного інспекцій (DPI), що є актуальним у корпоративних мережах.

3. Використання стеганографії може допомогти обійти перевірку в AntiAPT-продуктах, оскільки останні не можуть обробляти всі графічні файли (їх занадто багато в корпоративних мережах, а алгоритми аналізу є дорогими).

Які висновки можна зробити з цього дослідження?

Адже сучасні технології стеганографії розвиваються, і таким чином стають все більш складними і надійними. Означені технології використовують різні методи, включаючи LSB стеганографію, фреквенційну стеганографію та здійснення текстових форматів. Застосування стеганографії має свої переваги, такі як забезпечення конфіденційності та захист від аналізу даних.

Проте, важливо зауважити, що використання стеганографії для зловживання або злочинних цілей може бути незаконним і порушувати приватність та безпеку.

Таким чином, розвиток алгоритмів стеганографії вимагає постійно динамічного оновлення та адаптаціїв системі превентивних заходів кібер безпеки, оскільки методи виявлення стеганографії також постійно розвиваються. Тому важливо триматися в курсі останніх тенденцій у цій сфері для захисту ефективного та безпечного використання стеганографії в різних галузях.

1.2 Класифікаційно-категоріальний характер приорітетних алгоритмів у захисті інформації

Мультирівнева модель даних щодо кібербезпеки критичних інфраструктур

У сучасному цифровому світі, де кіберзагрози стають все більш складними та небезпечними, забезпечення кібербезпеки критичної інфраструктури постає надзвичайно важливою задачею. Це вимагає класифікаційно-категоріального характеру вдосконалення підходів до захисту від кіберзагроз та здійснення ефективно-діючих інноваційних стратегій. Одним із класифікаційних лейтмотивів цієї проблеми є розробка та впровадження мультирівневої моделі даних.

При цьому, питання класифікаційного регулюванння мультирівневої моделі даних, саме щодо *системи кіберзахисту* об'єктів критичної інфраструктури, і діагностика стану кібербезпеки є одним із важливих та актуальним в умовах повоєнної України. У сучасних кібервійнах XXIго століття, що є надто актуальним для усього світу, у яких весь світ перейшов (змістився) саме у такі війни, надає нам питомої ваги. Українські організації мають бути максимально захищені від кібератак. Як зазначають в державній службі спеціального зв'язку та захисту інформації України «кібербезпека критичної інфраструктури – це один із пріоритетів національної безпеки України» (136).

Також варто зазначити, що у сучасному світі, в якому нормативно-правове середовище постійно змінюється та стає все складнішим, ідентифікація вимог стає надзвичайно важливою для бізнесу, урядових органів та для всієї критичної інфраструктури загалом. Тому, у воєнній кіберсучасності, захист *критичної інфраструктури* є одним із першочергових завдань держави, зважаючи на те, що в Україні впроваджуються новітні інформаційно-комунікаційні технології в усіх сферах життевого світу.

За умов кіберсучасності існує ряд нормативних документів, які визначають класифікаційно-котегоріальні лейтмотиви кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями,

які відповідно до законодавства віднесені до об'єктів критичної інфраструктури. Це: Постанова Кабінету Міністрів України від 19.06.2019 № 519 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»; Постанова Кабінету Міністрів України від 11.11.2020 № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»; Постанова Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»; Постанова Кабінету Міністрів України від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»; Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 (із змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку від 10.07.2022 № 343); Наказ Адміністрації Держспецзв'язку від 01 грудня 2023 року №1011 «Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» та інші.

Питання кібербезпеки критичної інфраструктури в своїх працях досліджували такі вчені: Гнатюк С.О. [13], Іванюта С.П. [128], Кондратов С.І. [38], Лук'янчук Р.В. [56], Леонов Б.Д. [5], Рижов І.М. [104], Серьогін В.С. [54], Суходоля О.М. [20], Цяпа С.М. [122], та ін. Напрями розвитку кібербезпеки розглядали в своїх працях Лєбєдєвим В., Огороднiковим Д., Олейніком М., Прозоровим Д., Свищевим А. Питання мультирівневої моделі в кібербезпеці Харченко В.П., Корченко О.Г., Гнатюк С.О. [119,120] та інші.

Знову-таки питанням безпеки інформації почали приділяти увагу наприкінці 80-х років. У наш час з'явилися перші моделі захисту інформації для вищих органів влади і потужних комерційних структур. Оскільки основна шкода інформації, як правило, завдається злочинними діями (вірусами, зломами секретних ключів, викраденням даних тощо), для боротьби з ними створюються

різні механізми безпеки, що включають організаційні, технічні і програмні заходи і засоби захисту інформації [38, С.16]. Проте, системного аналізу щодо мультирівневої моделі даних у ідентифікації кібер безпеки не було досліджено.

Адже в умовах стрімкого розвитку інформаційних технологій та діджиталізації, все більше інформації цифровізується і тому кібербезпека стає надзвичайно важливою для забезпечення безпеки та конфіденційності інформації. Тому, мультирівневі моделі даних виступають як важливий категоріальний інструмент у боротьбі з кіберзагрозами, надаючи комплексний підхід до захисту інформації .

Крім того мультирівнева модель даних в класифікаційно-категоріальному розумінні забезпечує структурований підхід до збору, організації та аналізу інформації про нормативно-правове середовище. Ця модель дозволяє розглядати дані на кількох рівнях абстракції, починаючи від конкретних вимог і закінчуючи високорівневими політиками та стратегіями.

Адже багаторівнева (мультирівнева) модель безпеки побудована на моделях перевірки повноважень і істинності, надає санкціонований доступ користувачам до закритої інформації БД за заздалегідь визначеними повноваженнями. Проте, для захисту цього недостатньо, оскільки такі моделі не мають класів секретності, а в БД, як правило, зберігається інформація від відкритої до цілком таємної. Для таких цілей призначена багаторівнева модель безпеки Белла-ЛаПадула (Bell-LaPadula), яку ще називають «моделлю вищого рівня секретності» [99, 98] , котра надає користувачам доступ до секретних даних БД за різними класами секретності і є класичною моделлю повноважного (мандатного) розмежування доступу до даних. В моделі Белла-ЛаПадула використовуються такі поняття, як рівень секретності, заданий і поточні рівні допуску користувача, рівень ієрархії об’єктів, інші [86].

Таким чином, переваги використання мультирівневої моделі даних включають уможливлення більш точного визначення вимог, підвищення ефективності аналізу ризиків та забезпечення відповідності з регуляторними вимогами.

Використання мультирівневої моделі даних також допомагає уникнути дублювання інформації та покращує управління знаннями в організації, що є прерогативою спецслужб.

В класифікаційно-котегоріальному характері пріоритетних алгоритмів у захисті інформації варто відзначити Ідентифіка́цію (лат. Identifico). – «Це упізнання чого-небудь або кого-небудь. У цьому значенні термін використовується в психології загальній, інженерній і юридичній, де розуміється як процес зіставлення, звірення одного об'єкта з іншим на підставі будь-якої ознаки або властивості, в результаті чого встановлюється їхня подібність або відмінність. Ідентифікація – це дія встановлення ідентичності.»

У цьому змісті Ідентифікація зокрема (інформаційна безпека) – це процедура розпізнавання користувача в системі, як правило, за допомогою превентивно визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Ідентифікація використовується для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється автентифікація та авторизація. [137]

Тому, саме нормативно-правове регулювання класифікаційно-котегоріального характеру мультирівневої моделі даних варто розуміти як предмет юрисдикції, закріпленний Конституцію України, щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації. Відповідно до цього мають бути визначені правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. [138]

При цьому, Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (24).

На наш погляд стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – як збереження конфіденційності, цілісності та доступності інформації у кіберпросторі.

Згідно з Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

1) створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

2) підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

3) вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

4) розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація. [139]

Об'єкти критичної інфраструктури – це стратегічно важливі підприємства та установи необхідні для функціонування суспільства країни та її економіки.

Підприємства що відносяться до об'єктів критичної інфраструктури:

1. урядування та надання найважливіших публічних (адміністративних) послуг;
2. енергозабезпечення (у тому числі постачання теплової енергії);
3. водопостачання та водовідведення;
4. продовольче забезпечення;
5. охорона здоров'я;
6. фармацевтична промисловість;

Терміном «критична інфраструктура», зазвичай, охоплюються ті об'єкти, системи, мережі або їх частини, порушення функ-