МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **КІБЕРБЕЗПЕКА АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ**

Студентка групи СЗД-41 Ізюменко Анастасія Ярославівна _____
(підпис)

Науковий керівник: к.т.н., доц Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студентці: Ізюменко Анастасії Ярославівні

1.Тема роботи: Кібербезпека автоматизованої системи управління, затверджено наказом від « 24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси кіберзахисту автоматизованих систем управління.

4. Предметом дослідження: технології захисту автоматизованих систем управління.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій кіберзахисту автоматизованих систем управління;
- аналіз та дослідження існуючих методів кіберзахисту автоматизованих систем управління;
- створення рекомендацій щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняв до виконання _____Ізюменко А.Я.

(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «____» _____2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студентка: СЗД -41 Ізюменко А.Я. _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Г.В. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 50 сторінок, 3 рисунки, 6 таблиць.

В кваліфікаційній роботі розглядаються проблеми створення спеціальної системи виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси автоматизованих систем управління. Надано аналіз світової правової практики в частині захисту від інформаційних загроз та аналіз вирішення цього питання на підприємствах різної форми власності. Наведено основні етапи реалізації атак на автоматизовані системи та структуру системи їх виявлення та нейтралізації. Обґрунтовано необхідність створення ефективної системи протидії кібератакам, зазначено складнощі на шляху її створення, зокрема, надано аналіз стану та перспектив розвитку вітчизняної електронної галузі. На основі проведеного аналізу запропоновано та обґрунтовано варіанти розв'язання цього завдання, сформульовано основні висновки та рекомендації для її вирішення. Для вирішення поставлених у кваліфікаційній роботі завдань застосовується метод теоретичного аналізу вихідних даних у різних сегментах питань, що розглядається, метод узагальнення отриманих результатів і вироблення необхідних шляхів вирішення. Актуальність розглянутої проблематики пов'язана з постійним загостренням протистояння світових держав в інформаційному просторі та відкритим нав`язуванням низки країн в участь у інформаційній війні.

Об’єктом дослідження: процеси кіберзахисту автоматизованих систем управління.

Предметом дослідження є технології захисту автоматизованих систем управління.

Мета роботи удосконалення та рекомендації щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій кіберзахисту автоматизованих систем управління;
- аналіз та дослідження існуючих методів кіберзахисту автоматизованих систем управління;
- створення рекомендацій щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

ABSTRACT

Thesis contains 50 pages, 3 figures, 6 tables

The qualification work considers the problems of creating a special system for detecting, preventing and eliminating the consequences of computer attacks on information resources of automated control systems. The author analyzes the world legal practice in terms of protection against information threats and analyzes the solution of this issue at enterprises of various forms of ownership. The main stages of implementation of attacks on automated systems and the structure of the system for their detection and neutralization are presented. The author substantiates the need to create an effective system for counteracting cyberattacks, and points out the difficulties in creating such a system, in particular, analyzes the status and prospects of development of the domestic electronic industry. Based on the analysis, the author proposes and substantiates options for solving this problem, formulates the main conclusions and recommendations for its solution. To solve the tasks set out in the qualification work, the method of theoretical analysis of initial data in various segments of the issues under consideration, the method of generalizing the results obtained and developing the necessary solutions are used. The relevance of the issues under consideration is associated with the constant aggravation of the confrontation between world powers in the information space and the open imposition of a number of countries in the information war.

Object of research: cybersecurity processes for automated control systems.

The subject is protection technologies for automated control systems.

The purpose of the work is to improvement and recommendations for the application of cybersecurity methods for automated process control systems.

To achieve this goal, the following main tasks are performed:

- analysis of implemented technologies for cybersecurity of automated control systems;
- analysis and research of existing methods of cybersecurity of automated control systems;
- development of recommendations for the use of cybersecurity methods for automated process control systems.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПОКП	Проблемно-орієнтований комплексний підхід	Problem-oriented integrated approach
ОТВ	Організаційно-технічні вимоги	Organizational and technical requirements
ІМЗ	Інформаційно-математичне забезпечення	Information and mathematical support
АСУ	Автоматизовані системи управління	Automated control systems
ІБ	Інформаційна безпека	Information security
ІПК	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	

ЗЗІ	Засоби захисту інформації
ІС	Інформаційна система
ІТС	Інформаційно-телекомунікаційна система
ОЗП	Оперативний запам’ятовувальний пристрій
УВЧ	Ультра високі частоти

ВСТУП

Стрімко зростаючий інтерес до проблематики кіберпростору багато в чому пов'язаний з активністю розвинених країн у питаннях *кібервійськ* , *кібербезпеки* та захисту інформації. Префікс "*кібер*" до відомих термінів "*війна*", "*зброя*", "*безпека*" означає, як це прийнято в науковій літературі, застосування цих термінів до інформаційної сфери та сфери інформаційних технологій. Однією з причин можливих конфліктів в інформаційному просторі і, зокрема, виникнення *кібервійськ*, є відсутність міжнародних документів, що обмежують розробку і застосування *кіберзброї*.

З погляду міжнародного права важливими є два міжнародних документи, в яких розглядаються завдання інформаційного протистояння. Першим документом є Конвенція Ради Європи "Про кіберзлочинність", яка відкрита для підписання 23 листопада 2001 року і набула чинності в 2004 році. Другим документом є проект Конвенції Організації Об'єднаних Націй "Про забезпечення міжнародної інформаційної безпеки", підготовлений у 2011 році Україною в рамках Шанхайської організації співробітництва .

Унаслідок появи зазначених документів у світовому правовому просторі сформувалися дві правові парадигми, жодна з яких наразі не прийнята провідними країнами. Наслідком цієї обставини є той факт, що в разі початку великомасштабних конфліктів у кіберпросторі, правові інструменти зупинки агресії будуть малоефективними. Слід зазначити, і це, зокрема, відображено у військових доктринах багатьох країн, що серйозний конфлікт у кіберпросторі може потягти за собою реальний військовий конфлікт. Крім того, метою кібератак можуть бути об'єкти підвищеної небезпеки, зокрема, атомні електростанції, гідроелектростанції, збій у роботі яких може спричинити негативні наслідки.

Актуальність теми Питання дослідження кібератак та методів їх виявлення досить має на теперішній час великий науковий та практичний інтерес, так інформаційний захист залежить від надійності самої автоматизованої системи.

Ще певного часу назад автоматизовані системи були розраховані на одного користувача та обмін інформацією відбувався каналах, які мали не велику швидкість. Побудова мереж на основі комутації пакетів дала змогу значно підвищити швидкість обміну інформацією. На теперішній час будь-яка діяльність, пов'язана з обміном інформацією, не можлива без використання корпоративних мереж. Пропускна здатність і охоплення найбільшої мережі - мережі Інтернет постійно зростає. Це сприяє розвитку розподілених додатків для роботи по всьому світу. Такі системи широко використовуються в галузях кредитування, страхування, охорони здоров'я, права, військових додатків, зв'язку та багатьох інших. Спільне використання інформаційних ресурсів дає змогу значною мірою підвищити якість обслуговування споживачів, ефективність роботи бізнесу та державних організацій. Таким чином, для організацій та окремих користувачів характерний високий ступінь пов'язаності через відкриті мережі і, отже, залежність від безперебійної роботи та захищеності інформаційних потоків.

Разом з тим, неперервне впровадження мереж збільшило кількість потенційних зловмисників, які мають доступ до відкритих систем. Одним із небезпечних видів злочинної діяльності в мережі Інтернет є мережеві кібератаки.

Об’єктом дослідження: процеси кіберзахисту автоматизованих систем управління.

Предметом дослідження є технології захисту автоматизованих систем управління.

Мета роботи удосконалення та рекомендації щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій кіберзахисту автоматизованих систем управління;
- аналіз та дослідження існуючих методів кіберзахисту автоматизованих систем управління;
- створення рекомендацій щодо застосування методів кіберзахисту автоматизованих систем управління технологічними процесами.

РОЗДІЛ 1 ПРОБЛЕМИ СТВОРЕННЯ НАДІЙНОЇ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ НА АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ

1.1. Атаки на інформаційні системи та їх виявлення

Запобігання мережевим атакам на автоматизовані системи є одним з найскладніших завдань в завданнях інформаційного захисту автоматизованих систем. Більшість сучасних автоматизованих систем мають розподілену структуру, в фундаменті її побудови закладено використання мережевих технологій. Досвід показав, що забезпечення стійкої роботи таких систем залежить від здатності протистояти несанкціонованому втручанню в системи, яке спрямовано на порушення роботи як самої мережі, так і автоматизованої системи, що функціонує в самих рамках.

Дані інтернет-джерел, зокрема, щорічні звіти Інституту Комп'ютерної безпеки *CSI*, Координаційного Центру Негайного Реагування Сполучених штатів та Центру реагування на комп'ютерні інциденти України, свідчать про те, що число мережевих атак прогресивно зростати, а методи, що їх використовують злочинці, мають свій розвиток та своє вдосконалення. Варто зазначити, що сучасні системи виявлення вторгнень ще не досконалі та недостатньо ефективні з точки зору захисту інформації. Тому протидія несанкціонованому вторгненню на теперішній час є необхідним та актуальним завданням.

Успішні атаки з боку зловмисників реалізуються шляхом активізації вразливості, яка має місце в даній автоматизованій системі управління. Такими вразливостями можуть бути некоректно створена політика безпеки підприємства, відсутність певних засобів захисту інформації, а також помилки в самому програмному забезпеченні, що функціонує в автоматизованій системі. На малюнку 1.1 представлено види вразливостей, атак та можливі наслідки від них.

Рисунок 1.1. Вразливості на АСУ, атаки та наслідки

Кібератака уявляє собою сукупність дій зловмисника, що призводять до порушення інформаційного захисту автоматизованої системи. У результаті успішно реалізованої атаки порушник отримує несанкціонований доступ до інформації. Це призводить до порушення працездатності системи або спотворити вміст даних. Як потенційні цілі кібератаки можуть виступати сервери, робочі станції користувачів або комунікаційне обладнання. Узагальнюючи, будь-яка кібератака може бути розділена на чотири стадії:

Перша стадія – стадія *рекогностування***.** На цій стадії порушник намагається отримати якомога більше інформації про об'єкт кібератаки, в результаті чого створюється план подальшого етапу кібератаки. В першу чергу ця інформація стосується типу та версії операційної системи, список користувачів, зареєстрованих у системі, відомості про прикладне програмне забезпечення, яке використовується, та інша інформація, за допомогою якої можна здійснювати несанкціонований доступ.

Друга стадія – стадія *вторгнення* **.** На цьому етапі порушник отримує несанкціонований доступ до ресурсів тих автоматизованих систем, на які здійснюється кібератака.

Третя стадія – стадія атакуючого впливу. Ця стадія кібератаки спрямована на досягнення зловмисником тих цілей, для яких реалізовувалась кібератака. Прикладами таких дій можуть бути порушення працездатності, крадіжка конфіденційної інформації, що зберігається в автоматизованій системі, видалення або модифікація даних системи тощо. При цьому особа, яка здійснює кібератаку може також здійснювати дії, які можуть бути спрямовані на видалення слідів його присутності.

Четверта стадія – стадія подовження кібератаки. На цьому етапі виконуються заходи, які необхідні для продовження кібератаки на інші об'єкти. Процес виявлення кібератак на автоматизовані системи, представлено на рисунку 1.2.

Рисунок 1.2. Процес виявлення кібератак на АСУ.

З рисунку 1.2 видно, що процес виявлення кібератаки починається зі збору вихідних даних, необхідних для того, щоб визначити мету здійснення кібератаки. Такими початковими даними є:

- відомості про інформативні сигнали, які передаються в системі;
- інформація про продуктивність програмно-апаратного забезпечення, в яке входить інформація про обчислювальне навантаження на процесор, завантаженість оперативної пам'яті, швидкість роботи прикладного програмного забезпечення та інша інформація, яка стосується процесу прийому, обробки та передачі інформації в АСУ;
- відомості про можливості доступу до файлів, які уявляють собою конфіденційну та таємну інформацію;
- інформація про реєстрацію нових користувачів в автоматизованій системі та інша інформація, яка для цього необхідна.

Збір вихідних даних здійснюється за допомогою спеціалізованих датчиків системи виявлення кібератак, які розташовані в самій автоматизованій системі. Система виявлення може містити два типи датчиків - *мережеві* та *хостові*.

Мережеві датчики призначені для збору інформації про інформативні сигнали, що передаються в тому кластері автоматизованої системи, де відповідний датчик встановлено.

Що стосується *хостових* датчиків, то їх призначенням є збір інформації про події, що виникають на комп'ютерах, де вони встановлені. Прикладами такої інформації є відомості про мережевий трафік, що надходить на цей *хост* , а також системні події, що реєструються в журналах аудиту операційної системи *хосту*.

При цьому в одній кінцевій точці може бути встановлено одночасно певне число *хостових* датчиків, призначених для збору різноманітної інформації. Інформація, зібрана *мережевими* та *хостовими* датчиками, аналізується системою виявлення кібератак, метою якої є виявлення можливих кібератак зловмисників.

Розглянемо наявні проблеми на шляху створення експертної системи виявлення, попередження та ліквідації наслідків кібератак на інформаційні

ресурси підприємств різних форм власності, яка потребує створення та постійного вдосконалення.

Однією з головних задач створення такої системи є наявність у різних підприємств єдиної політики в сфері захисту інформації. Незважаючи на наявність у Раді Національної безпеки України державної служби спеціального зв`язку та захисту інформації, багато питань захисту інформації вирішуються в різних установах та підприємствах різних форм власності індивідуально, зважаючи на відсутність єдиної, опрацьованої ідеології, політики і нормативної бази.

Серед інженерно-технічних та апаратно-програмних проблем варто відмітити наступні:

- відсутність власного програмного забезпечення, операційних систем, зокрема й захищених. Наявні ліцензійні операційні системи та ліцензійне програмне забезпечення створюється в багатьох випадках на основі вільно розповсюджуваного програмного забезпечення, і до вітчизняних розробок їх можна віднести досить умовно;

- відсутність виробництва вітчизняної елементної бази. Стан української електронної промисловості веде до використання певних схемотехнічних рішень, які все рівно складаються з імпортного комплектування;

- телекомунікаційне обладнання на всій території України має іноземне походження. Як наслідок критичною є проблема застосування еталонного обладнання для мереж, яке має іноземне походження. Використання телекомунікаційного обладнання, яке не пройшло спеціальної державної сертифікації, породжує високі ризики працездатності мереж України;

- графова топологія транспортної мережі України вимагає перегляду та перебудови, зокрема, з точки зору її живучості в умовах війни з Росією. Донедавна під час побудови багатьох мереж, зокрема й державних, питання забезпечення живучості та надійності були на другому плані, що призвело до наявності багатьох завад у частині забезпечення доступності.

Похідними інженерно-технічних проблем є наступні:

- відсутність сертифікованого обладнання та програмного забезпечення систем виявлення кібератак;

- відсутність сертифікованого обладнання та програмного забезпечення систем протидії кібератакам.

Варто відмітити, що системи та продукти, які мають відповідні сертифікати Державного підприємства «Українські спеціальні системи», Служби безпеки України, Державної служби спеціального зв`язку та захисту інформації України не можуть бути гарантовано віднесені до сертифікованих. Проходженню сертифікації такими установами можна надати тільки певний рівень довіри - мінімальний ризик. На практиці встановлено, що використання сертифікованих систем, що базуються на іноземному апаратному та програмному забезпеченні, виправдане, з погляду можливого ризику, тільки в системах, що не належать до критично важливих.

1.2. Проблема створення систем захисту автоматизованих систем від кібератак

Важливим зазначити, що електронна промисловість уявляє собою галузь, в якій виробляється різноманітна компонентна база для електронної техніки, а також обладнання та засоби, які складаються з цих компонент.

Середній річний приріст світової електронної промисловості становить понад п`ятнадцяті відсотків, при товарообігу в двісті мільярдів доларів. Ця закономірність спостерігається вже понад тридцяти років та, за прогнозами експертів, триватиме ще протягом кількох наступних десятиліть. Для порівняння зазначимо, що обсяг усього нафтовидобутку країн, які мають нафтові сировинні ресурси у грошовому вираженні менший, ніж обсяг виробництва електронних компонентів.

У період Радянського Союзу союзна електронна промисловість працювала практично повністю на оборонний сегмент. Та частина електронної промисловості, яка обслуговувала цивільні галузі народного господарства, відігравала другорядну роль і була ніби придатком військового промислового

комплексу. Отже з переходом до ринкової економіки вітчизняна побутова техніка не була конкурентною з електронною базою найрозвиненіших країн не лише на світовому, а й на українському ринку, а скорочення армії та військового замовлення поставило підприємства галузі на межу банкрутства. Тільки наприкінці дев`яностих років спостерігалось вихід електронної промисловості з кризи.

Як зазначалося вище, для забезпечення захисту інформації України, країна потребувала в необхідності створення власного виробництва мікроелектроніки.

У всьому світі електронна промисловість розвивається як бізнес, в Україні ринкові відносини були відсутні. В Україні електронна промисловість може стійко розвиватися тільки за державної підтримки. Крім того, державі та бізнесу необхідно тісно взаємодіяти, оскільки бізнесу необхідні державні замовлення.

В Українській електронній промисловості поки що спостерігається недостатня конкуренція через незначну кількість власної продукції. Слабкий розвиток пояснюється також невеликим числом споживачів цієї продукції. Основна частина споживачів орієнтована на імпортну продукцію, практично повністю відсутні масштабні замовлення вітчизняної продукції. За рівнем виробництва і споживання електронної продукції Україна дуже сильно відстає від інших країн, таких як США або Японія.

За спостереганням багатьох фахівців та експертів, останнім часом намітилися кроки до поліпшення, зокрема, електронну промисловість назвали одним з основних, пріоритетних національних напрямів державної політики України. У 2020 році ухвалено Стратегію розвитку електронної промисловості до 2035 року. Крім того, в цю сферу надходять досить великі інвестиційні кошти.

Однією з головних переваг України перед іншими країнами є те, що Український ринок ще недостатньо розвинений, і бізнес ще може його заповнити. Зараз головне забезпечити не тільки приватні інвестиційні кошти, а й державні. Держава і бізнес повинні працювати в тісній взаємодії один з одним. Суттєво покращити становище зможе загальна модернізація Українських ключових виробництв в електронній промисловості, а також оптимізація галузі

на засадах приватно-державного партнерства та створення ринкової інфраструктури.

1.3. Підходи до створення системи захисту інформації в автоматизованих системах

Існує два основних підходи створення ефективної системи виявлення, попередження та ліквідації наслідків кібератак на автоматизовані системи управління.

ПЕРШИЙ ПІДХІД. На теперішній час на підприємствах різних форм власності в Україні існує в наявності багато ресурсів інформаційних технологій, які уявляють свою цінність для держави. Існуючі нормативні документи, які забезпечують виявлення інцидентів кібератак, не включають вимоги щодо поділу активів за ступенем важливості, що небезпечним як наслідки успішно реалізованих інцидентів. Для усунення цієї проблеми, розроблено проект доктрини кібербезпеки та захисту інформації України.

Відповідно до проекту даної доктрини, безпека автоматизованих систем управління критичної інфраструктури забезпечується за рахунок організації взаємодії цієї системи з розробленою системою виявлення, попередження та ліквідації наслідків кібератак на автоматизовані системи управління. Крім того, проект доктрини впроваджує проведення диференційованого захисту різних об'єктів, оскільки забезпечення надійного захисту всіх ресурсів України призведе до досить значних витрат бюджетних та приватних коштів, а в умовах війни це практично неможливо. Варто зазначити, що слабким місцем проекту доктрини є відсутність інструкцій для компаній та організацій щодо порядку проведення класифікації критичних автоматизованих систем управління, а також положення, відповідно до якого оцінку цінності активів організації та рівня захищеності об'єктів повинні проводити акредитовані спеціалізовані організації.

Важливо визначити підхід до створення системи виявлення, попередження та ліквідації наслідків кібератак на автоматизовані системи управління підприємств та організацій України, за допомогою якого здійснюється закріплення класифікації можливої цінності активів підприємств

та організацій на законодавчому рівні з розподілом вимог щодо захисту, а не шляхом вирішення цього питання організаціями, які мають відповідну акредитацію. Отже, необхідно на державному рівні здійснювати заходи з аналізу цінності активів, включаючи в першу чергу державні критичні інфраструктури, ресурси банків, приватні ресурси. Це призведе до спроможності оцінити захищені активи з позиції застосування адаптованих заходів та засобів захисту.

Розглядання цінності активів на законодавчому рівні усуне значну частину невизначеності, які виникають в процесі розв'язання проблем безпеки у масштабі держави. Важливим є розглядання міжнародного досвіду побудови захищених систем, таких як стандарти серії *ISO*27000 та вітчизняних інваріантів. Сильним боком міжнародних стандартів з інформаційної безпеки є застосування принципу "розумної достатності" в питаннях установлення цінності активів організацій і застосовності адекватних засобів захисту. Важливим етапом роботи після проведення сегментації активів є розмежування критично важливих об'єктів та інших структур інформаційного забезпечення.

Так як елементна база електронних засобів вітчизняного виробництва відсутня а внутрішнє програмне забезпечення має певні обмеження, то виникає необхідність в ізоляції особливо важливих корпоративних мереж та системи. Виходячи з даного підходу, виникає можливість в односторонньому зв'язку із зовнішніми мережами, при наявності умови гальванічної розв'язки. Необхідність в ізоляції особливо важливих систем зумовлена відсутністю гарантії в надійності захисту інформації автоматизованих систем управління.

Кількість активів, які не є критичними, значно більша за ті які є критичними, і тому їх спроможним є захищати за допомогою наявних сертифікованих засобів. До таких активів інтерес менший і тому до них не застосовується такі потужні структури, які спроможні здійснювати кібератаки як спецслужби іноземних держав. Враховуючи те, що сертифіковане обладнання уявляють собою засобами більшої довіри, то варто використовувати їх для захисту більшого сегменту систем.

Перевагою такого підходу є те, що постійно існує можливість створення системи структури, яку можна гнучно проектувати. Крім того вартість таких робіт не велика.

Процес ізоляції особливо критичних інфраструктур призводить до істотної гарантії власної безпеки, на відміну при підключенні через перевірені засоби.

Серед недоліків даного підходу є необхідність ізоляції окремих блоків системи, що призведе до незручностей та зниження оперативності роботи в системи.

ДРУГИЙ ПІДХІД. При такому підході здійснюється паралельне створення ідентичних систем інформаційних технологій, зокрема у сфері захисту інформації, у різних підприємствах та відомствах України. Таке забезпечення призводить до копіювання функцій, наявності різнотипного програмного та апаратного забезпечення, невиправданих втрат на утримання подібних систем, великих втрат на об`єднання систем. Також створення власних систем підприємств та відомств, які не об'єднані єдиним координаційним центром, призводить до прогресивного зростання корупції. Варто сказати, що присутність абсолютно ідентичних власних систем та мереж, які виконують однакові функції на підприємствах та відомствах є достатньо розкішною для великих та багатих підприємств. Те що було створено в Україні, призвело не тільки до величезних не потрібних втрат, а й погіршує управління системами та мережами в масштабах держави, оскільки керування ізольованими системами завжди вкрай ускладнене.

Головним завданням такого підходу в створенні автоматизованої системи управління, на відміну від першого, полягає в пошуку критичних місць та їх захист повністю тими засобами, які успішно пройшли спеціальні вимірювання. Видається доцільним не ділити активи за їхньою важливістю, а застосувати єдину вітчизняну новостворену систему. програмно-технічну платформу. Варто відмітити, що не є необхідністю створювати сегменти підприємств та відомств і не розкривати й так обмежені

ресурси, а використати всі засоби для створення системи на одній програмно-апаратній платформі з єдиною політикою безпеки та з заданою функціональною стійкістю. При такому підході постійно виявляються критичні точки розміщення засобів виявлення загроз, в тому числі в шлюзах підключення до автоматизованих систем інших держав. В таких випадках, при спроможності здійснювати концентрацію адміністративного, людського та фінансового ресурсу для вирішенні головного завдання, з'являється спроможність створення надійних вітчизняних проектів інженерно-технічних заходів та практична спроможність забезпечення цілісної системи захисту не тільки в державних підприємствах, а й в інших автоматизованих системах управління.

З позиції організації процесу проектування системи, необхідно призначити відповідального виконавця з надзвичайними повноваженнями. Дозволити тільки один, у виняткових випадках два ступені субпідряду. Пропонований підхід за рахунок фахового та зваженого керівництва призводить до створення ефективної систему виявлення, запобігання та ліквідації наслідків кібератак на інформаційні ресурси України.

Перевагою такого підходу є те, що по-перше, не є необхідним здійснювати процес ізоляції сегментів, так як створюється єдиний захищений інформаційний простір з прозорістю адміністрування. Як наслідок, в цьому випадку відбувається процес підвищення оперативності, поліпшується контроль проходження усіх процесів. По-друге, захист усієї інфраструктури України забезпечується вітчизняними інженерно-технічними засобами з найбільш високим рівнем захисту.

До недоліків пропонованого підходу слід віднести високу вартість проекту, так як в цьому випадку виникає необхідність в розробці, реалізації та впроваджені власних інженерно-технічні заходів. Крім того на етапах реалізації проекту виникають часові втрати.

Висновки до розділу 1

В результаті проведеного аналізу проблеми інформаційного захисту автоматизованих систем управління, можна зробити наступні висновки: 1. З точки зору міжнародного права Українські підприємства не захищені від великої кількості кібератак, які мають різні підходи .

2. Створення ефективної гарантованої Системи виявлення, попередження та ліквідації наслідків кібератак на автоматизовані системи управління підприємств різних форм власності можливе тільки шляхом розроблення повністю вітчизняних систем захисту інформації.

3. Перед введенням в експлуатацію вітчизняних систем захисту інформації, необхідно відокремити автоматизовані системи управління та корпоративні мережі критично важливої інфраструктури.

5. У сфері забезпечення захисту інформації необхідна адаптована державна політика, що включає вирішення всіх питань захисту інформації.

РОЗДІЛ 2 НОРМАТИВНО-ТЕХНІЧНІ ЗАВДАННЯ РОЗРОБКИ БЕЗПЕЧНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

2.1. Концептуальна модель нормативно-технічного регулювання автоматизованих систем

На теперішній час штучний інтелект розвивається в напрямі розв'язання практичних завдань, за допомогою яких відбувається наближення його спроможності до інтелектуальних спроможності фахівців. Найбільш активний розвиток штучний інтелект отримав в проектуванні та створенні автоматизованих систем управління та підтримки завдань прийняття рішень у реальному режимі часу або наближеному до реального, в системах динамічного планування, в засобах зберігання, вилучення, аналізу та моделювання практичних знань. Фахівець, який використовує автоматизовану систему управління для розв'язання поточних завдань, може досягати за результатами спроможності експертів у галузі інформаційних технологій, що дає змогу різко підвищити кваліфікацію інших спеціалістів за рахунок акумуляції знань у системі, зокрема знань експертів вищої кваліфікації.

Одним з таких завдань є автоматична обробка візуальної інформації, що уявляє собою одним із найважливіших напрямів у галузі розвитку штучного інтелекту. На теперішній час постійно виникають різноманітні завдання аналізу безлічі даних. Широке розмаїття сфер застосування вимагає підвищення якості оброблення зображень, що безпосередньо призводить до необхідності розроблення нових технологій, методів і алгоритмів оброблення . Завдання обробки інформації дедалі частіше потребують вирішення в режимі реального часу, тому дедалі більш затребуваними стають системи, що використовують машинний зір як основне джерело інформації. Технічний зір, сфера застосування якого безперервно розширюється, набуває нині великого значення в багатьох сферах діяльності людини і вважається однією з найперспективніших і затребуваних цифрових автоматизованих технологій. Зображення є формою найповнішого представлення інформації, яку, як правило, неможливо нічим замінити. Автоматизований зір може розглядатися як складова частина

технологій у галузі штучного інтелекту. Своєю чергою, розпізнавання образів є одним із найважливіших завдань штучного інтелекту, метою якого є копіювання та імітація інтелектуальної роботи людини.

На відміну від людського мозку робота технологій штучного інтелекту передбачає математичний вибір і розпізнавання шаблонів із масивів навчальних даних.

Основними науково-технічними напрямами розвитку технологій штучного інтелекту на теперішній час є технології віртуальної реальності, роботи та їх системи, а також експертно-аналітичні системи, крім того технології інтелектуального пошуку, аналізу та синтезу різних видів інформації. Нейронні мережеві технології знаходять застосування в системах аналізу та передбачення подій.

Здатність алгоритмів щодо прогнозування поведінки значно перевершують можливості людини. На досить високому рівні визначається потреба в експертних автоматизованих системах. В експертних системах база знань є формалізованими емпіричними знаннями висококваліфікованих фахівців у будь-якій вузькій предметній галузі. Автоматизовані системи призначені для розв'язання завдань у діалоговому режимі з фахівцями (кінцевими користувачами), від яких не вимагається знання програмування. Можна виокремити такі основні класи завдань, які розв'язуються автоматизованими інформаційними системами. Такими завданнями є діагностика, прогнозування, ідентифікація, управління, проектування, а також моніторинг.

Найпоширеніші галузі діяльності, що потребують використання експертних систем є медицина, обчислювальна техніка, військова справа, мікроелектроніка, радіоелектроніка, юриспруденція, економіка, екологія, управління технологічними процесами, геологія.

Концептуально-логічну модель нормативно-технічного регулювання систем, заснованих на технологіях штучного інтелекту, можна подати у вигляді безлічі взаємопов'язаних на різних рівнях комплексів і компонентів, що мають

властивості цілісності. За цільовим призначенням система нормативно-технічного регулювання штучного інтелекту є складною відкритою нерівноважною інформаційно-кібернетичною системою, що забезпечує нормативне регулювання і характеризується високим ступенем динамічності, нестійкості та невизначеності. Система правового регулювання базується на таких основних підсистемах: правова система , правова свідомість, правові відносини, та містить дворівневий внутрішній інформаційно-кібернетичну структуру правового нормативного та індивідуального регулювання та три зовнішні інформаційно-кібернетичні структури.

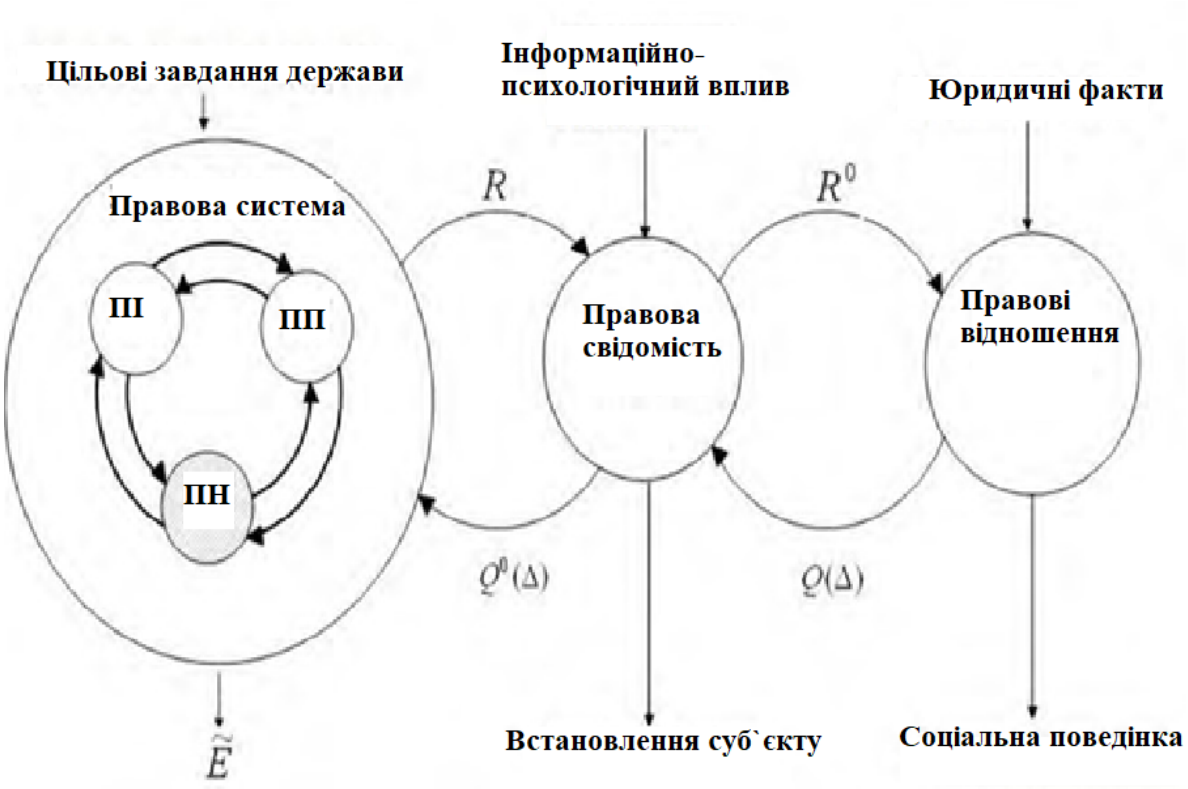

Рисунок 2.1. Концептуальна модель нормативно-технічного регулювання автоматизованих систем

Варто відмітити, що інформаційно-кібернетичний ланцюжок внутрішнього регулювання має такий вигляд: "*правова система* - *правові приписи* R - *правова свідомість* - R_0 - *правові відносини правова інформація* $Q(\Delta)$, що характеризує якість Δ *дотримання правових норм та принципів* - *правова свдомість* -

логічно оброблена правова інформація $Q_0(\Delta)$, що логічно оброблена - *правова система* ". Головними зовнішніми вхідними впливами та їм відповідними внутрішніми відгуками або результатами в даній підсистемі є цільові настанови держави та інтегральна оцінка ефективності правового регулювання, інформаційно-психологічні впливи, юридичні факти та правова поведінка.

Дослідження таких систем, які мають багато зв`язків на теперішній час проводяться на базі *концептуально – логічного* моделювання з використанням інваріантних *архітектур концептуального моделювання*. Архітектура системи моделюється на базі штучного інтелекту з використанням інваріантну функціональної структури *ергосистеми*, яку подано у вигляді комплексу функціональних підсистем, а саме: *вимірювання* P_1, *спостереження* P_2, *ідентифікації* P_3, *ухвалення рішень* P_4, *координації* P_5, *інформаційного обміну* P_6 та *інформаційного захисту* P_7, які потрібні в умовах функціонування в умовах інформаційного протистояння та які забезпечують необхідну захищеність інформації, яка обробляється. На вхід об'єкту керування P_0 в момент часу t надходять інформаційні впливи різної природи. Такими впливами є *функціональні* $R(t)$, *зовнішні цільові* $X(t)$ та *зовнішні координуючі* $X(t)$. На ці впливи система формує кожному свій відгук.

У загальному випадку технічна система, яка основана на штучному інтелекті, уявляє собою автоматизовану систему, що забезпечує розподіл інформаційних функцій та функцій керування між користувачем та робочим місцем, а також аналіз та видачу інформації, яка вимірюється, в зручному для користувача виді. Отже, основним результатом роботи системи є підготовка інформації з високим ступенем достовірності для ефективного ухвалення подальших рішень користувачем з одночасним отриманням інформації, яка уявляє собою рекомендацію щодо прийняття рішень користувачем. Існують критичні ситуації, коли виникає потреба в переході системи в автономний режим, в якому забезпечується виконання повного виробничо-операційного

циклу, включаючи ті рішення, які в подальшому застосовують отриману аналітичну інформацію без дій користувача.

Створення функціонально-стійкої автоматизованої системи моніторингу можливо на базі застосування проблемно-орієнтованого варіанту комплексного підходу (ПОКП), структурну схему якого представлено на рисунку 2.2.

Рисунок 2.2. Проблемно-орієнтований комплексний підхід

ПОКП за своїми інформаційними, кібернетичними та дидактичними характеристиками, націлений на інтеграцію методології інформаційного підходу при якому сам об'єкт визначається як цілеспрямована інформаційна система.

Методологія кібернетичного підходу полягає в тому, що об'єкт розглядається як система керування на рівні інформаційних процесів та алгоритмів функціонування інформаційної бази. Сама методологія дидактичного підходу полягає в тому, що об'єкт розглядається як система, що здатна адаптуватись до створення функціонально-стійкої автоматизованої оптико-електронної системи наземно-космічного моніторингу, що забезпечує захищене опрацювання візуальної інформації в умовах інформаційного протистояння.

Основними організаційно-технічними вимогами (ОТВ) інформаційного математичного забезпечення (ІМЗ), що впливають на функціональну стійкість

роботи АСУ, є точність, яка визначає якість дешифрування візуальної інформації, та оперативність, яка визначає забезпечення необхідного швидкого своєчасного виконання завдання.

Додатковими ОТВ до ІМЗ АСУ є:

1. Стійкість в імітації, яка визначає здатність не допускати нав'язування дезінформації в умовах інформаційного протистояння.
2. Стійкість, яка визначає здатність зберігати стан рівноваги в умовах деструктивних впливів.
3. Живучість, яка визначає здатність виконувати встановлений мінімальний обсяг функцій в умовах деструктивних негативних зовнішніх впливів.
4. Добротність, яка визначає спроможність функціонування в умовах відмов.

Показники інформаційно-цільової ефективності [11] можуть бути охарактеризовані таким чином:
Інформаційна точність:

$$I_{1ц} = \frac{E_ц}{\tau}, \tag{2.1}$$

де

$$E_ц = \max\left|I_z(M,T)\right| = \max\sum_{m=1}^{M}\left|\ln\left(\frac{T(O_m)}{T}\right)\right|. \tag{2.2}$$

$I_z(M,T)$ - кількість спостережень роботи підсистеми, при яких отримується інформація якісного змісту, O_m - оператор перетворення *тезаурісу* T, який відповідає одиничному інформаційному масиву $m \in M$, τ - середній проміжок часу протягом якого здійснюється обробка інформації, яка здійснюється одним об`єктом керування. Тоді інформаційна складова функціональної стійкості визначається наступним чином

$$I_{зц} = \frac{I}{I_S + I_z(T)} = \frac{E_ц + I_0 + I_V + I_z(T)}{I_V + I_z(T)} = 1 + \frac{E_ц + I_0}{I_V + I_z(T)}, \tag{2.3}$$

де I - загальний об`єм інформації, яка зберігається та циркулює в *ергасистемі*, $I_0$ - загальний об`єм інформації, яка зберігається в *ергасистемі*. Ще одним показником є інформаційна оперативність, яка визначається як

$$I_{2ц} = \frac{1}{E_ц}. \tag{2.4}$$

Інформаційно-технологічний показник якості (функціональної стійкості) функціонування автоматизованої системи управління визначається наступним чином

$$I_{2ц} = \frac{E_T}{E_T + I_S(\theta)},\ J_{1T} \in (0;1), \tag{2.5}$$

де

$$E_T = H(M_1) - \sum_i p(m_{01}) \cdot H(M_1 / m_{01}). \tag{2.6}$$

Представлення (2.6) уявляє собою міру технологічної функціональної стійкості автоматизованої системи управління, яка визначається i- ю інформаційною кінцевою точкою (вузлом) протягом процесу обробки інформаційних масивів. Статистична ентропія множини інформаційних масивів, які пройшли обробку визначається наступним представленням

$$H(M_1) = \sum_j p(m_{1i} / m_{0i}) \ln p(m_{1i} / m_{0i}). \tag{2.7}$$

2.2. Математична модель структури автоматизованих систем управління

Як правило вхідний інформаційний потік, що надходить на АСУ і який необхідно обробити, містить велику кількість характеристик, які є парметрами властивостей об'єкту. Ці характеристики, в багатьох випадках містять формалізовані та неформалізовані проекції об'єкту. Формалізовані проекції об'єкту уявляють собою множину формалізованих описів об'єкту, що відображають семантичні зв'язки між його змістовними елементами та множину перевірок, що реалізуються під час розв'язання задачі аналізу. Неформалізовані проекції об'єкту містять множину знань про об'єкт, якими система володіє і потужність цієї множини спроможна збільшуватись за рахунок поповнення знань в процесі роботи. Крім того до неформалізованих проекцій відноситься множина запитів, які формулюють під час ухвалення рішення. Інформаційно-математичну структуру АСУ представлено на рисунку 2.3

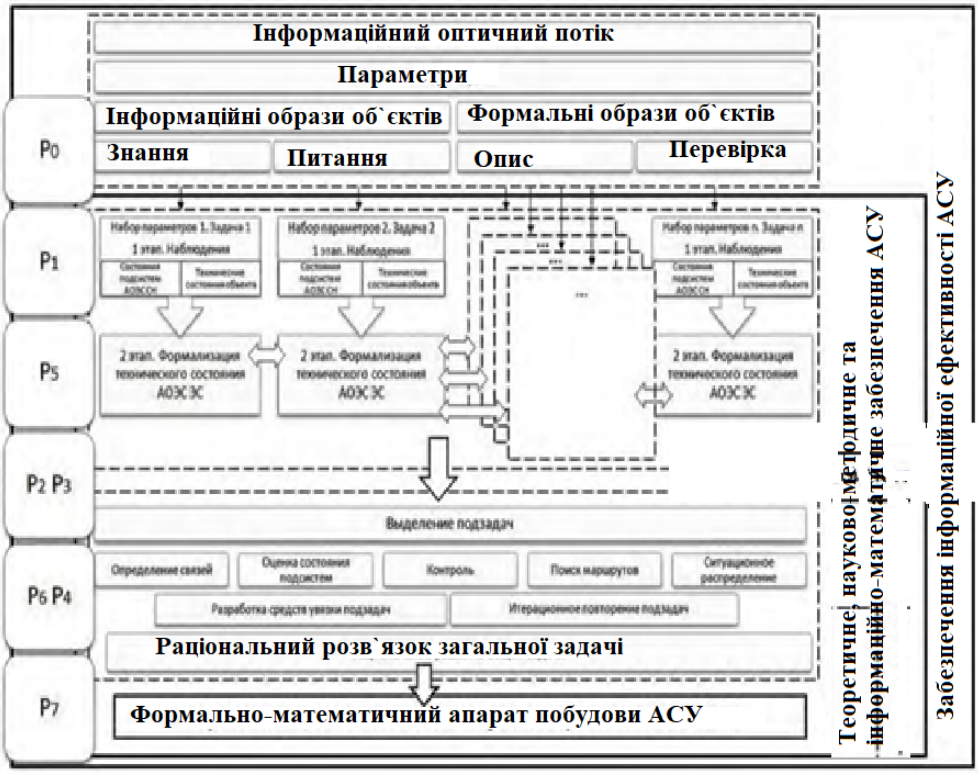

Рисунок 2.3. Інформаційно-математична структура АСУ

Для розв'язання кожної задачі обробки вхідної візуальної інформації вводять певну кількість характеристик (параметрів). Важливо відмітити, що різні комбінації параметрів можна застосовувати для постановки та розв'язання найрізноманітніших завдань. Реалізація процесу, як правило, проходить через два послідовні етапи:

Перший етап. Відбувається спостереження за поточними станами об'єкту та відповідними їм функціональними станами системи.

Другий етап. Здійснюється формалізація технічного стану системи, і як результат обробки, формується інформаційна модель розв'язання задачі.

Щоб розв`язати складну задачу функціонування АСУ, було розроблено методику, що використовує нову функціонально-стійку технологію обробки візуальної інформації в АСУ у режимі реального часу з заданим критерієм якості.

Розроблення технології створення програмно-апаратних засобів переробки візуальної інформації, що ґрунтується на ІМЗ багаторівневої АСУ, здійснюється

шляхом послідовного виконання сукупності етапів для отримання необхідного результату. Послідовність кроків уявляє собою технологію, яка реалізується впорядкованою сукупністю необхідних моделей, методів та алгоритмів.

Етап 1. Введення вихідних даних для обробки з урахуванням заданої ситуаційної моделі функціонування АСУ.

Етап 2. Здійснення оцінки руху відеокамери та забезпечення стабілізації оптичного зображення. Відновлення кадрів візуального інформаційного потоку, формування стабілізованого оптичного зображення.

Етап 3. Процес формування інформаційної бази АСУ, навчання нейронних мереж для розв'язання задач розпізнавання візуальної інформації. Процес підготовки інформаційної бази складається з розмітки зображень за допомогою розробленого універсального методу, що враховує основні принципи побудови навчальних вибірок для навчання нейронних мережевих алгоритмів за комплексними сценаріями.

Крок 4. Дешифрування стабілізованого оптичного зображення здійснюється за допомогою розроблення та модифікації ефективних алгоритмів оперативного перетворення візуальної інформації за допомогою формалізованих процедур детектування, локалізації та класифікації об'єктів на аерокосмічних оптичних зображеннях.

Крок 5. Проведення функціонального діагностування АСУ, оцінювання відповідності заданого критерію якості.

Крок 6 . Здійснення видачі результату у формі впорядкованої інформаційної послідовності станового типу, який необхідно для прийняття подальших рішень, а також для здійснення процесу прогнозування та оперативного планування тактики поведінки в умовах інформаційного протистояння.

2.3. Проблеми впровадження технології штучного інтелекту

Процес впровадження новітніх технологій істотно породжує велику кількість завдань. Швидкі темпи технологічного прогресу в галузі штучного інтелекту породжують нові задачі в захисті інформації від негативних наслідків несанкціонованого застосування технологій. Однією з перешкод для широкого впровадження технологій штучного інтелекту наразі є відсутність нормативної бази, що визначає єдині формати представлення даних на всіх стадіях життєвого циклу, принципи відображення специфічних загроз в задачах інформаційної безпеки та захисту інформації, а також регламентує актуальні питання створення та експлуатації безпечних, надійних та функціонально-стійких систем, створені за допомогою штучного інтелекту. Повна відсутність нормативного та правового і технічного регулювання умов та специфіки розроблення, введення в експлуатацію, функціонування, та організацію інтеграції в споріднені системи та контролю застосування технологій штучного інтелекту наразі є загальносвітовою. Різноманіття сфер застосування визначає різні форми нормативно-правового регулювання систем штучного інтелекту. Це також впливає на розвиток програмних технологій підтримки прийняття рішень в режимі реального часу з елементами штучного інтелекту, а також залучення систем штучного інтелекту під час

аналізу великих масивів даних та видобутку знань, включно з новими методами та алгоритмами для збирання, зберігання та інтелектуального аналіз

Визначають 5 критично важливих направлень для виявлення ризиків, що виникають, у зв`язку з використанням штучного інтелекту, Ступінь впливу цих чинників на суспільство схематично можна подати у вигляді перевернутої піраміди, в вершині якої зазначено етику, що здійснює на суспільство максимальний вплив, а в основі піраміди - доступність програмного забезпечення, вплив якого може бути максимальним. На рисунку 2.4 представлено це схематично.

Рисунок 2.4. Критично-важливі галузі в штучному інтелекті

Програмне забезпечення є ключовим елементом систем штучного інтелекту. Наявність відкритих кодів ПЗ створює ризики ненавмисного неправильного застосування технологій. За відсутності ПЗ у відкритому доступі з'являється ризик виникнення шкідливого штучного інтелекту, створеного групою фахівців, допущених до розробок, також існує ризик використання ШІ злочинцями і терористами.

Для забезпечення безпеки необхідні превентивні заходи, що дають змогу знизити ризики ненавмисних наслідків. Для безпечного впровадження необхідна організація обов'язкового тестування технічних систем, заснованих на штучному інтелекті, в умовах наближених до реальності. Підконтрольність передбачає прозорість і можливість перевірки ухвалення штучним інтелектом рішень. Таким чином, повинна забезпечуватися забезпечуватися можливість пояснення причин, через які ухвалено те чи інше рішення. Прозорість ухвалення рішень дасть можливість забезпечення об'єктивності результатів незалежно від особистих характеристик споживача і з

урахуванням того, що навчання алгоритмів проводиться з використанням згенерованих людиною даних.

Висновок до розділу 2

1.В основі інформаційного захисту технологій штучного інтелекту лежить спроможність зовнішнього моніторингу інформації, чітке виконання розпоряджень користувача, а також обов'язкове включення до програми штучного інтелекту правил морального та етичного характеру.
2.Розглянуті підходи до розв'язання задачі функціонально-стійкого створення, функціонування та експлуатації безпечних, надійних та якісних систем, які базуються на штучному інтелекті.
3.Формування моделей нормативно-технічного регулювання систем, заснованих на технологіях штучного інтелекту, умов та особливостей розроблення, введення в експлуатацію, функціонування, здійснення інтеграції в споріднені системи та контролю застосування технологій штучного інтелекту може здійснюватися на основі багаторівневого концептуально-логічного моделювання *ергосистем* та інформаційних нормативно-технічних відносин.

РОЗДІЛ 3 ЗАПОБІГАННЯ ІНЦИДЕНТАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

3.1. Основні завдання запобіганню інцидентів інформаційної безпеки

Методи математичної інформатики та теорії нечітких множин. Отриманий результат. Інцидент інформаційної безпеки, включаючи інцидент комп'ютерний, розглядається як факт порушення або припинення функціонування автоматизованої інформаційної системи та порушення інформації, що зберігається та обробляється в цій системі, у тому числі викликаний комп'ютерною атакою. Інформаційні описи представлені у вигляді структурованих даних про ознаки комп'ютерних атак. Структуровані дані є кінцевими послідовностями рядків символів формальної мови. Як метрика вимірювання відстані між рядками символів з певного алфавіту запропоновано використовувати редакційну відстань *Дамерау – Левенштейна*. Обґрунтовано можливість подання семантики інформаційних описів ознак атак у вигляді нечітких множин. Визначено кластери поділу нечітких інформаційних описів. Оцінено вплив семантичної визначеності інформаційних описів ознак , тобто кластерів розмитості нечітких інформаційних описів, при прийнятті рішень про їхню ідентичність, тобто схожість. Показано, що семантична складова інформаційних описів ознак комп'ютерних атак передбачає наявність деякої семантичної метрики і яка, як правило, формально погано визначена, неоднозначно інтерпретована та характеризується невизначеністю типу нечіткості, наявністю семантичної інформації та неможливістю безпосереднього застосування ймовірності заходу визначення ступенів подібності вхідних та збережених інформаційних описів ознак. Запропоновано підхід до ідентифікації нечітких інформаційних описів ознак комп'ютерних атак та застосування методів поділу елементів опорних множин, на яких визначено ці інформаційні описи. Показано, що результати процедури ідентифікації нечітких інформаційних описів ознак комп'ютерних атак залежать від ступенів поділу опорних множин та показників семантичної невизначеності цих описів.

Під інцидентом інформаційної безпеки (ІБ), включаючи інцидент комп'ютерний, розумітимемо факт порушення або припинення функціонування автоматизованої інформаційної системи (АІС) та (або) порушення інформації, що зберігається та обробляється в цій системі, у тому числі викликаний комп'ютерною атакою

КА – це цілеспрямований несанкціонований вплив на інформацію, на ресурс АІС, що захищається, або отримання несанкціонованого доступу до них із застосуванням програмних або програмно-апаратних засобів. Попередження інцидентів ІБ пов'язане з оцінкою ризиків порушення критично важливих властивостей (цілісність, доступність і конфіденційність) ресурсів АІС, що захищаються, з різними категоріями важливості в результаті впливу КА. З цією метою відповідна система моніторингу RF повинна розпізнавати (ідентифікувати) загрозу безпеці інформації (БІ), що виникла, в динаміці функціонування АІС. КА можна подати у вигляді сукупності інформаційних описів ознак, яку необхідно ідентифікувати у процесах технологічного циклу, що реалізується АІС при спробах порушника виведення її з ладу або зниження ефективності застосування. Сукупність інформаційних описів ознак КА формується, декомпозується та систематизується на основі апріорних знань про досвід експлуатації АІС та класифікацію загроз безпеці інформації (БІ), а потім уточнюється за апостеріорною інформацією. Основними засобами та джерелами інформації для ідентифікації інформаційних описів ознак КА та запобігання виникненню інцидентів ІБ в АІС є датчики засобів протидії. Засоби протидії КА разом із засобами моніторингу небезпеки впливу КА здійснюють збирання даних від датчиків для формування сукупності інформаційних описів ознак атак та оцінки можливого порушення стійкості функціонування АІС та ступеня небезпеки. Якщо КА реалізує відому загрозу БІ, можна застосувати методи аналізу (порівняння) інформаційних описів характерних ознак атаки (збережені інформаційні описи ознак КА – сигнатури атак), що використовуються їх виявлення. Методи аналізу сигнатур призначені для ідентифікації відомих атак і засновані на контролі програм і даних у системі та еталонному звірянні

послідовності символів та подій у мережі з базою даних сигнатур атак. Недоліком методів аналізу сигнатур є неможливість виявлення нових (модифікованих атак) без суворої формалізації ключових слів мережевого трафіку та оновлення бази даних сигнатур атак. Якщо виявляється аномальна поведінка системи відмінна від типового (інформаційні описи ознак КА відсутні в базі сигнатур), то на підставі цього факту можна ухвалити рішення про можливу наявність атаки (виявлена невідома атака). Виявлення аномальних відхилень у мережі здійснюється за ознаками КА - зазвичай використовують синтаксичні сигнатури, взяті безпосередньо з тіла атаки. Так як інформаційні описи ознак реалізованої КА і збережені інформаційні описи ознак КА являють собою синтаксичні конструкції, то для їх порівняння є сенс використовувати метрику, що є функцією відстані між двома словами (рядками), що дозволяє оцінити ступінь їх подібності в даному контексті. Суворе математичне визначення метрики включає необхідність відповідності умові нерівності трикутника (X - безліч слів, p - метрика)

$$(\ p(x,y) \leq p(x,z) + p(z,y), \qquad x,y,z \in X$$

Тим часом, у більшості випадків під метрикою мається на увазі більш загальне поняття, яке не вимагає виконання такої умови, але яке можна також розглядати як відстань. До найбільш відомих з таких метрик відносяться відстані Хеммінга, Левенштейна і Дамерау-Левенштейна. Слід зазначити, що відстань Хеммінга є метрикою лише на безлічі слів однакової довжини, що обмежує область його застосування.

Основні завдання, які вирішуються у процесі попередження інцидентів НСД

-обґрунтування можливості подання семантики інформаційних описів ознак у вигляді нечітких множин .

-Визначення порогів кластерів поділу нечітких інформаційних описів.

-Оцінка впливу семантичної визначеності інформаційних описів ознак , тобто кластерів розмитості нечітких інформаційних описів) на прийняття рішень про їх ідентичність.

Змістовна постановка завдання запобігання інцидентам НСД

Ідентифікації інформаційних описів ознак : пошук за вхідним інформаційним описом схожих на нього збережених інформаційних описів в умовах можливих спотворень, неповного складу та часткового порушення порядку слідування даних у вхідному та збережених описах.

Під інформаційним описом розумітимемо структуровані дані про ознаки. Дані представлені значеннями, тобто кінцевими послідовностями рядків символів формальної мови, відповідних атрибутів. Атрибути можуть бути згруповані за деякою семантичною ознакою.

Особливості завдання:

1) обробка та аналіз рядків символів. Це здійснюється за рахунок моделювання ідентифікації інформаційних описів, у тому числі і в умовах неповних та спотворених відомостей про них;

2) довільна кількість помилок під час аналізу символьних рядків, тобто довільна кількість операцій редагування . Це є вставка, заміна, видалення, перестановка;

3) клавіатурна модель помилок із визначенням середньозваженої редакційної відстані між рядками;

4) наявність ваги помилок, що залежать від символу, над яким здійснюється операція в залежності від особливості формальної мови, що визначається обраним алфавітом; вага помилки залежить від розташування символу в слові; облік ваги помилки з близьким символом, який є на клавіатурі;

5) велика кількість операцій над рядками, а саме заміна, вставка, видалення рядків для обробки помилок транскрибування;

6) наявність нечіткого заходу за рахунок урахування ваг помилок; невизначеність типу нечіткості; нечіткість, розмитість співвідношення вхідного інформаційного опису до виділеного підмножини збережених; перехід від повної ідентичності вхідного опису зберігається до повної не ідентичності відбувається поступово *нечіткість = неточність + невизначеність*.

3.2. Формальна мова

Визначено певний алфавіт ℵ і ℵ* - більшість визначених над цим алфавітом рядків

$$\varepsilon_k \in \aleph^*, k = \overline{1, N^{str}}$$

Рядок $\varepsilon_k = (a_1, \dots, a_n)$ уявляє собою скінченна послідовність символів $a_i \in \aleph$. Алфавіт ℵ включає в себе символ «пробіл» («_»), а ℵ* - пусту строку ε.

Якщо $str_1 \in \aleph^*$ - рядок довжини m, а $str_2 \in \aleph^*$ - строка довжини n, то їх об'єднання $str_1 \cup str_2$, що позначається як $str_1 str_2$, являє собою строку довжини m+n, в якій перші m символів складають строку, що співпадає з str_1, а останні n символів складають строку, що співпадає з str_2. Якщо $str_3 = str_1 str_2$, де $str_3, str_1, str_2 \in \aleph^*$, то строка str_1 – префікс строки str_3, а строка str_2 – суфікс строки str_3.

Побудова префіксних дерев значно скорочує час пошуку рядків символів (слів). Префіксне дерево має багато корисних властивостей для вирішення задачі ідентифікації інформаційних описів.

Перше. При обході дерева будь-який префікс будь-якого імені проходить лише один раз. Це не лише заощаджує час перегляду набору унікальних імен. Можна побудувати такий алгоритм, який буде використовувати стан таблиці динамічного програмування попередньої вершині для обчислення стану в поточній вершині. Іншими словами, стан таблиці динамічного програмування

для обчислення оптимальної редакційної відстані завжди відповідає префіксу будь-якого слова із заданого алфавіту.

Друге. Якщо префікс якогось імені вже містить кількість помилок редагування більше, ніж допустима кількість k, то всі вирівнювання всіх імен, що починаються з цього префікса (і що знаходяться в піддереві цього префікса), можна не проводити.

Третє. Можна ввести ваговий поріг на оптимально зважену редакційну відстань. Тоді, якщо префікс якогось імені важить більше, ніж поріг, то всі вирівнювання всіх імен, що починаються з цього префікса (і в піддереві цього префікса) можна не проводити.

Четверте. Застосування префіксного дерева робить очевидним пошук скорочених ознак, тому що скорочення є не що інше, як префікс і потрібно просто дістати всі продовження цього префікса з піддерева цього префікса. Довільне підмножина множини $\aleph^*$ називають формальною мовою Λ. Якщо строка str може бути отримана зі строки str' за допомогою одного або декількох правил виводу, то $str' => str$.

Два рядки str_1 і str_2 називаються схожими, якщо редакційна відстань між ними не перевищує заданої припустимої кількості помилок k. Редакційне припис – послідовність дій, необхідні отримання з першого рядка другий найкоротшим чином. Зазвичай події позначаються так: D - видалити, I - вставити, R - замінити, M - збіг. Кожна операція редагування має вагу: I – p, D – q, R – r, T – v. Тоді зважена редакційна відстань між двома рядками str_1 і str_2 визначається як сумарна вага мінімального числа редакційних операцій, необхідних для перетворення str_1 в str_2 .

Якщо σ^{Π} поріг на зважену редакційну відстань, два рядки str_1 і str_2 схожі, якщо редакційна відстань між ними не перевищує припустимої кількості помилок k, а зважена редакційна відстань не перевищує σ^{Π}.

Ступінь схожості s_1та s_2 визначається величиною σ. Чим менше σ, тим більше str_1 схожа на str_2.

Відстань Дамерау-Левенштейна – це міра різниці двох рядків символів, яка визначається як мінімальна кількість операцій вставки, видалення, заміни та перестановки сусідніх символів, необхідних для переведення одного рядка в інший. Є модифікацією відстані Левенштейна, відрізняється від нього додаванням операції перестановки.

Семантика будь-якої інформації про ознаку передбачає наявність наступних чотирьох величин: реперної множини X описів, семантичного покажчика x однієї з описів X, тобто $x \epsilon X$, підмножини δ ознаків з X, тобто $\delta \subset X$ і семантичної достовірності виконання головної умови $x \epsilon \delta$. Якщо x_0 - точка X і δ – деякий час непорожня підмножина X, котре визначається властивістю δ, то факт належності $x_0 \epsilon \delta$ або істинний вираз «точка x_0 із X має властивість δ» записується у вигляді одномісного предикату $\delta\,(x_0), x_0 \epsilon X$.

Якщо P – решітка достовірності, X – опорна множина, $x_0 \epsilon X$ і $\delta \subset X$, і якщо про точку x_0 відомо із семантичної достовірністю p ϵ P, що $x_0 \epsilon \delta$, то існує свідчення про точку $x_0 \epsilon X$, яке записується як приналежність $x_0 \epsilon \delta$, з достовірністю p або вираз «точка x_0 з X наділена властивістю δ із семантичною достовірністю p». Якщо більш точно, то згідно з основними положеннями математичної інформатики під інформаційним описом $\Delta(x)$ довільного знака x, піднімається структуровані зведення виду (p)δ(x):

$$\Delta(x) = \{(p_i)\delta_i\}(x), i = \overline{1, N_\delta}$$

В зведення $\{(p_i)\delta_i\}(x)$ інтерпретуються як «ознака x із X характеризується властивістю δ_i з семантичною достовірністю p_i», δ_i – підмножина ознак з X , що характеризуються однойменною властвістю $\delta_i \subset X$, а p_i семантична достовірність того, що $x \epsilon \delta_i$.

Розглянемо інформаційний опис $\Delta(x) = \{(p)\delta_p; 0 < p \leq 1\}(x_i)$ де δ – група підмножин таких, що $x_i \in \delta_p$, $0<p\leq 1^p$із семантичною достовірністю р. Для δ_p можна підібрати інформаційний опис

$$\Delta(x_j^p) = \{(p')\delta_{p'}; 0 < p' \leq 1\}(x_j), \; i \neq j$$

Такі, що $$\delta_p = \{x_j \mid x_j \in \delta_{p'}, p' \geq p\}$$

Отже, δ_p і $\delta_{p'}$ - множини рівнів р і р' нечіткої властивості множини $\tilde{\delta} : \tilde{\delta} = \{x, p_{\tilde{\delta}}(x)\}$.

$p_{\tilde{\delta}}(x) = \mu_{\tilde{\delta}}(x) : X \to [0,1]$ - функція належності. Отже, семантика інформаційного стану $\Delta(x_i)$ и $\Delta(x_j)$ у відповідності з математичною інформатикою формально представлена нечіткою властивістю $\tilde{\delta}$.

Таким чином, семантика інформаційного стану ознаки може бути представлена НМ , тобто формалізація через безліч рівнів і, отже, може оброблятися з використанням відомих операцій над НМ.

Зазначимо, що семантична складова інформаційних описів ознак передбачає наявність деякої семантичної метрики (для її виміру та інтерпретації) і, як правило, формально погано визначена, неоднозначно інтерпретована.

Таким чином, інформаційні описи ознак характеризуються невизначеністю типу нечіткості, наявністю семантичної інформації та, як наслідок, неможливістю безпосереднього застосування імовірнісного заходу для визначення ступенів подібності інформаційних описів різних ознак.

Нагадаємо, що якщо деяка ознака $x_0 \in X$ має властивість $\tilde{\delta}$, і лише частково $0 < \mu_{\tilde{\delta}}(x_0) < 1$, то внутрішня невизначеність, двосмисловість ознаки x_0, по відношенню до властивості $\tilde{\delta}$, проявляється в тому, що він, хоча й в різній степені, належить одразу двом протилежним класам: «класу ознак, що має властивість $\tilde{\delta}$», та класу ознак, що «не має властивості $\tilde{\delta}$». Ця двосмисловість

ознаки x_0 по відношенню до властивості $\tilde{\delta}$ максимальна, коли степені належності ознаки x_0 до класів «$\tilde{\delta}$» і «не $\tilde{\delta}$» рівні, тобто $\mu_{\tilde{\delta}}(x_0)=0{,}5$ і $\mu_{не\tilde{\delta}}(x_0)=1-\mu_{\tilde{\delta}}(x_0)=0{,}5$

.

Та навпаки, двосмисловість ознаки мінімальна, коли ознака належить тільки одному з класів тобто або: $\mu_{не\tilde{\delta}}(x_0)=1$, або $\mu_{\tilde{\delta}}(x_0)=0$, або $\mu_{не\tilde{\delta}}(x_0)=0$, або $\mu_{не\tilde{\delta}}(x_0)=1$

Таким чином, показник семантичної невизначеності нечіткої властивості $\tilde{\delta}$ можна подати у вигляді показника розмитості (заходи ентропії) відповідного НМ [8].Зокрема, показник семантичної невизначеності нечітких властивостей $\tilde{\delta}$ можна визначити за аналогією з шенненівською ентропією теорії інформації у вигляді логарифмічної ентропії:

$$d(\tilde{A})=k\sum_{j=1}^{N}S(\mu_{\tilde{A}}(x_j)),$$

де S - функція Шеннона $S(y)=-y\ln y-(1-y)\ln(1-y)$ і k-позитивна константа.
Згортка векторних нечітких відносин переваги має вигляд:

$$\mu_P(x,y)=\sum_{j=1}^{m}\lambda_j\mu_j(x,y),$$

де λ_j- коефіцієнт важливості для нечіткого відношення-
ня переваги з функцією приналежності μ_j.

Змістовна постановка задачі ідентифікації інформаційних описів передбачає застосування методів поділу елементів опорних множин, на яких визначено нечіткі властивості залежно від ступенів поділу та від показників семантичної невизначеності нечітких властивостей. Показник семантичної невизначеності нечітких властивостей було розглянуто раніше. Розглянемо поняття ступеня поділу нечітких інформаційних описів [9].

8. Ступінь поділу нечітких інформаційних описів. Нехай на опорній множині ознак X визначено нечіткі властивості

$\tilde{\delta}_i = \{(x, \mu_{\tilde{\delta}}(x))\}$.

Оскільки будь-які дві нечіткі властивості $\tilde{\delta}$ и $\tilde{\delta}_j$, $i \neq j$, ,обмежені ступенями приналежності

$\sup \mu_{\tilde{\delta}_i}(x)$ i $\mu_{\tilde{\delta}_j}(x)$) в точках α_i та α_j

відповідно, то їх перетин $\tilde{\delta}_i \cap \tilde{\delta}_j$ набуває максимального значення

$\sup_x \mu_{\tilde{\delta}_i \sim \tilde{\delta}_j}(x)$ в У. Найвищий ступінь поділу нечітких властивостей $\tilde{\delta}_i$ и $\tilde{\delta}_j$ досягається в точці

$\gamma = 1 - \sup_x \mu_{\tilde{\delta}_i \sim \tilde{\delta}_j}(x)$.

Для поділу елементів, що відповідають властивостям $\tilde{\delta}_i$ и $\tilde{\delta}_j$ можна використовувати поняття порога поділу. У цьому випадку поріг поділу Pr обмежений умовою

$$\Pr < \max_x \min [\mu_{\tilde{\delta}_i}(x), \mu_{\tilde{\delta}_j}(x)] = \sup_x \mu_{\tilde{\delta}_i \sim \tilde{\delta}_j}(x).$$

Таким чином, для обраного порога поділу Pr області Mi і Mj поділу порівнюваних елементів щодо переваг будь-яких двох властивостей (далі – області поділу) $\tilde{\delta}$ и $\tilde{\delta}_j$, $i \neq j$, визначаються нечіткими підмножинами рівня

$$M_i = \{x \mid \mu_{\tilde{\delta}_i}(x) \geq \max_x \min [\mu_{\tilde{\delta}_i}(x), \mu_{\tilde{\delta}_j}(x)]\} \text{ и}$$
$$M_j = \{x \mid \mu_{\tilde{\delta}_j}(x) \geq \max_x \min [\mu_{\tilde{\delta}_i}(x), \mu_{\tilde{\delta}_j}(x)]\}$$

Для всіх $x \in M_i$.

Представлена вище модель узагальнюється на N_3 нечітких властивостей $\tilde{\delta}_i$, $i = \overline{1, N_3}$.

Якщо $\tilde{\delta}_i = \{(x, \mu_{\tilde{\delta}_i}(x))\},\ i = \overline{1, N_{\tilde{\delta}}}$ обмежені опуклі нечіткі властивості, то нечіткі підмножини $\tilde{\delta}_1 \cap \tilde{\delta}_2, \tilde{\delta}_1 \cap \tilde{\delta}_3, \ldots, \tilde{\delta}_1 \cap \tilde{\delta}_Q, \tilde{\delta}_2 \cap \tilde{\delta}_3, \ldots, \tilde{\delta}_{Q-1} \cap \tilde{\delta}_m$ будуть такими ж опуклими й обмеженими. Таким чином можна визначити області розділення $\underline{M}_1, \underline{M}_2, \ldots, \underline{M}_{N_{\tilde{\delta}}}$ и $\overline{M}_1, \overline{M}_2, \ldots, \overline{M}_{N_{\tilde{\delta}}}$, елементів з використанням нижнього та верхнього порогів розділення:

$$\underline{M}_i = \{x \mid \mu_{\tilde{\delta}_i}(x) \geq \min_{i,j} \max_x \min[\mu_{\tilde{\delta}_i}(x), \mu_{\tilde{\delta}_j}(x)]\} \text{ и}$$

$$\overline{M}_i = \{x \mid \mu_{\tilde{\delta}_i}(x) \geq \max_{i,j} \max_x \min[\mu_{\tilde{\delta}_i}(x), \mu_{\tilde{\delta}_j}(x)]\}$$

Для всіх $x \in \overline{M}_i, \underline{M}_i$.

Якщо $\mu_{\tilde{\delta}_i}(x) = \underline{\Pr}$, то $(\underline{\Pr})\delta_{i_{\Pr}}(x)$ – відомості про те, що ознака х має властивість $\tilde{\delta}_1$ з семантичною достовірністю$\underline{\Pr}$.Тут $\tilde{\delta}_i^0$ - безліч рівня $\underline{\Pr}$ нечіткої властивості$\tilde{\delta}_1$. Сказане справедливо і для $\underline{\Pr}$

Нехай $\Delta(x_{so}) = \{(p_i^{so})\delta_i^{so}\}(x_{so})$ збережені інформаційні описи, $i = \overline{1, Q}, so = \overline{1, N_{so}}$, Q - Число нечітких властивостей в інформаційному описі,

N_{50} кількість збережених інформаційних описів, та $\Delta(x_0) = \{(p_i^0)(\delta_i^0)\}(x_0)$ -- інформаційний опис0вхідних ознак. Тут Тут$\tilde{\delta}_i^0$– значення і-ї властивості у вхідному інформаційному описі x_0, δ_i^{so} – значення і-го властивості збереженого інформаційного опису X_{50}.

Формальне розв'язання задачі ідентифікації КА передбачає

1) формування семантичних метрик для вимірювання та інтерпретації нечітких властивостей вхідного та збереженого інформаційного опису;
2) визначення значення

$$(\mu_{\tilde{\delta}_i}(x_0, x_{so}))(\delta_i^0 \sim \delta_i^{so})(x_{so})$$

Де $\mu_{\tilde{\delta}_i}(x_0, x_{so})$ ступінь подібності зберігається X_{50}.

та вхідного X_0 описів щодо значень властивості δі зберігається $\tilde{\delta}_i^{50}$ та вхідного $\tilde{\delta}_i^{0}$ інформаційного опису;

3) визначення верхнього Pr та нижнього Pr порогів поділу збережених інформаційних описів з урахуванням ступенів подібності $\mu_{\tilde{\delta}_i}(x_0, x_{50})$ з вхідним інформаційним описом щодо нечітких властивостей δі;
4) класифікування збережених інформаційних описів за ступенями подібності до вхідного інформаційного опису:

збережені інформаційні описи еквівалентні вхідному інформаційному опису

$$M_э = \{x_i \mid \mu_P(x_0, x_i) \geq \Pr\}, \quad (3)$$

$$M_п = \{x_i \mid \underline{\Pr} \leq \mu_P(x_0, x_i) \leq \overline{\Pr}\}, \quad (4)$$

$$M_н = \{x_i \mid \mu_P(x_0, x_i) \leq \underline{\Pr}\}. \quad (5)$$

5) за значеннями (2) визначити переваги

$$\mu_P(x_0, x_i) = f((^0p_i^{50})(\delta_i^0 \sim \delta_i^{50})(x_{50})). \quad (6)$$

Визначимо еквівалентні, ідентичні, схожі і несхожі ІО, що зберігаються по відношенню до вхідного ІО.

Якщо $\overline{\Pr} = 1$ и $M_\sim = \cap \overline{M}_i$ непорожня безліч, то $x \in M$ еквівалентні інформаційні описи

ВИСНОВОК

1. Показано, що семантична складова інформаційних станів ознак кібератак передбачає наявність певної семантичної метрики для її вимірювання та інтерпретації.

2. Ця метрика формально не зовсім раціонально визначена, неоднозначно інтерпретована та характеризуються невизначеністю в рамках нечіткості, наявністю семантичної інформації та неможливістю безпосереднього застосування відповідного заходу для визначення кластерів подібності інформаційних ознак станів.

3. Запропоновано підхід до ідентифікації нечітких інформаційних описів ознак кібератак та застосування методів поділу елементів реперних множин, на яких визначено ці інформаційні описи.

4. Показано, що результати процедури ідентифікації нечітких інформаційних станів ознак кібератак залежать від кластерів поділу реперних множин та показників семантичної невизначеності цих станів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.

18. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – Москва, 2006. – 197 с.