Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут комп’ютерних наук та штучного інтелекту

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ

Марина ЄСІНА

«Допущено до захисту»

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Аналіз та розробка заходів комп’ютерної протидії застосуванню хакерами NCDP»

оцінка « _____ »

Керівник: к.т.н. Громико І.О.

Голова ЕК

Рецензент: к.т.н. Шостак А.В.

Мичуда Л.З.

Виконавець: студент групи КБ-42

Юрченко М.П.

Харків 2025

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи бакалавра містить 48 сторінок, 10 рисунків, 1 таблицю, 31 посилання на джерела.

Мета роботи полягає у комплексному аналізі загроз, пов'язаних із застосуванням нейроколородинамічного програмування зображень (NCDP) у комп'ютерних мережах, а також у розробці й апробації методів та інструментів для виявлення і протидії атакам такого типу.

Об'єкт дослідження — механізми впливу NCDP у комп'ютерних мережах.

Предмет дослідження — теоретичні засади NCDP, психофізіологічний вплив динамічного візуального контенту на користувача, основні вектори атак, програмно-апаратні засоби захисту, а також методи виявлення й блокування шкідливого візуального контенту.

Основними методами дослідження є аналіз літератури, моделювання NCDP-атак у honeynet-середовищі, аналіз зображень, тестування програмних та апаратних засобів захисту, використання спеціалізованого програмного забезпечення для моніторингу та аналізу логів.

У роботі систематизовано теоретичні та практичні основи нейроколородинамічного програмування зображень, проаналізовано сучасні загрози, пов'язані з NCDP, розроблено практичний інструментарій для ідентифікації та блокування шкідливого динамічного візуального контенту, запропоновано архітектуру honeynet-системи для тестування атак та експериментально перевірено ефективність впроваджених захисних рішень.

Результати роботи можуть бути використані у корпоративних мережах, операторських диспетчерських центрах, SCADA-системах, VR/AR-технологіях, а також при створенні спеціалізованого захисного програмного забезпечення для масового користувача.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, NCDP, КІБЕРБЕЗПЕКА, КОМП'ЮТЕРНА МЕРЕЖА, ПСИХОФІЗІОЛОГІЧНИЙ ВПЛИВ, ХАКЕРСЬКІ АТАКИ, ДИНАМІЧНИЙ ВІЗУАЛЬНИЙ КОНТЕНТ, HONEYPOT, HONEYNET,

CYBER DECEPTION, ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ, ВИЗНАЧЕННЯ ЗАГРОЗ, ЗАХИСТ КОРИСТУВАЧА.

ABSTRACT

The explanatory note for the bachelor's qualification thesis contains 48 pages, 10 illustrations, 1 table and 31 references.

The aim of the work is to conduct a comprehensive analysis of threats associated with the use of NeuroColorDynamic Programming (NCDP) of images in computer networks, as well as to develop and test methods and tools for detecting and counteracting such attacks.

The object of the research is the mechanisms of NCDP influence in computer networks.

The subject of the research is the theoretical foundations of NCDP, the psychophysiological impact of dynamic visual content on the user, main attack vectors, hardware and software protection tools, as well as methods for detecting and blocking malicious visual content.

The main research methods include literature analysis, modeling of NCDP attacks in an isolated honeynet environment, spectral and steganographic image analysis, testing of software and hardware protection tools, and the use of specialized software for monitoring and log analysis.

The thesis systematizes the theoretical and practical foundations of NeuroColorDynamic Programming of images, analyzes modern threats related to NCDP, develops practical tools for identifying and blocking malicious dynamic visual content, proposes a honeynet system architecture for testing attacks, and experimentally verifies the effectiveness of implemented protective solutions.

The results of this work can be applied in corporate networks, operator dispatch centers, SCADA systems, VR/AR technologies, as well as in the development of specialized protective software for mass users.

Keywords: INFORMATION SECURITY, NCDP, CYBERSECURITY, COMPUTER NETWORK, PSYCHOPHYSIOLOGICAL IMPACT, HACKER ATTACKS, DYNAMIC VISUAL CONTENT, HONEYPOT, HONEYNET, CYBER

DECEPTION, INFORMATION DISPLAY, THREAT DETECTION, USER PROTECTION.

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

API — Application Programming Interface
CIA — Confidentiality, Integrity, Availability
DDoS — Distributed Denial of Service
GIF — Graphics Interchange Format
GPU — Graphics Processing Unit
GUI — Graphical User Interface
HTML — HyperText Markup Language
ICC — International Color Consortium
IP — Internet Protocol
MITM — Man-In-The-Middle
NCDP — NeuroColorDynamic Programming
NLP — Neuro-Linguistic Programming
OS — Operating System
SCADA — Supervisory Control and Data Acquisition
SVG — Scalable Vector Graphics
TCP — Transmission Control Protocol
USB — Universal Serial Bus
VR/AR/XR — Virtual Reality / Augmented Reality / Extended Reality
WebGL — Web Graphics Library
LED — Light Emitting Diode
OEM — Original Equipment Manufacturer
ІКС — інформаційно-комунікаційні системи
ІТ — інформаційні технології
ІТЗ — інженерно-технічний захист
КС — комп’ютерна система
НСД — несанкціонований доступ
ОС — операційна система
ПЗ — програмне забезпечення

ПРД — правила розмежування доступу

ЦУС — центр управління системою

ВСТУП

Нейроколородинамічне програмування (NCDP) посідає особливе місце серед новітніх міждисциплінарних досліджень на перетині когнітивних наук, комп'ютерного зору, кібербезпеки та навіть технологій з використанням ШІ. Концептуально, нейроколородинамічне програмування спирається на класичну модель «сенсор - нейрон - поведінка» з перенесенням акценту із вербальних або аудіальних подразників на динамічні колірні стимули, що здатні модулювати зорову кору й глибші підкіркові структури мозку. Починаючи від робіт про підпорогову стимуляцію, які продемонстрували прямий вплив швидкоплинних візуальних сигналів на емоційну плинність та мотиваційні стани людини, учені дедалі частіше звертаються до питання: чи можна системно «кодувати» поведінку за допомогою керованих колірних патернів, що подаються через екрани, шоломи віртуальної реальності або світлодіодні інсталяції.

В даній ієрархії колір, як данність, перестає бути лише естетичним елементом інтерфейсу. Він починає набувати буквально фізіологічних властивостей. Завдяки високій чутливості фоторецепторів—людське око здатне реєструвати навіть поодинокі фотони—необхідна амплітуда впливу може залишатися нижчою за свідомий поріг помітності, але достатньою для формування довготривалих асоціативних зв'язків у лімбічній системі. Така «тиха» стимуляція, аналогічна принципам нейролінгвістичного програмування (НЛП), отримала в літературі окрему назву neurocognitive hacking—систематичне залучення підпорогових сигналів для активації вибраних зон мозку й, відтак, корекції поведінкових реакцій адресата. Саме цей підхід образно описується влучним висловом "the mind has no firewall" – що означає: мозок позбавлений природних механізмів фільтрації, що штучно сформовали б зорові ін'єкції, на відміну від інформаційно-комунікаційних інфраструктур, що захищаються програмними міжмережевими екранами.

В інформаційно-технічному вимірі NCDP розглядається як непрямий вектор атаки на критичні системи, адже, як відомо, кінцева ланка більшості кіберфункцій - людина-оператор, як ціль абсолютно всіх атак соціальної інженерії - залишається

найуразливішою. Історичним прецедентом стали координовані напади на спільноти людей з фоточутливою епілепсією у соцмережах, де зловмисники поширювали стробоскопічні GIF-зображення, що спричиняли епілептичні припадки в реальних постраждалих. Подібні інциденти засвідчили, що піксельний контент може виконувати функцію цілеспрямованої «зброї світла», здатної виводити з ладу як фізичний, так і когнітивний ресурс оператора ПК. У військово-стратегічних оцінках підкреслюється, що контроль над каналами візуального відображення відкриває шлях до нових форм інформаційно-психологічних операцій, оскільки навіть короткочасна дезорієнтація чергового персоналу ЦУС або SOC може мати ефект, співрозмірний із традиційною DDoS-атакою на апаратний сегмент мережі.

Крім безпосередніх фізіологічних ризиків (наприклад, судом або фотостресу), дослідження показують зростання психосоціальних загроз: негативно спрямовані підсвідомі повідомлення (зміщені до червоної гами флеш-кадри, “маскування” тривожних слів у колірній текстурі тощо) статистично ефективніше формують у користувача агресивні, упереджені судження чи навіть хибні уявлення про ті чи інші обставини — феномен, підтверджений експериментами з негативними субліміальними праймами. Технологічне ж підґрунтя атаки може варіюватися від стеганографічних вставок у відеопотоці та ін’єкцій на рівні драйверів GPU, передачі USB-носіями, проникненням в трафік і передачею «заражених» NCDP даних через пакети TCP до підмінених мікропрограм LED-панелей - тобто NCDP може наслідувати будь-який класичний ланцюг кіберзараження (kill-chain), але з кінцевою точкою «екран-око-мозок».

Нейроколородинамічне програмування формує нову площину загроз, де цифровий код безпосередньо перетікає у нейронний код глядача. Метою даного дослідження є всебічний аналіз NCDP у проєкції на кібербезпеку: теоретичні засади й нейрофізіологічні механізми кольоронавіювання; технічні методи ін’єкції та канали розповсюдження атак; підходи до детектування та попередження “колірних експлойтів”; правові, етичні та організаційні аспекти протидії. З урахуванням того, що людський фактор залишається “останньою милею” у

ланцюгу безпеки, подальші розділи окреслять, яким чином NCDP-засоби можуть перетворитися на повноцінну кіберзброю та як створити багаторівневу систему оборони проти таких невидимих, але відчутних атак.

Метою даного проекту є дослідження загроз нейроколородинамічного програмування (NCDP) в інформаційних системах, розробка й апробація методів виявлення та протидії атакам через динамічний візуальний контент. Проект спрямований на поглиблення розуміння механізмів впливу високочастотних кольорових патернів на операторів, а також створення практичного інструментарію для захисту користувачів від подібних когнітивних атак.

Результати даного проекту є актуальними для організацій, які експлуатують критичні інформаційні та керуючі системи — операторські диспетчерські центри, SCADA-системи, центри моніторингу промислової автоматизації, військові командні пункти, фінансові та медичні платформи, а також для розробників захисного ПЗ для масового користувача. З огляду на поширення візуальних інтерфейсів у повсякденній діяльності, запропоновані методи можуть бути впроваджені у корпоративних мережах, системах відеоспостереження, VR/AR-технологіях та освітньо-інформаційних платформах.

Виконанням проекту є розробка та реалізація комплексної системи, що включає в себе ізольоване лабораторне середовище (honeynet-архітектуру), інструменти моделювання NCDP-атак, систему серверного й клієнтського моніторингу, а також захисний скрипт для автоматичного виявлення та блокування шкідливого візуального контенту. У результаті проекту здійснено експериментальну перевірку ефективності розроблених рішень, сформульовано рекомендації щодо їх впровадження та визначено перспективи подальшого розвитку захисту від новітніх когнітивних загроз.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОНТЕКСТІ NCDP

1.1. Поняття інформаційної безпеки та її складові

Інформаційна безпека — це практика захисту інформації шляхом пом’якшення інформаційних ризиків [1]. Це частина управління інформаційними ризиками. Зазвичай це передбачає запобігання або зменшення ймовірності несанкціонованого чи неналежного доступу до даних або незаконного використання, розголошення, порушення, видалення, пошкодження, модифікації, перевірки, запису або знецінення інформації. Це також передбачає дії, спрямовані на зменшення негативних наслідків таких інцидентів. Захищена інформація може мати будь-яку форму, наприклад, електронну або фізичну, матеріальну (наприклад, папери) або нематеріальну (наприклад, знання). Основним напрямком інформаційної безпеки є збалансований захист конфіденційності, цілісності та доступності даних, зосереджуючись при цьому на ефективній реалізації політики, і все це без шкоди для продуктивності організації. Це значною мірою досягається завдяки структурованому процесу управління ризиками.

Щоб стандартизувати цю дисципліну, науковці та професіонали співпрацюють, щоб запропонувати вказівки, політики та галузеві стандарти щодо паролів, антивірусного програмного забезпечення, брандмауерів, програмного забезпечення для шифрування, юридичної відповідальності, обізнаності з питань безпеки та навчання тощо [2]. Ця стандартизація може додатково стимулюватися різноманітними законами та правилами, які впливають на те, як доступ до даних, їх обробка, зберігання, передача та знищення.

У той час як паперові ділові операції все ще переважають і вимагають власного набору практик інформаційної безпеки, все більше часу приділяється корпоративним цифровим ініціативам, причому зараз забезпеченням інформації зазвичай займаються спеціалісти з безпеки інформаційних технологій (IT). Ці фахівці застосовують інформаційну безпеку в технологіях (найчастіше в певній формі комп’ютерної системи).

Фахівці з інформаційної безпеки майже завжди є на будь-якому великому підприємстві/установі через характер і цінність даних у великих компаніях. Вони відповідають за захист усіх технологій у компанії від зловмисних атак, які часто намагаються отримати важливу особисту інформацію або отримати контроль над внутрішніми системами.

Існує багато ролей спеціалістів у сфері інформаційної безпеки, включаючи забезпечення безпеки мереж і суміжної інфраструктури, забезпечення безпеки додатків і баз даних, тестування безпеки, аудит інформаційних систем, планування безперервності бізнесу, виявлення електронних записів і цифрову криміналістику.

У контексті теми NCDP поняття інформаційної безпеки є фундаментальним. В тріаді CIA конфіденційність з боку NCDP – це захист зорового поля від «утікання» прихованих керуючих стимулів, які оператор не санкціонував і не усвідомлює їх наявність. Цілісність же відповідає за гарантування того, що зображення, яке бачить оператор не було невидимо модифіковано зловмисником для формування помилкового, упередженого рішення. Доступність в такому випадку – це здатність користувача отримувати безпечний, немодифікований контент у будь-який час.

1.2. Загрози несанкціонованого доступу в сучасних ІКС

Несанкціонований доступ — це процес втручання до системи, фізичної чи електронної, без дозволу власника чи адміністратора. Такий доступ можна отримати, обходячи заходи безпеки, використовуючи вразливі місця системи або використовуючи вкрадені облікові дані. Несанкціонований доступ є серйозним порушенням законів про конфіденційність і може призвести до тяжких наслідків, у тому числі до судових позовів.

У сфері кібербезпеки неавторизований доступ означає порушення комп’ютерних систем, мереж або баз даних. Ці порушення зазвичай пов’язані з проникненням хакерів у систему з метою викрадення, зміни або знищення інформації. Однак важливо зазначити, що неавторизований доступ не обмежується

атаками зовнішніх хакерів. Це також може включати доступ співробітника до файлів або інформації за межами його рівня авторизації.

Дедалі більш поширена загроза несанкціонованого доступу викликає серйозні занепокоєння щодо безпеки даних, конфіденційності та цілісності цифрових систем. Це становить значний ризик для окремих осіб, корпорацій і урядів [3][4].

Під несанкціонованим доступом (НСД) у комп'ютерних системах слід розуміти «доступ до інформації з використанням засобів, включених до складу КС, що порушує встановлені правила розмежування доступу (ПРД)» [5]. У контексті побудови системи захисту інформації в ІКС, поняття НСД має ключове значення, оскільки його попередження є основною метою впровадження політик інформаційної безпеки.

До основних способів реалізації НСД відносяться:

- «безпосереднє звертання до об'єктів з цілю одержання певного виду доступу»;
- «створення ПЗ, що виконують звертання до об'єктів в обхід засобів захисту»;
- «модифікація засобів захисту, що дозволяє здійснити НСД»;
- «впровадження в КС програмних або апаратних механізмів, що спотворюють структуру і функції КС і дозволяють здійснити НСД»

Під захистом від НСД «слід розуміти діяльність, спрямовану на забезпечення додержання ПРД шляхом створення і підтримки в дієздатному стані системи заходів захисту інформації» (розділ 6.4). Тобто захист полягає не лише у впровадженні технічних рішень, але й у безперервному підтриманні їх працездатності.

Для аналізу загроз також використовується модель порушника. «Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами». Залежно від можливостей, порушники класифікуються за такими рівнями:

- «можливість запуску фіксованого набору завдань»;

- «можливість створення і запуску власних програм»;
- «можливість управління функціонуванням КС»;
- «можливість включення до складу КС власних засобів» [6].

Таким чином, нормативний документ чітко окреслює як саме визначається НСД, якими можуть бути його способи реалізації, а також яку роль відіграє побудова захисту і класифікація потенційних порушників. Цей документ і комплект нормативних документів, що базується на ньому, присвячений питанням організації захисту від НСД і побудови засобів захисту від НСД, що функціонують у складі обчислювальної системи АС.

1.3. Методи та засоби захисту інформації. Головний закон захисту інформації

До методів і засобів організаційного захисту (див. рис. 1.1)[7] інформації належать організаційнотехнічні та організаційно-правові заходи, що проводяться в процесі створення та експлуатації КС для забезпечення захисту інформації [8][9].

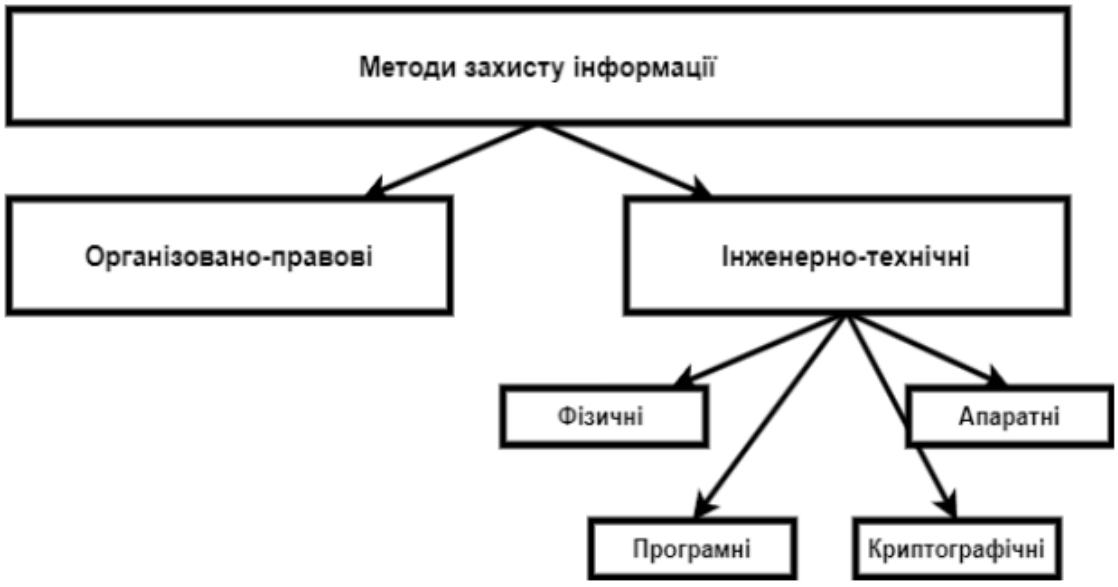

Рисунок 1.1. Класифікація методів захисту інформації в ІКС

Ці заходи мають проводитися під час будівництва або ремонту приміщень, у яких розміщуватимуться комп'ютери; проєктування системи, монтажу та налагодження її технічних і програмних засобів; випробувань і перевірки працездатності комп'ютерної системи. Основою проведення організаційних заходів є використання та підготовка законодавчих і нормативних документів у сфері інформаційної безпеки, які на правовому рівні мають регулювати доступ до інформації з боку споживачів. Методи та засоби інженерно-технічного захисту інформації. Інженерно-технічний захист (ІТЗ) - це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації. Різноманіття цілей, завдань, об'єктів захисту і заходів, що проводяться, передбачає розгляд деякої системи класифікації засобів за видом, орієнтацією та іншими характеристиками. Наприклад, засоби інженерно-технічного захисту можна розглядати за об'єктами їхнього впливу. У цьому плані вони можуть застосовуватися для захисту людей, матеріальних засобів, фінансів, інформації. Різноманіття класифікаційних характеристик дає змогу розглядати інженерно-технічні засоби за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким чиниться протидія з боку служби безпеки[10] За функціональним призначенням засоби інженерно-технічного захисту поділяються на такі групи:

1) фізичні засоби, що включають різні засоби і споруди, які перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних впливів;

2) апаратні засоби - прилади, пристрої, пристосування та інші технічні рішення, що використовуються в інтересах захисту інформації. У практиці діяльності підприємства знаходить широке застосування найрізноманітніша апаратура, починаючи з телефонного апарата до досконалих автоматизованих систем, що забезпечують виробничу діяльність. Основне завдання апаратних засобів - забезпечення стійкого захисту інформації від розголошення, витоку і

несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності;

3) програмні засоби, що охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різного призначення та засобах обробки (збирання, накопичення, зберігання, обробка та передача) даних [11];

4) криптографічні засоби - це спеціальні математичні та алгоритмічні засоби захисту інформації, яку передають системами і мережами зв'язку, зберігають і обробляють на ЕОМ із використанням різноманітних методів шифрування.

Фізичні засоби захисту - це різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників. До фізичних засобів належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для перешкоджання несанкціонованому доступу (входу, виходу), пронесенню (виносу) засобів і матеріалів, та інших можливих видів злочинних дій. Ці засоби застосовуються для вирішення таких завдань:

1) охорона території підприємства і спостереження за нею;

2) охорона будівель, внутрішніх приміщень і контроль за ними;

3) охорона обладнання, продукції, фінансів та інформації;

4) здійснення контрольованого доступу в будівлі та приміщення. Усі фізичні засоби захисту об'єктів можна поділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. Охоронна сигналізація та охоронне телебачення, наприклад, належать до засобів виявлення загроз; паркани навколо об'єктів - це засоби запобігання несанкціонованому проникненню на територію, а посилені двері, стіни, стелі, решітки на вікнах та інші заходи слугують захистом і від проникнення, і від інших злочинних дій (підслуховування, обстріл, кидання гранат і вибухових пакетів тощо). Засоби пожежогасіння належать до систем ліквідації загроз. Апаратні методи та засоби захисту інформації. До апаратних засобів захисту інформації належать найрізноманітніші за принципом дії, пристроєм і можливостями технічні конструкції, що забезпечують припинення

розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації. Апаратні засоби захисту інформації застосовуються для вирішення таких завдань:

1) проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;

2) виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;

3) локалізація каналів витоку інформації;

4) пошук і виявлення засобів промислового шпигунства;

5) протидія несанкціонованому доступу до джерел конфіденційної інформації та іншим діям. Програмні методи та засоби захисту інформації Системи захисту комп'ютера від чужого вторгнення вельми різноманітні і класифікуються, як:

1) засоби власного захисту, передбачені загальним програмним забезпеченням;

2) засоби захисту в складі обчислювальної системи;

3) засоби захисту із запитом інформації;

4) засоби активного захисту;

5) засоби пасивного захисту та інші. Основні напрями використання програмного захисту інформації. Можна виокремити такі напрями використання програм для забезпечення безпеки конфіденційної інформації, зокрема такі:

1) захист інформації від несанкціонованого доступу;

2) захист інформації від копіювання;

3) захист програм від копіювання;

4) захист програм від вірусів;

5) захист інформації від вірусів;

6) програмний захист каналів зв'язку. За кожним із зазначених напрямів є достатня кількість якісних, розроблених професійними організаціями і розповсюджуваних на ринках програмних продуктів.[12] Програмні засоби захисту мають такі різновиди спеціальних програм:

1) ідентифікації технічних засобів, файлів та автентифікації користувачів;

2) реєстрації та контролю роботи технічних засобів і користувачів;

3) обслуговування режимів обробки інформації обмеженого користування;

4) захисту операційних засобів ЕОМ і прикладних програм користувачів[13];

Згідно з визначенням, що надає Громико І.О., Інформація рахується захищеною, коли при здійсненні інформаційної діяльності у ланцюгах інформаційної співдії виконується режимна адекватність і комунікабельність всіх носіїв інформації, що знаходяться в данній ІКС [14][15].

Цей підхід спирається на фундаментальне положення про те, що інформація завжди існує у зв’язку з певним носієм — фізичним, цифровим, біологічним або змішаним. Інформація — це «зафіксоване на носії уявлення про предмети, процеси, події, природні явища тощо», і тому її захист неможливо розглядати у відриві від властивостей самого носія.

У цьому контексті режимна адекватність носіїв трактується як відповідність рівнів доступу всіх учасників інформаційної взаємодії, тобто дотримання правил допуску до інформації в рамках допустимих прав і повноважень. У свою чергу, комунікабельність носіїв означає їхню здатність взаємодіяти без помилок, з дотриманням узгоджених семантичних і технічних стандартів, які забезпечують цілісність інформації в процесі обміну.

2 АНАЛІЗ ЗАГРОЗ, ПОВ'ЯЗАНИХ З NCDP

2.1. Основи нейроколородинамічного програмування

Нейроколородинамічне програмування (NCDP) – це умовний термін для позначення методик впливу на нервову систему людини за допомогою динамічних кольорових візуальних стимулів. Ідея подібного «програмування» ґрунтується на тому, що колір та світлові патерни здатні викликати вимірювані нейрофізіологічні реакції і, як наслідок, впливати на психологічний стан та поведінку користувача. Сучасна наука накопичила значні дані про обробку кольорових сигналів зоровою системою та мозком (так звана колірна нейрофізіологія). Зокрема, відомо, що різні кольори можуть по-різному активувати ділянки мозку і гормональні реакції, впливаючи на емоції та навіть фізіологічні показники. Наприклад, встановлено, що червоний колір здатен підвищувати частоту пульсу і рівень збудження, тоді як блакитний – заспокоювати. Інші дослідження вказують, що червоні й жовті стимули підсвідомо роблять людей більш імпульсивними, тоді як сині – знижують рівень активації [16]. Отже, колірне середовище впливає не лише на свідоме сприйняття (естетику), але й на фундаментальні психологічні функції людини.

Не менш важливою є динаміка візуальних сигналів – зміна кольорів, мерехтіння, ритмічність. Мерехтливі світлові стимули можуть викликати явище фотостимульованої активності мозку, коли електричні ритми мозку починають синхронізуватися з частотою мерехтіння зовнішнього сигналу. Цей ефект, відомий як photic driving, демонструє прямий нейрофізіологічний вплив динамічного світла на мозок: при певній частоті зоровий центр переймає зовнішній ритм імпульсів, що може змінювати поточний стан мозкової активності. У контрольованих умовах це явище використовується, наприклад, для дослідження функцій зорової кори чи навіть для аудіовізуальної стимуляції з метою зміни настрою.

Нейроколородинамічне програмування описується як застосування наукових знань про вплив кольору і світло-колірної динаміки на нервову систему для цілеспрямованого формування реакцій психіки оператора. За аналогією з нейролінгвістичним програмуванням, що оперує словесними і поведінковими

патернами, NCDP оперує саме візуально-кольоровими стимулами. У відкритій літературі це поняття перетинається із дослідженнями в галузях сублімінального візуального впливу та когнітивного хакингу. Зокрема, фахівці з кібербезпеки вводять термін «когнітивний злом» для опису атак, націлених не на комп'ютерні системи, а на вразливості сприйняття та мислення людини. Вважається, що презентація інформації нижче порогу свідомості (так звана сублімінальна примінгова стимуляція) є одним із головних кандидатів на роль вектору такої атаки. Інакше кажучи, якщо зловмисник знайде спосіб програмувати підсвідомі реакції користувача через екран, минаючи його свідомий контроль, це може стати новим типом кібернетичної загрози[17]. NCDP саме і розглядається як концепція таких методів – потенційно небезпечних технік впливу на мозок користувача через кольорові сигнали, що відображаються на моніторі.

2.2. Психофізіологічний вплив зображень на підсвідомість користувачів

Підсвідомий рівень сприйняття візуальної інформації — ключовий елемент, що визначає вразливість людини до впливу динамічних зображень у цифровому середовищі. Нейропсихологічні дослідження останніх десятиліть демонструють, що більша частина вхідного зорового сигналу обробляється автоматично, без участі свідомого контролю (див. рис. 2.1) [19]. Саме це створює основу для впливу сублімінальних візуальних стимулів, які формують психоемоційні реакції або запускають автоматизовані поведінкові патерни без явного усвідомлення користувачем.

Сучасні дослідження в галузі когнітивної нейронауки виявили, що певні образи, кольори чи композиційні структури можуть викликати реакції в структурах головного мозку, відповідальних за емоції (лімбічна система), мотивацію (мезолімбічний дофаміновий шлях), або тривожність (амигдала). При цьому, як показують функціональні МРТ-дослідження, навіть короткочасна презентація зображення тривалістю менше 100 мс (нижче порогу свідомого розпізнавання) здатна викликати зміни у мозковій активності, що фіксуються інструментально[18].

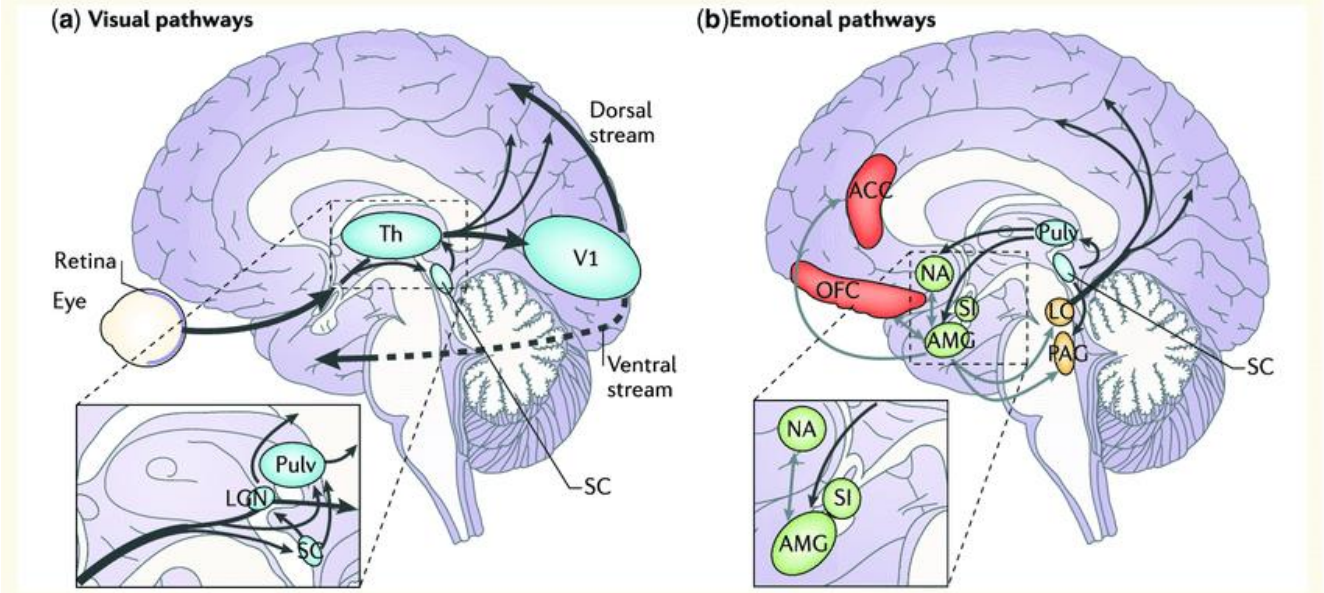

Рисунок 2.1 – Схема обробки зорового сигналу: шлях від сітківки до зорової кори головного мозку.

Візуальні патерни, що активують підкіркові центри, можуть бути використані для формування підсвідомих асоціацій, відрази або прихильності до певних об'єктів, ідей або дій. Це явище відоме як праймінг (англ. priming), і воно широко досліджується в контексті маркетингу, політики та інформаційно-психологічних операцій [20]. У випадку з NCDP, подібний ефект може бути штучно викликаний серіями зображень або кольорових змін, вмонтованих у робоче середовище користувача, наприклад, інтерфейс SCADA-системи чи цифрового щита операторської кімнати.

Окрему загрозу становлять модульовані кольорові послідовності, які за своїми характеристиками (частота зміни, контрастність, амплітуда яскравості) можуть провокувати нейрофізіологічний резонанс, або навіть викликати негативні соматичні ефекти — головний біль, дезорієнтацію, втому, а в деяких випадках — судомні стани (фотосенситивна епілепсія) [21]. Ці реакції посилюються за умови довготривалого впливу або при використанні периферійного бачення, де нейронна обробка менш підконтрольна свідомості.

Експерименти в галузі нейромаркетингу показують, що червоні кольори викликають стресову реакцію, а сині — заспокоюють. Але в умовах

високочастотної модуляції навіть «нейтральні» кольори можуть спричинити зниження когнітивної гнучкості, сповільнення реакцій або зменшення критичного мислення. Це особливо небезпечно в контексті інформаційних систем з високими вимогами до точності та швидкості прийняття рішень.

Важливо розуміти, що зображення в NCDP не обов’язково мають бути чітко вираженими — достатньо градієнтної, періодичної або хаотичної візуальної модуляції, яка сприймається фоторецепторами ока, але не розпізнається свідомістю. Таким чином, оператор може бути підданий впливу навіть у випадках, коли не помічає візуальної «аномалії». Це відкриває простір для впровадження атак за схемою zero-perception vector — тобто таких, що не викликають жодних підозр у цільової особи.

2.3. Потенційні вектори атак через монітори та колірні сигнали

У контексті нейроколородинамічного програмування (NCDP) монітор, дисплей або будь-який інший пристрій виведення зображення виступає не лише засобом інтерфейсу, а й потенційним каналом атаки. На відміну від класичних (див рис 2.2) [23] векторів компрометації (наприклад, експлойтів у програмному коді або мережевих протоколах), у випадку NCDP основною ціллю є сенсорне середовище користувача, зокрема його зорове сприйняття. Саме тому атаки через кольорові та візуальні сигнали вимагають принципово нового підходу до ідентифікації та нейтралізації загроз.

Основним способом реалізації NCDP-атаки є ін’єкція візуального контенту, який передається каналами зв'язку в межах локальної або глобальної мережі. Зараження може відбуватись:

- через модифіковані відеопотоки (наприклад, трансляція з камери спостереження чи навчального ресурсу);
- у вигляді вбудованих зображень у вебсторінки (HTML5/CSS-анімації, SVG-фрейми, WebGL);
- у вигляді модифікованих GUI-компонентів (кнопки, панелі, індикатори, які змінюють колір в специфічній частоті).

Такі вставки можуть бути згенеровані на боці зловмисника або сформовані внаслідок втручання у канали передачі даних (наприклад, підміна вмісту за допомогою MITM-атаки).

Більш складний, але потенційно непомітний метод реалізації полягає в модифікації відеосигналу на рівні драйверів відеокарти або мікропрограмного забезпечення монітора[22]. Відомі приклади фреймворків (наприклад, PixelAttack або GPUStalker), які дозволяють маніпулювати виведеним зображенням без втручання у видимий інтерфейс операційної системи. У такому разі модифікації зображень залишаються невидимими для традиційних засобів контролю безпеки. Атака може бути реалізована через:

- змінені прошивки LED-панелей (supply chain атаки);
- вбудовані кольорові «мерехтіння» в мікропрограму драйвера GPU;
- використання апаратних проксі, що перехоплюють і змінюють відеосигнал (наприклад, між ПК та монітором).

Особливої уваги заслуговують пасивні вектори, де NCDP-контент вже міститься у системі, але не викликає реакцій доти, доки не виконується певна умова: час, місце, IP-адреса, фоновий колір або активність користувача. Це дозволяє зловмиснику уникнути передчасного виявлення. Наприклад, у SCADA-системі певний колірний шаблон може активуватись лише під час нічного чергування, коли персонал найменш уважний.

Зважаючи на зростання популярності мобільних пристроїв, вектор атаки через OLED-дисплеї смартфонів та гарнітур віртуальної/доповненої реальності (XR/VR) набуває особливої загрози. У цих випадках зображення розміщується безпосередньо перед очима, і у разі динамічної стимуляції це створює ще більшу площину впливу. Частоти, близькі до альфа-ритмів мозку (8–13 Гц), у VR-гарнітурі можуть викликати резонансні зміни у стані користувача — зниження концентрації, сонливість, або, навпаки, тривожність.

У деяких випадках зловмисники можуть використовувати переносні носії — USB-диски, картки пам’яті тощо, які містять зображення або відеофайли, що активують механізми NCDP. Такі файли можуть мати вигляд звичайного

презентаційного відео або навіть системної інструкції, вбудованої у службовий матеріал. Це створює вектор офлайн-атаки, коли система фізично ізольована від мережі, але все одно вразлива до зорових ін'єкцій.

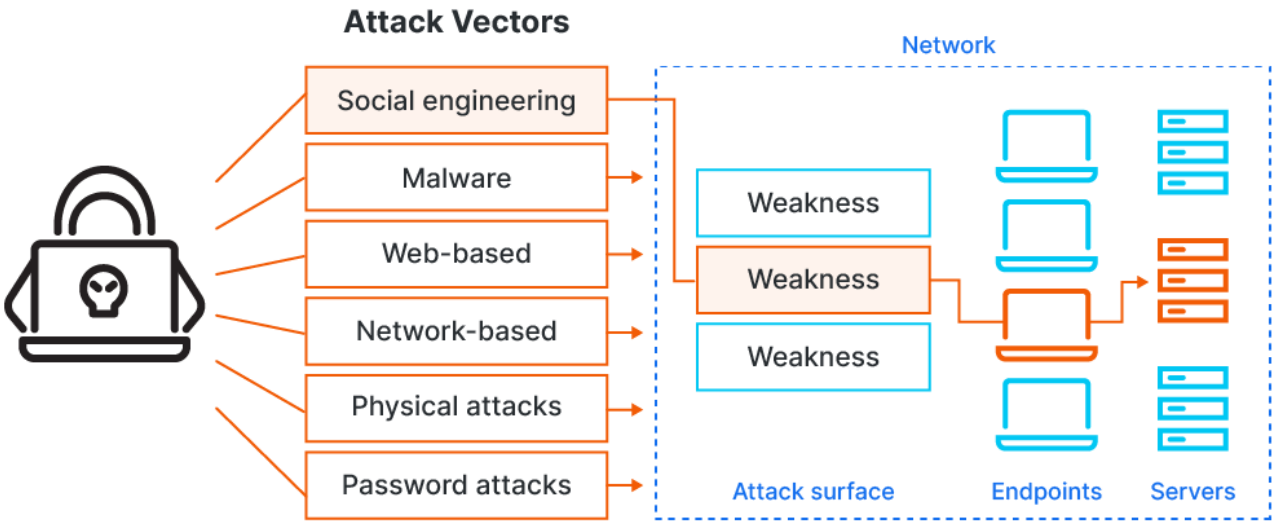

Рисунок 2.2 – Класичні вектори атак у комп'ютерних мережах

2.4. Аналіз місць уразливості комп'ютерних мереж щодо впливу NCDP

На відміну від класичних кіберзагроз, які спрямовані на порушення роботи мережевої інфраструктури або доступу до даних, загрози нейроколородинамічного програмування (NCDP) орієнтовані на найвразливішу ланку будь-якої інформаційної системи — людину-оператора (див. рис. 2.3)[24]. Однак, навіть незважаючи на «когнітивний» вектор впливу, реалізація NCDP-атак неможлива без використання певних технічних, програмних або організаційних слабких місць, через які шкідливий зоровий сигнал потрапляє до кінцевого користувача. Саме тому критично важливим є виявлення таких точок уразливості в інформаційно-комунікаційних системах.

Перш за все, до групи потенційних вразливостей належать компоненти мережевої інфраструктури, відповідальні за формування або передавання зображень. Зокрема, це сервери виводу даних, візуалізаційні модулі SCADA-систем, віддалені панелі моніторингу та аналітики, а також браузерні інтерфейси, що динамічно завантажують візуальний контент з мережі. У таких середовищах зловмисник має змогу інтегрувати модифіковані зображення, відеофрагменти або

анімації, які містять шкідливі кольорові патерни. Особливо небезпечними є випадки, коли контент завантажується з зовнішніх джерел без належного контролю, наприклад, через CDN, iframe або API-запити. Наявність збоїв у перевірці таких джерел відкриває шлях до NCDP-ін'єкцій без втручання в програмний код системи.

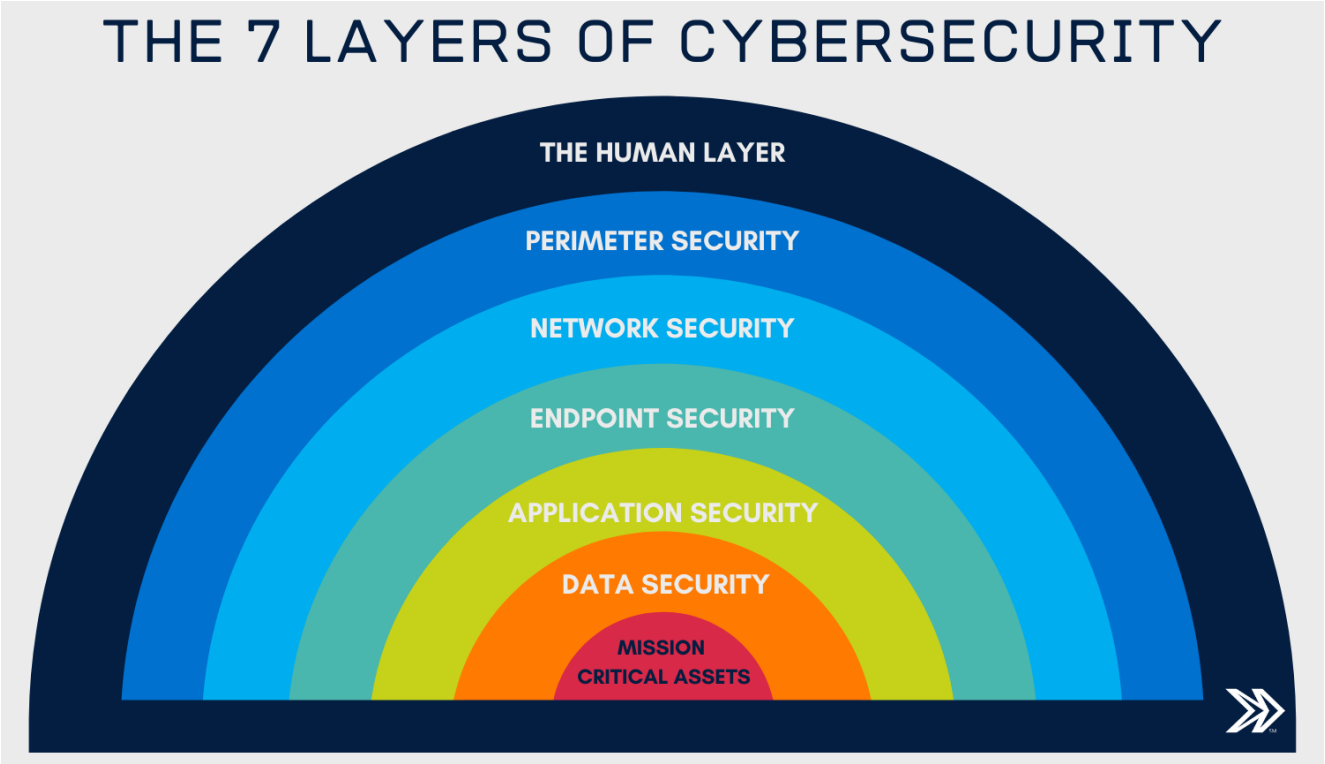

Рисунок 2.3 – Шари кібербезпеки за принципом «кільцевого захисту»

Окрему категорію становлять програмно-апаратні уразливості, пов'язані з можливістю маніпуляції відеосигналом на рівні GPU або драйверів. Зокрема, через зміну мікропрограмного забезпечення відеокарт або LED-дисплеїв, атакуючий може впливати на частоту, яскравість і кольорову палітру зображення, яке виводиться на екран користувача. Подібні атаки особливо важко виявити традиційними засобами моніторингу безпеки, адже вони не змінюють самих даних, лише їхнє візуальне представлення. Крім того, розширення практики застосування XR/VR гарнітур у критичних середовищах (наприклад, для навчання, моделювання або моніторингу ситуацій) створює додаткову вразливість, адже в таких пристроях користувач занурюється у віртуальне середовище, де контроль над кольоровим стимулом є абсолютним.

Не менш важливими є слабкі місця, пов’язані з людсько-машинною взаємодією. Візуальні інтерфейси сучасних інформаційних систем часто не мають механізмів виявлення візуального перевантаження, підсвідомих стимулів або динамічних аномалій у кольоровому спектрі. Так, оператор, який щоденно взаємодіє з десятками інформаційних панелей, не завжди здатен помітити наявність стробоскопічного ефекту або сублімінальної модуляції кольору. В системах, де вивід інформації є безперервним (ЦУС, SOC, диспетчерські пункти), навіть незначні відхилення у зоровому ритмі можуть мати кумулятивний вплив, спричиняючи зниження уважності, порушення сприйняття або помилкові рішення.

Варто зазначити, що значна частина таких уразливостей має не технічну, а організаційну природу. Відсутність політик щодо допустимого візуального навантаження в інтерфейсах, брак перевірок візуального контенту, переданого всередині корпоративної мережі, а також недостатній рівень підготовки персоналу щодо впливу підсвідомих зображень — усе це створює умови для ефективної реалізації NCDP-атак. Прикладом практичної загрози стали відомі випадки у соціальних мережах, де зловмисники навмисне поширювали флеш-графіку, що викликала приступи фотосенситивної епілепсії у вразливих осіб. Ці інциденти засвідчують, що зоровий контент, який формально не є зловмисним у класичному розумінні, може бути використаний як інструмент реального впливу на фізіологію та психіку користувача[25].

Таким чином, комп’ютерна мережа може містити приховані вектори проникнення NCDP навіть у випадках, коли зберігається цілісність даних та виконуються протоколи автентифікації. Вразливим є не тільки програмне середовище, а й те, як саме інформація відображається, сприймається і впливає на поведінку оператора. У наступних розділах буде розглянуто, якими технічними та організаційними засобами можна виявляти, блокувати та моделювати подібні атаки на візуальному рівні, включно з використанням honeynet-систем, алгоритмічного аналізу контенту та технологій когнітивної декепції.

2.5 Різниця між NCDP та NLP

Нейролінгвістичне програмування (NLP, від англ. Neuro-Linguistic Programming) — це підхід, який розглядає можливість впливу на психіку та поведінку людини за допомогою спеціально організованої вербальної або невербальної комунікації. В основі NLP лежить ідея про те, що мислення (нейро), мова (лінгвістика) і моделі поведінки (програмування) тісно пов’язані між собою. Згідно з цією концепцією, зовнішні сигнали — переважно слова, інтонації, жести, тактильні впливи — можуть змінювати способи сприйняття інформації, впливати на підсвідомість людини та програмувати її реакції. Таким чином, NLP активно застосовується у психології, коучингу, маркетингу й навіть кібербезпеці для аналізу й моделювання поведінки людей.

Проте в сучасних умовах розвитку цифрових технологій і візуальної комунікації з’являються нові вектори впливу на людину, які не обмежуються лише мовними чи аудіальними каналами. Одним із таких напрямків є нейроколородинамічне програмування (NCDP, NeuroColorDynamic Programming). Це концепція, що ґрунтується на здатності людини несвідомо сприймати динамічні візуальні стимули[26], зокрема колірні патерни, світлові імпульси та їхню зміну в часі.

Головна відмінність NCDP від NLP полягає у природі впливу. Якщо у випадку NLP ключову роль відіграє мова як засіб передачі інформації до підсвідомості, то у NCDP це роль візуального каналу, а саме — кольору, його динаміки й частотних характеристик. У рамках NCDP для дистанційного впливу на психоемоційний стан або поведінку людини використовуються ретельно підібрані динамічні комбінації кольорів, що можуть спричиняти певні фізіологічні або когнітивні реакції. Наприклад, періодичне миготіння кольорового елемента з частотою 8–13 Гц може впливати на альфа-ритми головного мозку, викликати зміну уваги, дискомфорт або підсвідомі дії оператора.

Таким чином, NCDP розширює ідеологію NLP на сферу сенсорних впливів, в яких мова відходить на другий план, а основним каналом стає орган зору. Це надзвичайно актуально для сучасних інформаційних систем, зокрема для

операторських інтерфейсів та систем управління, де зловмисник може спробувати здійснити когнітивний вплив не через фішинг чи соціальну інженерію, а через модифікацію візуальних компонентів — кольорові патерни, мерехтіння, контрастність тощо.

Схематичне порівняння задіяних функціональних елементів у NLP та NCDP наведено на схемі (див рис 2.4) [27]. NLP базується на вербальній взаємодії, моделюючи зв’язок між нейронними структурами, мовою та поведінкою. NCDP же акцентує увагу на динамічній обробці кольорових стимулів зоровою системою та їхньому впливі на центральну нервову систему, минаючи традиційні мовні чи аудіальні фільтри.

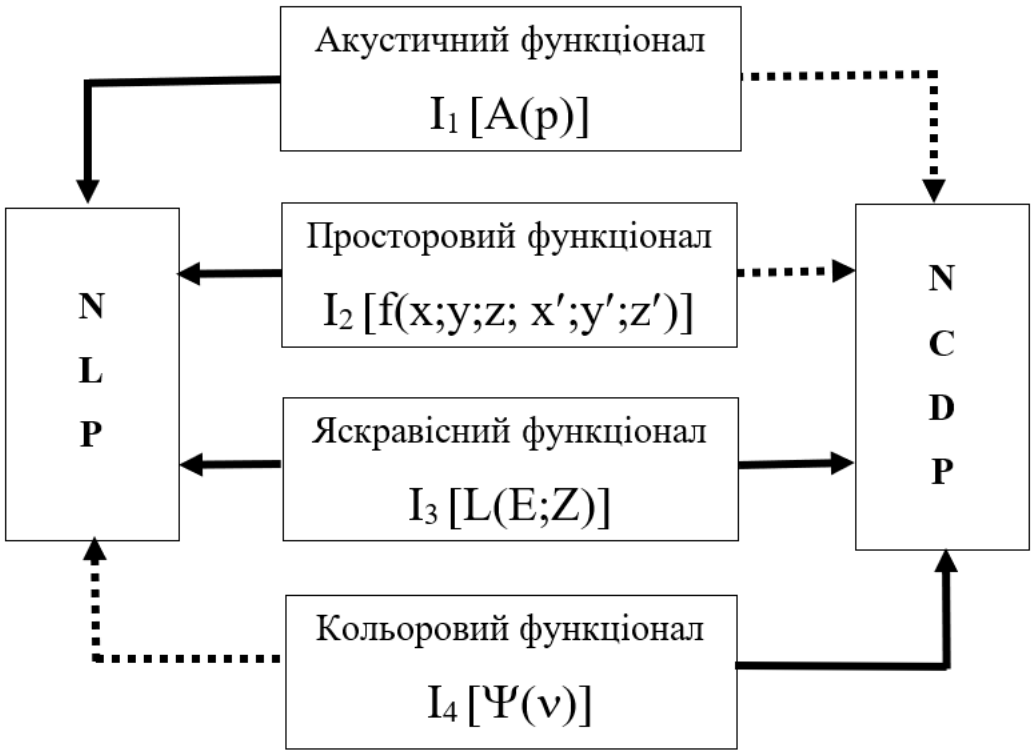

Рисунок 2.4 - Задіяність функціональних елементів у NLP та NCDP.

3 МЕТОДИ ПРОТИДІЇ NCDP В ІКС

3.1. Програмно-апаратні шляхи впливу на відображення інформації

У контексті сучасних інформаційно-комунікаційних систем відображення інформації стає не просто кінцевим етапом трансляції даних користувачу, а й потенційним полем для реалізації різноманітних загроз, зокрема пов’язаних із нейроколородинамічним програмуванням. У зв’язку з цим питання забезпечення безпеки візуального каналу отримує нове, підвищене значення, що вимагає цілісного підходу — як на програмному, апаратному рівнях і логічних рівнях.

З боку програмного забезпечення найбільшу небезпеку становлять ін’єкції модифікованого візуального контенту, які можуть здійснюватися через стандартні інтерфейси користувача, веб-додатки, а також через віддалене або локальне втручання у роботу графічних підсистем. Наприклад, шкідливі скрипти на вебсторінках або модифіковані GUI-компоненти можуть динамічно змінювати кольорову гаму, ритм, яскравість елементів інтерфейсу. Такі зміни здатні лишатися непомітними для користувача на свідомому рівні, однак викликати значний підсвідомий вплив або спричиняти фізіологічний дискомфорт.

Особливу увагу заслуговують атаки на рівні драйверів відеокарт та модулів обробки графіки (наприклад, шляхом модифікації API DirectX/OpenGL/Vulkan чи використання rootkit-підходів у середовищі ОС). У таких випадках візуальні сигнали можуть змінюватися безпосередньо перед виведенням на екран, минаючи більшість традиційних механізмів контролю. Схожі підходи використовуються і в атаках типу supply chain — через змінені або скомпрометовані бібліотеки, програмні пакети чи оновлення ПЗ.

Ще одним вектором є маніпуляції на рівні конфігурації ОС або користувацьких налаштувань. Наприклад, зловмисник може змінити теми оформлення, кольорові профілі, контрастність, встановити фонові зображення або анімації з небезпечними NCDP-патернами. Навіть легальні інструменти персоналізації системи за певних умов можуть використовуватися для прихованого впливу.

На апаратному рівні вразливими є як безпосередньо пристрої відображення (монітори, екрани, VR/AR-гарнітури), так і їх мікропрограмне забезпечення (firmware). Модифікація мікропрограми монітора або драйвера GPU може дозволити впровадження NCDP-елементів на рівні, непідконтрольному операційній системі чи антивірусному ПЗ. Наприклад, атаки через оновлення firmware LED-панелей, маніпуляції з контролерами дисплеїв або підміна даних у каналі HDMI/DisplayPort.

Окремо варто згадати про використання апаратних проксі-пристроїв — мініатюрних модулів, що встановлюються між відеокартою та монітором й здатні змінювати зображення «на льоту». Такі пристрої важко ідентифікувати без спеціалізованого аудиту обладнання, а їхня дія може бути максимально непомітною для користувача. Новою загрозою також є зростаюча популярність XR/VR-гарнітур додає нові вектори ризику: тут апаратні засоби повністю контролюють простір перед очима користувача, і будь-які втручання на рівні firmware чи програмного забезпечення пристрою можуть призводити до потужного NCDP-ефекту через максимальну інтерактивність і близькість зображення до органів зору.

Важливим аспектом забезпечення захисту від NCDP є врахування логічного рівня безпеки, як це визначає І.О. Громико. Згідно з його підходом, інформація може вважатися захищеною лише тоді, коли у всіх ланках інформаційної взаємодії дотримується режимна адекватність і комунікабельність носіїв. На практиці це означає, що всі учасники та компоненти системи повинні мати лише той рівень доступу, який відповідає їхнім повноваженням, а взаємодія між ними має відбуватися із суворим дотриманням визначених стандартів обміну. У контексті протидії NCDP це передбачає не лише технічний контроль за каналами відображення, а й логічне структурування доступу до налаштувань візуального контенту, моніторинг змін конфігурацій і чітке розмежування прав для адміністраторів, операторів і кінцевих користувачів. Тільки за умови цілісного виконання цих принципів можна гарантувати, що інформація на екрані

залишатиметься незмінною і захищеною від прихованих впливів на всіх рівнях функціонування ІКС.

3.2. Способи виявлення модифікованого візуального контенту

Одним із перших кроків у перевірці автентичності зображень є аналіз метаданих, що зберігаються у файлах (EXIF, ICC-профілі, відомості про редагування тощо). Метадані можуть містити інформацію про дату й час створення, тип пристрою, параметри зйомки, а також історію збережень. У разі модифікації чи маніпуляцій зображення ці дані часто змінюються або втрачаються. Для виявлення підробки слід звертати увагу на відсутність або аномальність інформації, невідповідність дат, некоректні профілі кольору, підозрілі програми-редактори у ланцюгу обробки. Особливо це актуально для цифрових знімків, які використовуються у важливих інформаційних потоках — перевірка метаданих дозволяє вчасно виявити неавторизоване втручання.

Часто NCDP-атаки використовують приховані зорові стимули, що впроваджуються у вигляді неявних змін у піксельній структурі або у частотних компонентах зображення[28]. Для їх виявлення застосовуються методи стеганографічного аналізу: це пошук прихованих повідомлень чи змін, які важко помітити неозброєним оком. Зокрема, використовуються алгоритми розкладу зображення на спектральні складові (перетворення Фур’є, дискретне косинусне перетворення), що дозволяє ідентифікувати аномалії, повторювані сигнали, ритмічні чи хаотичні модуляції, які можуть бути характерними для NCDP-елементів.

Додатково до спектрального аналізу застосовується аналіз змін яскравості та кольорової палітри по кадрах (особливо у відео чи GIF-анімаціях). Навіть незначні, але часті мікрозміни можуть сигналізувати про наявність небезпечних патернів. Для автоматизації таких перевірок існують спеціалізовані програмні засоби, здатні аналізувати відеопотоки на наявність підозрілих частотних компонентів чи нетипових змін.

Важливим інструментом у боротьбі з модифікованим візуальним контентом є підтримка так званих еталонних баз даних зображень та автоматизований порівняльний аналіз. Для критичних систем (операторські щити, SCADA, монітори відображення інформації в ЦУС) доцільно зберігати контрольні копії допустимого візуального контенту. Нові або отримані ззовні зображення автоматично порівнюються з еталонними — навіть незначна відмінність може стати приводом для додаткової перевірки. Такий підхід дає змогу швидко виявити навіть мінімальні модифікації, особливо якщо їх метою є прихований вплив.

Ще одним дієвим методом є застосування цифрових підписів або контрольних хеш-сум. Кожен файл із зображенням підписується на етапі створення або затвердження, а будь-яка зміна (навіть у кількох пікселях) веде до невідповідності підпису чи хешу. У такому разі система або адміністратор отримують сигнал про можливу підробку чи компрометацію файлу.

У сучасних атаках особливу загрозу становлять не статичні, а динамічні зміни — стробоскопічні ефекти, мерехтіння, мікрозміни кольорів та яскравості, які людське око не завжди фіксує на свідомому рівні. Для їх виявлення використовуються спеціалізовані моніторингові програми, що фіксують усі зміни у відображенні екрану в реальному часі, аналізують послідовність кадрів та автоматично відзначають появу аномальних частот, особливо у чутливому для людини діапазоні (наприклад, 8–13 Гц). Такі інструменти дозволяють не лише виявити факт впровадження шкідливих патернів, але й попередити користувача або автоматично заблокувати відображення небезпечного контенту.

На практиці можна використовувати низку доступних інструментів, які дають змогу швидко перевіряти файли на предмет змін чи підозрілих ознак. Наприклад, системи типу FotoForensics дозволяють детально аналізувати зображення на наявність слідів редагування, зміни структури JPEG чи PNG-файлів, невідповідності у палітрі або відсутність певних даних у метаданих. Для корпоративних мереж існують модулі сканування, інтегровані у антивірусне ПЗ або системи захисту кінцевих точок, що проводять базову перевірку файлів до відображення.

3.3. Рекомендації для користувачів щодо захисту від NCDP

З огляду на те, що одним із ключових векторів реалізації атак нейроколородинамічного програмування (NCDP) є саме вплив на людину-оператора, питання підвищення цифрової обізнаності та дотримання правил безпеки на робочому місці набуває особливої актуальності. Основна мета рекомендацій для користувачів полягає у зниженні ймовірності впливу шкідливих візуальних патернів, а також у підвищенні готовності оперативно реагувати на потенційні загрози.

Передусім варто наголосити, що оператори повинні використовувати виключно перевірене та сертифіковане обладнання для відображення інформації, таке як монітори, VR/AR-гарнітури та інші пристрої. Підключення невідомих чи неавторизованих пристроїв, а також встановлення драйверів або оновлень програмного забезпечення з неперевірених джерел суттєво підвищує ризик появи в системі елементів, що можуть бути використані для реалізації NCDP-атак.

Окрему увагу слід звертати на зовнішній вигляд та поведінку інтерфейсу. Оператори повинні бути обізнані з типовим виглядом робочого середовища, налаштуваннями тем оформлення, палітрами кольорів і частотою оновлення екрана. У разі виникнення незвичних графічних ефектів — раптового мерехтіння, зміни кольорової гами, появи сторонніх анімацій або несподіваних візуальних сигналів — користувач має негайно повідомити відповідальні служби (IT-відділ або відділ інформаційної безпеки). Навіть незначні аномалії можуть свідчити про спробу прихованого впливу.

Крім того, оператори мають дотримуватися основ цифрової гігієни при роботі з файлами: не відкривати зображення, відео чи презентації з невідомих джерел, утримуватися від переходу за підозрілими посиланнями, а також не встановлювати сторонні програми для зміни оформлення системи (теми, скрінсейвери, анімації тощо), особливо якщо вони були завантажені з неофіційних або сумнівних ресурсів. Рекомендується використовувати лише ті теми оформлення, які затверджені адміністраторами, та не змінювати їх без дозволу.

Важливу роль у забезпеченні захисту від NCDP відіграє своєчасне оновлення операційної системи, драйверів, антивірусного програмного забезпечення та програм моніторингу візуального контенту. Адже сучасні захисні рішення не лише блокують класичні віруси, а й можуть фіксувати появу аномальних частотних патернів, що є характерними для NCDP-атак. Разом із цим рекомендується дотримуватися встановлених режимів яскравості та контрастності, уникати роботи з максимальними параметрами, якщо в цьому немає нагальної потреби, а також проводити періодичну візуальну перевірку робочого місця на предмет підключення сторонніх пристроїв.

Не менш важливим аспектом є контроль фізичного доступу до робочого місця. Оператори повинні запобігати підключенню сторонніх пристроїв (флешок, зовнішніх відеоадаптерів, невідомих моніторів), а також бути уважними до появи апаратних проксі або подібних пристроїв у ланцюгу передачі сигналу між ПК і монітором.

У разі виникнення будь-яких незвичних фізіологічних реакцій — наприклад, головного болю, запаморочення, зниження концентрації, різкого дискомфорту під час роботи — не слід ігнорувати подібні симптоми. Користувач повинен зробити перерву в роботі та повідомити про такі випадки відповідальних осіб, адже ці стани можуть бути наслідком впливу прихованих візуальних стимулів. Також рекомендовано звертатись до сертифікованих спеціалістів: нейропсихіатрів та психологів.

Окрім технічних заходів, важливою є регулярна участь у тренінгах з інформаційної безпеки, підвищення власної обізнаності щодо нових типів атак та механізмів впливу через візуальний канал. Дотримання корпоративних політик, виконання розпоряджень адміністраторів і регулярні консультації з фахівцями значно знижують ризики стати об’єктом NCDP-атаки.

3.4. Огляд технологій Cyber Deception для обману та фіксації атак

Технології Cyber Deception відіграють дедалі важливішу роль у системах інформаційної безпеки, особливо в умовах появи складних загроз, таких як

нейроколородинамічне програмування (NCDP). Відмінність цього підходу полягає у його проактивності: замість виключно пасивного захисту та блокування шкідливих дій він передбачає створення у мережі спеціальних об'єктів-приманок, які імітують справжні ресурси, однак не містять цінної інформації. Завдяки цьому зловмисник, взаємодіючи з такими об’єктами, фактично витрачає свої ресурси на безплідні дії, водночас розкриваючи власну тактику та технічні засоби.

Основою deception-технологій є впровадження honeypot- та honeynet-систем — ізольованих пристроїв або цілих мереж, які зовні нічим не відрізняються від справжніх робочих станцій, серверів чи операторських інтерфейсів[29]. У межах боротьби з NCDP це дає змогу реалізовувати декілька важливих стратегій. Так, можна створювати віртуальні операторські панелі, здатні динамічно відображати різні візуальні стимули, ймітуючи вразливі для атак середовища. Зловмисник, який намагається змінити колірну палітру інтерфейсу, інтегрувати мерехтливі елементи або маніпулювати візуальним контентом, насправді взаємодіє лише з контрольованою пасткою, а не з реальними даними чи користувачами. Окрім цього, у honeynet-середовищах доцільно розміщувати спеціально підготовлені зразки зображень і відео з вбудованими маркерами. Будь-яка спроба їх модифікувати або використати для атак фіксується й аналізується, що дозволяє не лише ідентифікувати факт вторгнення, а й оцінити реакцію зловмисника на різні типи візуальних ефектів.

Сучасні deception-платформи дедалі частіше мають функції динамічного налаштування: вони здатні автоматично змінювати властивості приманок залежно від поведінки атакуючого. Наприклад, інтерфейс може підлаштовуватись під очікування зловмисника, змінювати структуру меню, додавати фіктивні налаштування чи фальшиві дані, стимулюючи його до подальших дій. Такі механізми не лише ускладнюють аналіз середовища для злочинця, але й розширюють можливості для збору інформації про його наміри, використовувані інструменти та рівень кваліфікації.

Окрім повноцінних honeypot- або honeynet-систем, deception-технології активно впроваджуються через розповсюдження фіктивних файлів, записів або

посилань, так званих decoy data чи honeytoken, у критичних сегментах корпоративної мережі. Наприклад, спеціально підготовлене зображення, яке не використовується у справжньому робочому процесі, але доступне для зловмисника, може слугувати індикатором несанкціонованого доступу або спроби маніпуляції з візуальним контентом. Виявлення активності навколо таких об’єктів дозволяє оперативно реагувати на інцидент, часто — ще до того, як буде завдано реальної шкоди інформаційній системі.

Важливою перевагою впровадження deception-технологій є можливість детального фіксування усіх дій атакуючого в ізольованому, контрольованому середовищі. Кожна спроба доступу, зміни налаштувань, маніпуляції з контентом або взаємодії з інтерфейсом фіксується у відповідних логах. Надалі ці дані дозволяють аналітикам безпеки не лише підтвердити сам факт атаки, а й глибше зрозуміти методи роботи зловмисника, своєчасно адаптувати політики захисту, розробити нові сценарії реагування та підвищити загальний рівень обізнаності персоналу.

Тенденції розвитку deception-систем свідчать про їхню інтеграцію з іншими рішеннями з кібербезпеки, зокрема із системами моніторингу подій (SIEM), автоматизованими платформами реагування на інциденти, а також хмарними рішеннями. Це дозволяє організувати багаторівневий захист, що здатний виявляти навіть найскладніші й нетипові загрози, як-то атаки через візуальний канал або вплив на підсвідомість користувачів.

У підсумку, впровадження технологій Cyber Deception в інформаційно-комунікаційних системах, особливо у поєднанні з іншими засобами захисту, дає змогу суттєво підвищити рівень стійкості до сучасних атак, оперативно ідентифікувати нові вектори загроз і постійно вдосконалювати захисні стратегії, ґрунтуючись на реальних сценаріях взаємодії зі зловмисниками.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ HONEYNET ДЛЯ ПРОТИДІЇ NCDP

4.1. Архітектура Honeypot/Honeynet систем

У сучасній кібербезпеці honeypot- і honeynet-технології є ключовими інструментами для виявлення, аналізу й попередження новітніх типів атак, зокрема й таких, що націлені на підсвідоме чи когнітивне маніпулювання оператором (NCDP). Від класичних систем захисту ці рішення відрізняються проактивністю: honeypot створює середовище-пастку, яке спеціально спроєктоване для залучення потенційних атакуючих, дозволяючи фіксувати їхню поведінку, аналізувати використовувані інструменти та методи обходу захисту.

Honeypot — це ізольований вузол або програмно-апаратний комплекс, який імітує уразливі сервіси або інтерфейси, що приваблюють зловмисника. На відміну від звичайних робочих станцій, honeypot не містить реальної цінної інформації, але ретельно моделює поведінку легітимної системи. При взаємодії атакуючого з honeypot-ом всі його дії фіксуються та можуть бути проаналізовані логуванням[29].

Honeynet — це розширена архітектура, яка включає цілу мережу взаємопов’язаних honeypot-ів, часто із додатковими системами моніторингу, аналізу трафіку та журналювання подій. Honeynet дозволяє моделювати складніші сценарії атак, у тому числі ланцюгові чи багаторівневі (наприклад, lateral movement усередині корпоративної мережі), а також тестувати реакцію системи на різні типи впливів — від класичних мережевих атак до експериментів із модифікованим візуальним контентом.

Ключовими перевагами використання honeypot/honeynet систем є:

- Ізольованість і безпечність: експериментальні атаки не впливають на реальні дані та користувачів, адже середовище повністю ізольоване.
- Гнучкість моделювання: можна емулювати різні типи служб, протоколів, інтерфейсів, у тому числі специфічні панелі операторів або SCADA-компоненти, що критично важливо для аналізу впливу NCDP-атак.

- Фіксація та збереження логів: усі дії зловмисника, включаючи мережеві запити, зміни інтерфейсу, спроби ін’єкцій, а також змінений візуальний контент детально протоколюються для подальшого аналізу.

З технічного погляду honeypot/honeynet-системи можуть бути реалізовані на базі віртуальних машин, контейнерних технологій (Docker, LXC), або ж спеціалізованих апаратних платформ із апаратною ізоляцією. Це дає змогу відтворити не лише мережеву, а й візуальну частину інфраструктури — наприклад, розгорнути операторську панель, яка буде реагувати на зовнішній вплив, фіксуючи спроби зміни кольорів, динамічні анімації або впровадження NCDP-патернів.

В рамках дослідження протидії NCDP-атакам архітектура honeynet була побудована на основі віртуалізованого середовища (VMware Workstation), в якому розгорнута віртуальна машина з ОС Ubuntu. На цьому сервері був запущений власний веб-сервер, що моделює “операторську панель” із можливістю генерувати динамічний візуальний контент (зокрема, мерехтливі кольорові блоки, характерні для NCDP-атак). Доступ до цього середовища здійснювався з клієнтського пристрою (Windows з браузером Chrome), що дозволяло імітувати реальний сценарій “атаки через візуальний канал”.

Завдяки цій архітектурі стало можливим:

- моделювати вплив шкідливого візуального контенту в ізольованому середовищі,
- фіксувати всі події (логи серверу, події у браузері, мережевий трафік через Wireshark),
- тестувати ефективність захисних скриптів та інструментів Cyber Deception,
- проводити подальший аналіз результатів за допомогою скріншотів, логів і власних утиліт.

4.2. Побудова середовища для тестування впливу NCDP

Для проведення практичних досліджень щодо протидії NCDP-атакам було створено спеціалізоване лабораторне середовище, яке забезпечує ізольованість, контрольованість експерименту та можливість повного моніторингу всіх етапів

атаки й реакції системи. Таке середовище дає змогу відтворювати реальні сценарії взаємодії оператора з потенційно шкідливим візуальним контентом, а також тестувати ефективність запропонованих захисних рішень.

В основі тестового комплексу була використана віртуалізована інфраструктура, розгорнута за допомогою платформи VMware Workstation. На створеній віртуальній машині із встановленою операційною системою Ubuntu 22.04 LTS було налаштовано мережевий інтерфейс для забезпечення доступу з фізичного клієнтського комп'ютера, який імітує робочу станцію оператора. У межах віртуальної машини було розгорнуто Flask-сервер, що доступний за локальною адресою 127.0.0.1:8080 та мережею 192.168.217.129:8080. (див рисунок 4.1), що виконує роль honeypot-платформи та відтворює "операторську панель" із інтерактивним елементом – кольоровим блоком, призначеним для моделювання впливу NCDP-атаки шляхом періодичної зміни кольору з частотою близько 10 Гц (див. рис. 4.2). Завдяки цьому вдалося імітувати той тип візуального впливу, що є характерним для NCDP-атак і потенційно здатний викликати небажані когнітивні реакції у користувача. З боку клієнта використовувався комп'ютер під управлінням операційної системи Windows із встановленим браузером Google Chrome, що дозволяло у повній мірі відтворити поведінку реального оператора, який отримує доступ до операторської панелі через веб-інтерфейс. Важливим елементом експерименту стало застосування засобів моніторингу та аналізу мережевого трафіку. Для цієї мети на хост-машині був інстальований Wireshark, який забезпечив детальну фіксацію усіх мережевих взаємодій між клієнтом і сервером. Крім того, серверний скрипт було доопрацьовано таким чином, щоб кожна зміна кольору у веб-інтерфейсі супроводжувалася логуванням відповідної події із зазначенням часу та IP-адреси клієнта.

Таким чином, побудоване середовище дало змогу повністю відтворити ланцюжок NCDP-атаки: від генерації шкідливого візуального контенту на сервері — до фіксації впливу на клієнта та збору всіх необхідних даних для подальшого аналізу. Додатковою перевагою такої архітектури є її масштабованість і можливість інтеграції додаткових інструментів, таких як скрипти автоматичного

виявлення аномального мерехтіння чи впровадження засобів cyber deception для протидії складнішим атакам. Отримані у цьому середовищі результати дозволяють обґрунтовано оцінити ефективність різних підходів до захисту від NCDP-атак у сучасних інформаційних системах.

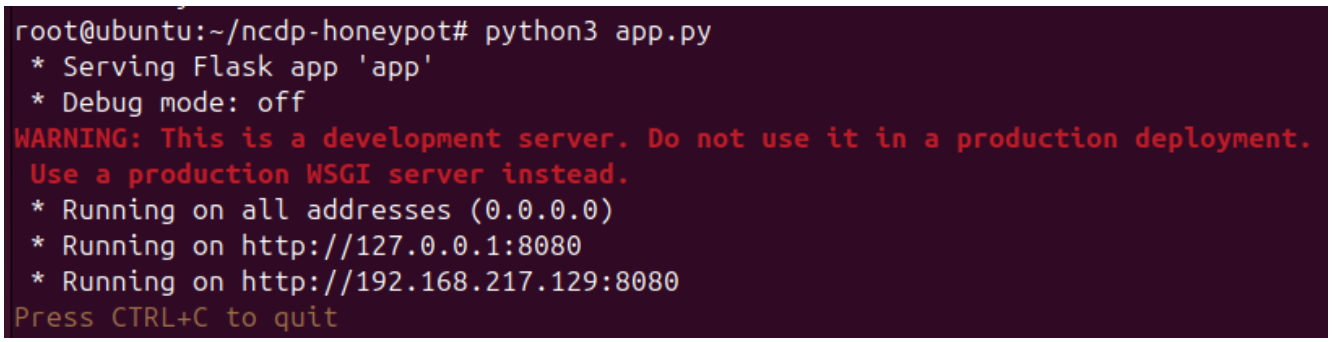

Рисунок 4.1 – Запуск сервера honeypot-сервера у Flask на Ubuntu.

Рисунок 4.2 – Візуалізація операторської панелі в тестовому середовищі

4.3. Використання інструментів Cyber Deception у захисті

Застосування інструментів cyber deception є однією з найперспективніших концепцій сучасної інформаційної безпеки, особливо у контексті захисту від маловідомих або новітніх типів атак, таких як NCDP-атаки через візуальні канали. На відміну від класичних методів захисту, що зосереджені переважно на

ідентифікації та блокуванні вже відомих векторів загроз, підходи cyber deception базуються на створенні контрольованих пасток (honeypot) та імітаційних середовищ (honeynet), які дозволяють не лише зафіксувати факт атаки, але й отримати цінну аналітичну інформацію про поведінку зловмисника, його інструменти та тактики[30].

У рамках даного дослідження інструменти cyber deception були інтегровані до тестового середовища у вигляді спеціально створеного honeypot-сервера, що емулює роботу операторської панелі із можливістю генерувати аномальний візуальний контент. Такий підхід дозволив спровокувати взаємодію потенційного атакуючого із системою та зафіксувати його дії у контрольованих умовах, не наражаючи на небезпеку реальні інформаційні ресурси. Важливою особливістю цієї реалізації стало поєднання класичних мережевих технологій обману із новітніми підходами до виявлення атак через візуальні стимули, що лише починають досліджуватись у сучасній науці.

У практичній частині експерименту honeypot-система виконувала одразу дві функції. По-перше, вона виступала “приманкою”, яка дозволяла імітувати реальну роботу критичного елементу інформаційної системи та відслідковувати спроби несанкціонованого впливу на візуальний контент. По-друге, у ній було реалізовано механізми детального логування усіх дій з боку клієнта: зміна кольорів, частота звернень, а також спроби модифікації скриптів або взаємодії із панеллю. Це дало змогу акумулювати масив даних для подальшого аналізу та побудови профілю потенційного зловмисника або типового сценарію атаки.

Інтеграція елементів cyber deception у процес моделювання NCDP-атак дозволила також апробувати засоби превентивного виявлення загроз. Зокрема, було випробувано використання клієнтських скриптів (на базі Tampermonkey) для моніторингу аномального мерехтіння, що може свідчити про спробу прихованого впливу на оператора. У випадку виявлення небезпечної частоти зміни кольору елемента система автоматично блокувала сторінку або повідомляла користувача про потенційну загрозу. Таким чином, було впроваджено багаторівневий підхід до

захисту, який поєднує в собі можливості класичного honeypot та сучасних засобів deception із активною клієнтською протидією.

4.4. Аналіз логів для виявлення візуальних аномалій

Виявлення та аналіз візуальних аномалій, які можуть бути пов’язані з NCDP-атаками, базуються на ретельному вивченні подій, зафіксованих у логах серверної частини honeypot-системи, а також у мережевих логах, отриманих за допомогою спеціалізованих засобів моніторингу трафіку[31]. У межах практичного експерименту кожна зміна кольору елемента операторської панелі супроводжувалася створенням відповідного запису у серверному журналі подій. Лог-файл містить інформацію про час події, IP-адресу клієнта, а також про новий колір елемента, що дозволяє відтворити точну хронологію дій під час імітації атаки.

Додатково для аналізу використовувалися дані, отримані за допомогою Wireshark (див рис 4.3). Цей інструмент дозволив детально зафіксувати мережеві взаємодії між клієнтською та серверною частинами, зокрема HTTP-запити, які надходили на сервер під час кожної зміни кольору в браузері користувача. Аналіз зібраних даних дозволяє не лише визначити факт виникнення аномальної активності, а й оцінити параметри потенційної NCDP-атаки, такі як частота зміни кольорів, тривалість впливу, та типові патерни поведінки клієнта.

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Lengtl	Info
454	40.078618	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
466	40.184814	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
485	40.281407	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
497	40.384776	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
509	40.477096	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
536	40.589290	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
548	40.692793	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
558	40.785708	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
578	40.883149	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
599	40.992344	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
628	41.086061	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
638	41.188634	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
648	41.281385	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
658	41.388975	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
672	41.482561	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
682	41.590399	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
696	41.684759	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
706	41.777559	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
716	41.885626	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
726	41.977872	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
740	42.084950	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
750	42.180572	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
760	42.289046	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
772	42.381976	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)
784	42.489425	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
794	42.587256	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
804	42.677480	192.168.217.1	192.168.217.128	HTTP/J…	542	POST /log_event HTTP/1.1 , JSON (application/json)
814	42.785185	192.168.217.1	192.168.217.128	HTTP/J…	544	POST /log_event HTTP/1.1 , JSON (application/json)

Рисунок 4.3 – Відсортовані логи за HTTP запитом.

У ході експерименту було отримано серію скріншотів та фрагментів лог-файлів, що ілюструють процес фіксації аномальних змін у реальному часі. На прикладі логу подій чітко простежується, що під час запуску скрипта для імітації NCDP-атаки зміна кольору елемента відбувалася з високою частотою, що є характерною ознакою такого типу впливу (див. рис. 4.4). Аналіз записів дозволяє встановити, чи відповідає частота зміни кольору пороговим значенням, визнаним небезпечними для користувача, а також ідентифікувати потенційно шкідливу поведінку ще на ранніх етапах атаки.

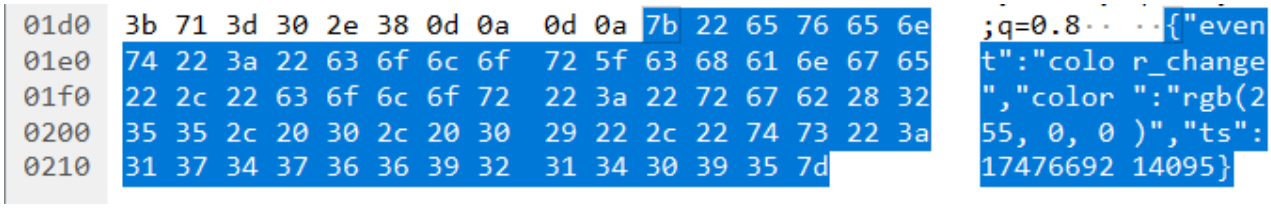

Рисунок 4.4 – виділений лог атаки з мерегтінням кольору.

4.5. Створення захисту від NCDP-атак

Результати практичного моделювання NCDP-атак засвідчили необхідність розробки та впровадження спеціалізованих заходів захисту, спрямованих на мінімізацію ризиків негативного впливу шкідливого візуального контенту на операторів інформаційних систем. Оскільки класичні антивірусні чи мережеві засоби захисту здебільшого не здатні своєчасно ідентифікувати аномальні патерни, що проявляються у вигляді високочастотного мерехтіння чи змін кольору, виникає потреба у впровадженні додаткових механізмів моніторингу та протидії.

Одним із найбільш ефективних практичних інструментів, апробованих у рамках цього дослідження, став користувацький скрипт на базі Tampermonkey для браузера Google Chrome. Даний скрипт постійно відслідковує частоту зміни кольору визначених елементів веб-інтерфейсу операторської панелі. Якщо фіксується частота, що перевищує заданий безпечний поріг (наприклад, 8 Гц), система автоматично сповіщає користувача про небезпеку або блокує доступ до сторінки, запобігаючи можливому шкідливому впливу на оператора. (див. рис. 4.5)

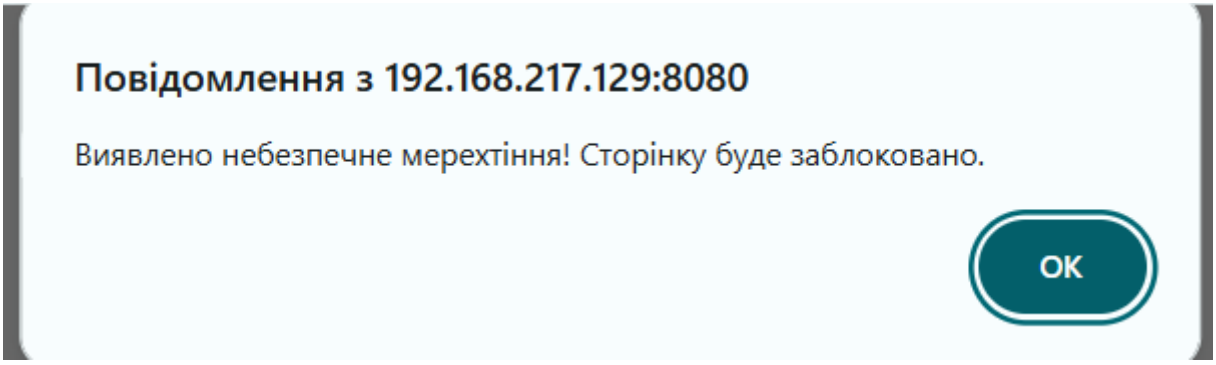

Рисунок 4.5 – повідомлення оператору про небезпечність сторінки

Такий підхід дозволяє реалізувати превентивний захист навіть у тому випадку, коли шкідливий скрипт вже отримав можливість змінювати візуальні елементи в браузері. Крім того, важливою складовою захисту є ізоляція підозрілих файлів та обмеження можливостей для виконання сторонніх скриптів у середовищі оператора. У корпоративній практиці це може реалізовуватися шляхом впровадження політик "білого списку" для дозволених скриптів та застосування розширень браузера, які блокують виконання стороннього коду. Додатково доцільним є використання sandbox- або віртуалізованих середовищ для первинного аналізу нового чи невідомого візуального контенту перед тим, як надати до нього доступ реальному користувачу. Ще одним напрямком підвищення стійкості системи є автоматизований аналіз журналів подій та мережевого трафіку із застосуванням спеціалізованих інструментів, що дозволяють виявляти характерні ознаки NCDP-атак — зокрема, нетипову частоту зміни кольору, підозрілі патерни звернень до серверу чи спроби ін’єкції скриптів. Такі підходи можуть бути реалізовані на базі систем класу SIEM, які автоматично генерують сповіщення для адміністратора при виявленні потенційно шкідливої активності.

Комплексне впровадження описаних заходів дозволяє значно знизити ймовірність успішної реалізації NCDP-атак і забезпечує більш високий рівень безпеки оператора інформаційної системи навіть у разі використання нових, малодосліджених векторів впливу.

4.6. Аналіз ефективності впровадження рішень

Ефективність розроблених та впроваджених заходів щодо протидії NCDP-атакам була проаналізована на основі експериментальних даних, отриманих у рамках побудованого лабораторного середовища. На першому етапі дослідження, до застосування захисних рішень, було зафіксовано, що скрипт, який генерує високоінтенсивне мерехтіння кольору елемента операторської панелі, не викликав жодної реакції з боку системи безпеки, а відповідні події лише логувалися у вигляді записів про зміну кольору та мережевих звернень. Це дозволяло NCDP-атакуючому потенційно здійснювати негативний когнітивний вплив на оператора протягом необмеженого часу.

Після впровадження спеціалізованого Tampermonkey-скрипта для автоматичного моніторингу частоти зміни кольору була істотно підвищена стійкість системи до такого роду атак. Експерименти показали, що у випадку виявлення частоти зміни кольору, яка перевищує встановлений безпечний поріг (наприклад, 8 Гц), скрипт миттєво блокував сторінку або виводив відповідне попередження користувачеві. Внаслідок цього час дії потенційно шкідливого контенту на оператора зводився до мінімуму, а сам користувач отримував можливість оперативно припинити роботу з небезпечним ресурсом.

Порівняльний аналіз логів до і після впровадження захисного механізму засвідчив повну відсутність довготривалих серій аномальних змін кольору після активації скрипта. В усіх випадках спроб NCDP-атаки система реагувала відповідно до налаштованого сценарію: сторінка автоматично закривалася або блокувалася для запобігання негативному впливу. Жодного хибного спрацьовування (false positive) під час тестування виявлено не було, що свідчить про достатню точність обраного підходу в умовах лабораторного середовища.

Таким чином, результати проведених експериментів підтверджують ефективність впроваджених заходів із протидії NCDP-атакам у межах розгорнутої тестової інфраструктури. Практичне застосування механізмів моніторингу візуальних аномалій на клієнтському рівні дозволяє значно підвищити рівень інформаційної безпеки операторських систем та забезпечує можливість

своєчасного реагування на появу новітніх загроз, пов’язаних із когнітивним впливом через візуальні канали. Таким чином, можна підсумувати систему захисту (див. табл. 4.1)

Таблиця 4.1 - Порівняльний аналіз ефективності системи до і після впровадження захисного механізму

Критерій	До впровадження захисту	Після впровадження Tampermonkey-скрипта
Виявлення частого мерехтіння кольору	Відсутнє	Автоматичне, з фіксацією частоти зміни
Реакція системи на NCDP-атаку	Відсутня	Миттєве блокування сторінки і попередження
Тривалість впливу шкідливого контенту	Необмежена	Мінімальна (до 1–2 секунд до спрацювання)
Кількість зафіксованих шкідливих сесій	Необмежена	0 (усі атаки були негайно заблоковані)
False positive спрацювання	Не визначено	Не зафіксовано під час експерименту
False negative спрацювання	Можливі, не фіксувалися	Не зафіксовано під час експерименту
Зручність для користувача	Не гарантується	Захист без відчутних незручностей

ВИСНОВКИ

У ході виконання дипломної роботи було здійснено комплексне міждисциплінарне дослідження проблематики нейроколородинамічного програмування (NCDP) у контексті інформаційної безпеки сучасних інформаційно-комунікаційних систем. Основні результати, висновки та наукова новизна проведеної роботи підсумовано нижче.

На основі огляду сучасних наукових джерел та міждисциплінарних праць було доведено, що NCDP являє собою якісно новий вектор атак на інформаційні системи, в основі якого лежить цілеспрямований вплив на нервову систему оператора через динамічні кольорові патерни, що відображаються на екрані. Відмінною особливістю цього підходу є використання сенсорних (візуальних) каналів замість традиційних вербальних або аудіальних, як це реалізується у класичному нейролінгвістичному програмуванні (NLP). Доведено, що NCDP-атаки можуть не лише призводити до фізіологічних реакцій (головний біль, дезорієнтація, фотострес, напади у людей з фоточутливою епілепсією), а й спричиняти глибші когнітивні ефекти — формування підсвідомих установок, модифікацію поведінки, помилки у прийнятті рішень оператором критичних систем.

Вперше в українській науковій практиці детально проаналізовано нейрофізіологічні механізми сприйняття кольору, ритмічної стимуляції які стають основою ефективності NCDP-атак. Встановлено, що використання високочастотного мерехтіння (у діапазоні альфа-ритмів мозку) є найбільш небезпечним з точки зору когнітивного впливу, а також що більшість сучасних інтерфейсів не містить механізмів виявлення та блокування подібних атак.

У роботі систематизовано основні вектори ін’єкції небезпечних кольорових стимулів у цифрових середовищах, серед яких:

- модифікації візуального контенту на рівні веб-інтерфейсів, SCADA-систем, відеопотоків;
- атаки через зміни драйверів GPU та firmware LED-дисплеїв;

- фізичне впровадження апаратних проксі-пристроїв між відеокартою і монітором;
- використання мобільних пристроїв, XR/VR-гарнітур як нових площин впливу.

Проведено детальний аналіз організаційних та програмно-апаратних уразливостей, які полегшують впровадження NCDP-атак, зокрема брак політик перевірки візуального контенту, відсутність моніторингу динамічних змін кольору в інтерфейсах, а також низьку цифрову гігієну операторів.

У рамках практичної частини дослідження було спроєктовано та впроваджено ізольоване тестове середовище на базі honeynet-архітектури із застосуванням віртуалізованої інфраструктури, honeypot-сервера (на Flask, Ubuntu) та системи моніторингу мережевого трафіку (Wireshark). Розроблено скрипт для моделювання NCDP-атаки шляхом генерації високочастотного мерехтіння кольорових елементів у веб-інтерфейсі, що дозволило відтворити реальні умови впливу на оператора.

Проведено детальний аналіз серверних логів і мережевих журналів, що дало змогу виявити характерні патерни поведінки під час атаки — зокрема, аномально високу частоту зміни кольору, яка автоматично фіксувалася honeypot-системою. Зібрані дані лягли в основу побудови алгоритмів виявлення і блокування NCDP-атак.

Одним із ключових досягнень роботи стала розробка й апробація клієнтського захисного механізму на базі Tampermonkey-скрипта для браузера Google Chrome, який здійснює постійний моніторинг частоти зміни кольору у веб-інтерфейсі. У разі виявлення частоти, що перевищує безпечний поріг, система автоматично блокує сторінку або сповіщає користувача про загрозу. Практичне тестування показало високу ефективність такого підходу — усі спроби ініціювати NCDP-атаку були миттєво зупинені, а тривалість впливу шкідливого контенту скоротилася до мінімуму.

Комплексна реалізація засобів deception (honeypot, honeynet, логування, аналіз трафіку), а також автоматизованих клієнтських рішень продемонструвала

можливість створення багаторівневої системи протидії NCDP-атакам навіть у складних інформаційних середовищах.

Отримані результати підтверджують доцільність та ефективність впровадження клієнтських і серверних засобів моніторингу візуальних аномалій, ізоляції підозрілих компонентів і використання deception-архітектур для підвищення рівня інформаційної безпеки. Сформульовано рекомендації щодо впровадження політик перевірки візуального контенту, регулярного оновлення програмного забезпечення, а також організаційних заходів з підвищення цифрової грамотності операторів.

Запропонована в роботі методика може бути масштабована для використання у промислових ІКС, центрах моніторингу, диспетчерських системах, а також у системах, що використовують VR/AR-технології.

Уперше проведено повний цикл дослідження — від нейрофізіологічного підґрунтя до реалізації реального тестового середовища і розробки дієвого захисного інструментарію. Доведено, що:

- NCDP-атаки становлять реальну загрозу для ІКС, а класичні засоби захисту не забезпечують належного рівня безпеки;
- honeynet-архітектури можуть бути ефективно використані для виявлення, моделювання і аналізу новітніх атак через візуальний канал;
- клієнтські скрипти Tampermonkey можуть забезпечити превентивний захист операторів у реальному часі;
- системна інтеграція таких підходів дозволяє створити ефективний бар’єр для NCDP-атаки на різних рівнях ІКС.

Мета дослідження була досягнута повністю: від глибокого теоретичного аналізу до практичної розробки, тестування та оцінки ефективності захисних заходів у реальному лабораторному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary [Електронний ресурс]. Geneva: ISO, 2018. Режим доступу: https://www.iso.org/standard/73906.html (дата звернення: 20.01.2025).

2. NIST Special Publication 800-12 Rev.1: An Introduction to Information Security [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, June 2017. (дата звернення: 23.01.2025).

3. ENISA Threat Landscape 2023 [Електронний ресурс]. European Union Agency for Cybersecurity, Oct 2023. (дата звернення: 25.01.2025).

4. Kerimov K., Azizova Z. Methodology of information security risk assessment of electronic resources under unauthorized access threats [Електронний ресурс] // Proc. of 15th Int. Sci.–Pract. Conf. “Environment. Technology. Resources”, Rezekne (Latvia), 2024, vol. 2, pp. 175–182. DOI: 10.17770/etr2024vol2.8043 (дата звернення: 03.02.2025).

5. Aslan Ö., Aktuğ S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions [Електронний ресурс] // Electronics, 2023, 12(6): 1333. DOI: 10.3390/electronics12 (дата звернення: 28.01.2025).

6. Дудкевич В.Б., Хорошко В.О., Яремчук Ю.Є. Основи інформаційної безпеки: навч. посіб. [Електронний ресурс]. – Вінниця: ВНТУ, 2018. – 316 с. Режим доступу: http://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf (дата звернення: 06.02.2025).

7. Аль-Амморі А. Н., Дехтяр М. М., Іщенко Р. М., Клочан А. Є. Методи та засоби захисту інформації [Електронний ресурс] // Системи управління, навігації та зв’язку. – 2024. – № 1. – С. 38 (PDF-версія). DOI: 10.26906/SUNZ.2024.1.038 (дата звернення: 04.04.2025).

8. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 31.01.2025).

9. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]. – Київ: ДСТСЗІ СБ України, 2005 (зі змінами 2012). Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 09.02.2025).

10. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls [Електронний ресурс]. Geneva: ISO, 2022. Режим доступу: https://www.iso.org/standard/75652.html (дата звернення: 12.02.2025).

11. Guri M., Bykhovsky D., Elovici Y. BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness // Proc. of 12th CMI Conf. on Cybersecurity and Privacy. – 2019. – DOI: 10.1109/CMI48017.2019.8962137. (дата звернення: 21.03.2025).

12. Whitman M.E., Mattord H.J. Principles of Information Security. 6th ed. [Електронний ресурс]. – Boston: Cengage Learning, 2018. – 672 p. Режим доступу: https://unidel.edu.ng/focelibrary/books/Principles%20of%20Information%20Security%20by%20Whitman,%20Michael%20Mattord,%20Herbert%20(z-lib.org).pdf (дата звернення: 21.02.2025).

13. NIST Special Publication 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations [Електронний ресурс]. Gaithersburg, MD: NIST, Sept 2020. (дата звернення: 18.02.2025).

14. Громико І.О. Головний закон захисту інформації. Комунікабельність носіїв інформації // Theoretical and empirical scientific research: concept and trends: матеріали VII Міжнародної науково-практичної конференції (Оксфорд, 16 серпня 2024 р.), секція "Information Technologies and Systems". – Оксфорд, Велика Британія: Logos Science, 2024. – С. 177–187. – DOI: 10.36074/logos-16.08.2024.037. – Режим доступу: https://archive.logos-science.com/index.php/conference-proceedings/article/view/2190 (дата звернення: 15.02.2025).

15. Денисюк Д., Сорочинський О., Гнатчук Є., Дрозд А. Інформаційна технологія виявлення зловмисних кодів в інформаційних системах на основі аналізу

паралельних процесів // Вісник Хмельницького нац. ун-ту. Серія: Технічні науки. – 2025. – Т. 347, № 1. – С. 80–88. (дата звернення: 24.03.2025).

16. Elliot A.J., Maier M.A. Color Psychology: Effects of Perceiving Color on Psychological Functioning in Humans [Електронний ресурс] // Annual Review of Psychology, 2014, 65, с. 95–120. DOI: 10.1146/annurev-psych-010213-115035 (дата звернення: 24.02.2025).

17. Hsu L., Chen Y. Neuromarketing, subliminal advertising, and hotel selection: An EEG study [Електронний ресурс] // Australasian Marketing Journal, 2020, 28(4), с. 200–208. DOI: 10.1016/j.ausmj.2020.04.009 (дата звернення: 08.03.2025).

18. Koch C., Tsuchiya N. Attention and consciousness: two distinct brain processes [Електронний ресурс] // Trends in Cognitive Sciences, 2007, 11(1), с. 16–22. DOI: 10.1016/j.tics.2006.10.012 (дата звернення: 05.03.2025).

19. Tamietto, M., & de Gelder, B. Neural bases of the non-conscious perception of emotional signals // Nature Reviews Neuroscience. – 2010. – Vol. 11, No. 10. – P. 697–709. – DOI: 10.1038/nrn2889. – Режим доступу: https://www.nature.com/articles/nrn2889 (дата звернення: 07.04.2025).

20.Farid H. Digital image forensics [Електронний ресурс] // Scientific American, 2008, 298(6): 66–71. DOI: 10.1038/scientificamerican0608-66 (дата звернення: 17.04.2025).

21. Mankowska N.D., Grzywińska M., Winklewski P.J., Marcinkowska A.B. Neuropsychological and Neurophysiological Mechanisms behind Flickering Light Stimulus Processing [Електронний ресурс] // Biology, 2022, 11(12): 1720. DOI: 10.3390/biology11121720 (дата звернення: 27.02.2025).

22. Kan M. This PC monitor hack can manipulate pixels for malicious effect [Електронний ресурс] // PCWorld, 6 серпня 2016 р. Режим доступу: https://www.pcworld.com/article/415964/this-pc-monitor-hack-can-manipulate-pixels-for-malicious-effect.html (дата звернення: 12.03.2025).

23. AppOmni. Вектор атаки (Attack Vector) [Електронний ресурс] // AppOmni SaaS Glossary. – Режим доступу: https://appomni.com/saas-glossary/attack-vector/ (дата звернення: 10.04.2025).

24. SoftwareG. 7 рівнів мережевої безпеки [Електронний ресурс] // SoftwareG. – Режим доступу У: https://softwareg.com.au/en-it/blogs/internet-security/7-layers-of-network-security (дата звернення: 14.04.2025).

25. Gajanan M. Epilepsy Foundation Presses Charges After Hackers Sent Seizure-Inducing Images to Its Twitter Followers [Електронний ресурс] // Time, 18 грудня 2019 р. Режим доступу: https://time.com/5752038/epilepsy-foundation-cyberattack-cause-seizures/ (дата звернення: 15.03.2025).

26. Костючков С. К. Нейрокогнітивний хакінг як елемент «дестабілізаційної змії» у контексті сучасної гібридної війни // Вісник Львівського університету. Серія філософсько-політологічні студії, 2020, вип. 30, с. 161–169. (дата звернення: 02.03.2025).

27. Громико І.О. NCDP – Neurocolordynamic Programming / І.О. Громико // Внутрішнє видання кафедри кібербезпеки інформаційних систем, мереж та технологій ННІ КН та ШІ Каразінського університету. – Харків, 2024. (дата звернення: 18.03.2025).

28. Morić Z., Dakić V., Regvart D. Advancing Cybersecurity with Honeypots and Deception Strategies // Informatics. – 2025. – Vol. 12, No. 1. – Art. no. 14. (дата звернення: 31.03.2025).

29. Imperva. What is a Honeypot [Електронний ресурс] // Imperva Learning Center. – Режим доступу: https://www.imperva.com/learn/application-security/honeypot-honeynet/ (дата звернення: 21.04.2025).

30. Honeynet vs Honeypots [Електронний ресурс] // Lupovis. – Режим доступу: https://www.lupovis.io/honeynets_vs_honeypots/ (дата звернення: 10.05.2025).

31. Микитин Г. В., Руда Х. С. Концептуальний підхід до виявлення deepfake-модифікацій біометричного зображення засобами нейронних мереж // Комп’ютерні системи та мережі. – 2024. – Т. 6, № 1. – С. 124–134. (дата звернення: 27.03.2025).