ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Науково-навчальний інститут комп'ютерних наук і технологій
Кафедра прикладної математики та інформатики

«До захисту допущено»
Завідувач кафедри ПМІ
_____ **О.А. Дмитрієва**
(підпис) (ініціали, прізвище)
«____»_____2020 р.

Випускна кваліфікаційна робота

магістра
(освітній ступінь)

на тему
«Аналіз особливостей застосування методів класифікації інформації в криптографії»

Виконав (-ла): студент (-ка) 2 курсу, групи ІПЗм-19
(шифр групи)

напряму підготовки (спеціальності) спеціальності 121 Інженерія програмного забезпечення
(шифр і назва напряму підготовки)

Дем'яненко Віктор Дмитрович _____
(прізвище та ініціали) (підпис)

Керівник доц. кафедри ПМІ, к.т.н., доц. Маслова Н. О._
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Нормоконтролер доц. кафедри ПМІ, к.т.н., доц. Назарова І.А._
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Покровськ – 2020

ДВНЗ «Донецький національний технічний університет»
Факультет Науково-навчальний інститут комп'ютерних наук і технологій
Кафедра прикладної математики та інформатики
Освітній ступінь магістр
Напрям підготовки (спеціальність) 121 Інженерія програмного забезпечення
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ /О.А. Дмитрієва/
«____»_____2020 року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Дем'яненку Віктору Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Аналіз особливостей застосування методів класифікації інформації в криптографії»
Спецчастина

Керівник роботи Маслова Н. О., к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від « 28 » вересня 2020 року № 727
2. Строк подання студентом роботи 11 грудня 2020 року
3. Вихідні дані до роботи результати переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) - 1) аналіз основ інформаційної безпеки та проблем, які вона вирішує
2) пошук прикладів застосування методів Data Mining в захисті інформації;
3) - систематизація методів класифікації інформації відносно застосування в криптології;
метрик та характеристик типових шаблонів; -
4) визначення критеріїв обрання методів класифікаціїї для розв'язання конкретних задач кібербезпеки;
5) оцінка ефективності методів та розробка структури таблиці для аналізу.
5. Перелік графічного матеріалу
робота містить 6 таблиць та 18 рисунків

-

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 3 вересня 2020 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури з предметної області	3.09.2020 – 27.09.2020	
2	Збір інформації і методичних відомостей щодо застосування методів класифікації у криптографії та криптоаналізі	28.09.2020 – 05.10.2020	
3	Розробка структури програмного забезпечення, вибір даних для обробки та експериментів.	06.10.2020 – 20.10.2020	
4	Тестування системи	21.10.2020 – 10.11.2020	
5	Оформлення пояснювальної записки	11.11.2020 – 30.11.2020	
6	Нормоконтроль пояснювальної записки, її перевірка антиплагіатною системою	01.12.2020- 12.12.2020	
7	Оформлення супутніх матеріалів (розробка графічного матеріалу, написання доповіді, тощо) та рецензування роботи	13.12.2020- 21.12.2020	
8	Захист роботи	22.12.2020	

Студент _____ Дем’яненко В.Д. .
(підпис) (прізвище та ініціали)

Керівник роботи _____ Маслова Н.О.
(підпис) (прізвище та ініціали)

А Н О Т А Ц І Я

Дем’яненко Віктор Дмитрович. Аналіз особливостей застосування методів класифікації інформації в криптографії / Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 121 «Інженерія програмного забезпечення». – ДВНЗ ДонНТУ, Покровськ, 2020.

Об’єкт дослідження - технології застосування методів класифікації для проведення криптографічного захисту інформаційних систем від комп’ютерних атак.

Предмет дослідження –методи класифікації в захисті інформаційних систем.

Метою роботи є аналіз застосування методів класифікації інформації в криптології та розробка програмного інструменту аналізу атак за допомогою Data Mining.

Методи досліджень базуються на сучасних положеннях криптології, теорії інформації, інтелектуального аналізу даних, сучасних застосуваннях в кібербезпеці та кібераналізі.

Наукова новизна полягає в створенні аналітичного огляду застосування сучасних методів класифікації в кібербезпеці.

Практичне значення полягає у можливості використання розробленого інструменту для допомоги дослідникам в обранні та використанні сучасних методів класифікації інформації, з метою проведення оперативного виявлення шкідливого програмного втручання, його нейтралізації та аналізу.

Ключові слова: криптологія, класифікація, data mining, інформаційна система, атака, мова Pyton.

ABSTRACT

Viktor Demianenko. Analysis of the peculiarities of applying information classification methods in cryptography / Graduation thesis for the degree of "master" in the speciality 121 "Software Engineering". - SHEI DonNTU, Pokrovsk, 2020.

The object of research is the technology of the application of classification methods for the cryptographic protection of information systems from computer attacks.

The subject of research is the methods of classification in the protection of information systems.

The work aims to analyze the application of information classification methods in cryptology and develop a software tool for analyzing attacks using Data Mining. Research methods are based on modern provisions of cryptology, information theory, data mining, modern applications in cybersecurity, and cyber analysis.

The scientific novelty is to create an analytical review of the application of modern classification methods in cybersecurity.

Practical significance consists in the possibility of using the developed tool for assisting researchers in the selection and use of modern methods of information classification for quickly identifying malicious software, its analysis, and neutralization.

Keywords: cryptology, classification, data mining, information system, attack, Python language.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DML - Detection Maturity Level

CTI - Cyber Threat Intelligence

ІБ - Інформаційна Безпека

ВД – великі дані

ASCII - семибітний код, стандарт для обміну інформацією

DES – алгоритм шифрування

AES – стандарт шифрування

ML - machine learning, машинне навчання

IR - information retrieval, інформаційний пошук

CybOX - Cyber Observable eXpression XML

STIX - Structured Threat Information Expression

TAXII - Trusted Automated eXchange of Indicator Information

IODEF - Incident Object Description and Exchange Format

IODEF-SCI - Structured Cyber Security Information

RID - Real Time InterNetwork Defense

OpenIOC - Open Indicators of Compromise

CPE - Common Platform Enumeration

CCE - Common Configuration Enumeration

OTX - Open Threat Exchange

CIRCL - The Computer Incident Response Center Luxembourg

MISP - Malware Information Sharing Platform

SVM - Support Vector Machine

IOC - Indicators of Compromise

ВСТУП

У сучасному світі інформація є одним із головніших ресурсів людської діяльності. Кожної хвилини, кожної секунди носії інформації поповнюються новими тисячами ексабайтів даних. Збір, передача та зберігання інформації стають важливими елементами роботи важливих підприємств. В той же час, зростає кількість спроб зловмисників незаконним чином отримати доступ до конфединційних даних. Тому унеможливлювання доступу правопорушників до інформації є важливою та актуальною задачею кіберпростору.

Одним з методів, котрі застосовуються при визначенні порушницьких дій є застосування методів Data Mining, зокрема, методів класифікації.

Data mining – це технологічний та науковий напрямок, який займається обробкою інформації з подальшим виявленням в ній, так званних, закономірностей і тенденцій. Вони, в свою чергу, можуть допомогти у підтримці прийняття певних рішень.

Об’єктом даної кваліфікаційної роботи є технології застосування методів класифікації для проведення криптографічного захисту інформаційних систем від комп’ютерних атак.

Предметом дослідження виступають методи класифікації в захисті інформаційних систем.

Загальною метою роботи є аналіз застосування методів класифікації інформації в криптології та розробка програмного інструменту аналізу атак.

Для досягнення поставленої мети намічено рішення наступних задач:

1) аналіз основ інформаційної безпеки та проблем, які вона вирішує;
2) пошук прикладів застосування методів Data Mining в захисті інформації;
3) систематизація методів класифікації інформації відносно застосування в криптології;

4) визначення критеріїв обрання методів класифікаціїї для розв’язання конкретних задач кібербезпеки;
5) оцінка ефективності методів та розробка структури таблиці для аналізу.

Основним методом дослідження є аналітичний підхід, аналіз застосування математичних алгоритмів методів класифікації інформації в криптології.

Кваліфікаційна робота складається з 4 розділів, включає 18 рисунків, 6 таблиць, 51 джерел інформації, загалом 81 сторінок.

РОЗДІЛ 1
ОСНОВИ КРИПТОГРАФІЇ Й КРИПТОАНАЛІЗУ

Поняття криптологія походить з грецьких kryptos («прихований») і logos («слово»). Вже більш ніж дві тисячі років тому люди почали замислюватися над тим, що треба захищати повідомлення від потрапляння їх в не ті руки. Впливові люди цього часу відсилали повідомлення з посильними. Була присутня велика невпевненість, чи досягнення посильний місці призначення, чи буде перехоплений ворогом. На випадок гіршого розвитку подій і були розроблені секретні шифри, тільки справжній отримувач знав ключі шифрування і міг зрозуміти написане.

Криптологія і захист даних у наш час, коли, наприклад через мережу Internet, пересилається велика кількість конфіденційної інформації є, без перебільшення, найбільш важливішою наукою останнього століття. Як і раніше, секретність інформації може бути ціною перемоги чи поразки, але, якщо тоді, це була поразка на полі битви, зараз, у більшості випадків, поразка передбачає отримання економічних збитків компанією, дані якою були вкрадені.

Метод захисту інформації, який досі вважається найбільш надійним, вважається шифрування – процес перетворення інформації, ціллю якого є приховання інформації від нелегітимних користувачів і, в той же час, можливість надавання інформації легітимним.

Безпека отримується за рахунок того, що легітимний користувач має можливість перетворити інформацію за допомогою секретного ключа або ключів. Результатом цього процесу є шифр, який неможливо зрозуміти або прочитати без секретного ключа. Шифр може бути розшифрований будь-ким, хто має доступ до ключа за допомогою якого відбувається і відновлення прихованої інформації. Секретність, хоча все ще є важливою функцією в

криптології, часто більше не є головною метою використання перетворення, і отримане перетворення може лише вільно розглядатися як шифр.

1.1 Основні поняття та задачі криптології, сучасні виклики

Криптологія – сучасна сфера знань, що складається з двох основних розділів – криптографії й криптоаналізу. Сучасна криптологія ґрунтується на сукупності фундаментальних понять математики, фізики, теорії інформації, складності обчислень [1].

Криптографією називають науку, яка використовує математичні методи для шифрування інформації. Це дає можливість зберігати секретну інформацію, чи передавати її через незахищені мережі, у тому числі Internet. Таким чином дані не можуть бути зчитані ніким, окрім законного отримувача.

Якщо криптографія це наука захисту даних, то криптоаналіз є наукою аналізу і подолання захисних комунікацій. Класичний криптоаналіз включає цікаві комбінації аналітичні міркування, застосування математичних інструментів, пошук шаблонів, терпіння, рішучість і вдача. На рисунку 1.1 відображена загальна схема криптології й її основні розділи.

Рисунок 1.1 - Загальна схема Криптології

Криптографія це давня наука, але з приходом інформаційного віку, комп’ютери підняли її на геть новий рівень. Конфіденційність та безпека в інтернеті важливіше, ніж будь-коли, залежать від шифрування та підтримки високих стандартів безпеки [2].

Терміни які найчастіше плутають і якими зловживають в криптології - це код і шифр. Навіть експерти час від часу використовують ці терміни, ніби вони є синонімами.

Код - це просто незмінне правило для заміни частини інформації (наприклад, букви, слова чи фрази) на інший об'єкт, але не обов'язково такого ж сорту; Азбука Морзе, яка замінює буквено-цифрові символи на символи з крапок і рисок, є звичним прикладом. Мабуть, найбільш широко відомим кодом, що використовується сьогодні, є Американський стандартний код для обміну інформацією (ASCII, рисунок 1.2).

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	TAB	LF	VT	FF	CR	SO	SI
1.	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2.		!	"	#	$	%	&	'	(	)	*	+	,	—	.	/
3.	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4.	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5.	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6.	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7.	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

Рисунок 1.2 - Таблиця значень кодів ASCII

Код працює на всіх персональних комп'ютерах і терміналах, він складається з 128 символів і таких операцій, як переведення рядка і повернення каретки у формі семи розрядних двійкових чисел - тобто, як рядок із семи одиниць та нулів. У ASCII мала літера «а» завжди дорівнює 1100001, а

великі літери «А «завжди 1000001 тощо. Скорочення також є широко відомими та вживаними кодами, як, наприклад, Y2K (для "2000 року") та COD (що означає "накладеним платежем") [3]. Іноді таке кодове слово досягає незалежного існування, тоді як оригінальна еквівалентна фраза забута - наприклад, модем, який спочатку називався «модулятор - демодулятор».

Шифри, як і у випадку з кодами, також замінюють частину інформації (елемент відкритого тексту, який може складаються з букви, слова або рядка символів) іншим об’єктом. Різниця в тому, що заміна відбувається згідно з правилом, визначеним секретним ключем, відомим лише передавачу та законному приймачу, це означає що сторонній, не знаючи ключа, не зможе інвертувати заміну, щоб розшифрувати шифр. У минулому розмивання відмінностей між кодами та шифрами було відносно незначним. Однак у сучасних комунікаціях інформація часто кодується та шифрується так, тому важливо знати різницю. Наприклад, лінія супутникового зв'язку може кодувати інформацію в символах ASCII, якщо вона текстова, або, якщо це аналоговий сигнал, такий як мова, модулюється та оцифровується у двійковому кодуванні десяткової форми (BCD). Отримані кодовані дані потім зашифровуються в шифр за допомогою стандарту шифрування даних або розширеного стандарту шифрування (DES або AES). Нарешті, отриманий потік зашифрованих даних декодується, за допомогою кодів з виправленням помилок. Схематично робота алгоритму AES наведена на рисунку 1.3.

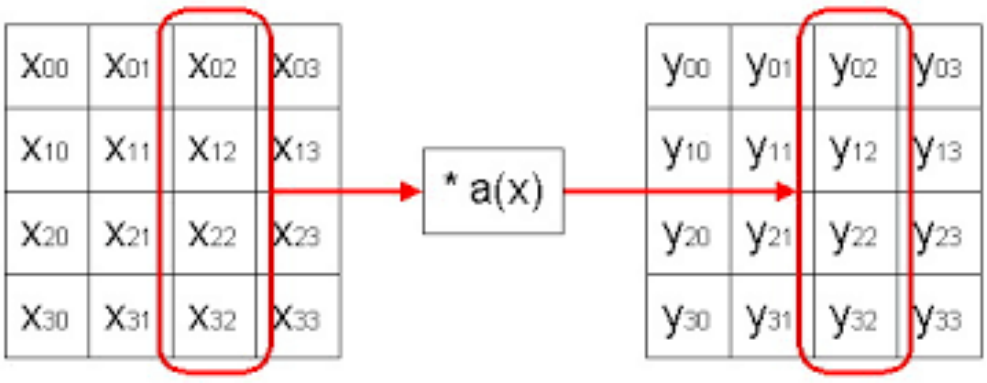


Рисунок 1.3 - Алгоритм шифрування AES

1.2 Етапи розвитку криптографії

У 1943 році два британські винахідники розробили Colossus, перший у світі цифровий електронний комп'ютер. Метою було допомогти в криптоаналізі та розшифровуванні німецьких повідомлень під час другої світової війни. В той час винахід значною мірою досяг своєї мети.

Шифр VIC використовувався радянськими шпигунами з 1953 року. VIC вважається найскладнішою модифікацією сімейства паролів Nihilist. Вважається одним із найсильніших паролів, які можна використовувати вручну без комп’ютера [4].

Розглянемо основні етапи розвитку криптографії (рисунок 1.4).

Рисунок 1.4 - Етапи розвитку криптографії у новітній історії

Обширні академічні дослідження криптографії були розпочаті відносно недавно, лише в середині 1970-х. Співробітники IBM розробили алгоритм, який став Федеральним стандартом кодування даних США.

В 1976 році Уітфілд Діффі та Мартін Хеллман опублікували свій криптографічний протокол, який зараз відомий як «протокол Діффі-Хеллмана».

Алгоритм RSA був опублікована в 1977 р. у рубриці Наукова Америка Мартіна Гарднера [5]. З тих пір шифрування широко застосовується в багатьох сферах, таких як комунікації, комп'ютерні мережі, інформаційна

безпека, банківська справа та електронна комерція. Деякі сучасні криптографічні методи можуть тримати свої ключі в секреті лише в тому випадку, якщо певні математичні питання не можуть бути вирішені такі як цілочисельне розкладання на множники або дискретні проблеми логарифму, тому існують глибокі зв'язки з абстрактною математикою.

Одна з сучасних систем криптографії, розроблена Філом Циммерманом у 1991 році [6]. PGP широко використовується для шифрування та розшифровування електронних листів, особливо через Internet. Віна також може автентифікувати повідомлення. AES (скорочення від Advanced Encryption Standard) - це симетричний алгоритм шифрування. Алгоритм був розроблений двома бельгійцями криптографами Джоаном Даменом та Вінсентом Рійменом. AES був розроблений, для того щоб використовуватися як в апаратному, так і в програмному забезпеченні, і підтримувати довжину блоку 128 біт та довжину ключів 128, 192 та 256 біт.

SHA-3 (Secure Hash Algorithm 3) - останній член сімейства стандартів Secure Hash Algorithm, випущений NIST у серпні 2015 року. Хоча алгоритм є частиною однієї серії стандартів, SHA-3 внутрішньо відрізняється від MD5-подібної структури SHA-1 та SHA-2.

Якщо звернутись до вітчизняної криптографії, то слід визначити розробку й затвердження українського стандарту шифрування, так званого шифру «Калина» [7]. А найсучаснішими розробками є застосування квантових обчислень у галузі криптографії [8,9].

1.3 Data Mining в кібербезпеці

Data Mining є популярною технологією, яка перетворює купу даних у корисні знання, які можуть допомогти користувачам чи власникам інформації робити зважений вибір і здійснювати розумні дії для власної користі. Зокрема, інтелектуальний аналіз даних шукає приховані закономірності серед величезних наборів даних, які можуть допомогти зрозуміти, передбачити та скерувати майбутні дії [10].

Тобто Data Mining - це набір методологій, які використовуються при аналізі даних з різних вимірів та перспектив, знаходячи раніше невідомі приховані закономірності, класифікації і групи даних, а також узагальнення виявлених стосунків.

Інтелектуальний аналіз даних - це, по суті, пошук шаблонів. Спеціалісти в Data Mining є експертами з використання спеціалізованого програмного забезпечення, яке допомагає знаходити закономірності у великих наборах даних. Ось є кілька конкретних застосувань у кібербезпеці, де може використатися інтелектуальний аналіз даних [11]:

- відфільтрувати дані з метою виділення реальних атак;
- визначати помилкові сигнали тривоги;
- знаходити аномальну активність, яка розкриває справжній напад.

Для виконання цих завдань спеціалісти використовують одну або декілька з наступних метод:

- узагальнення даних зі статистикою;
- візуалізація: подання графічного переліку даних;
- кластеризація даних за природними категоріями;
- пошук асоціаційних правил: визначення нормальної активності та використання досліджень, які дозволяють виявити аномалії;
- класифікація: прогнозування категорії, до якої конкретний запис належить.

Data Mining для програм кібербезпеки, наприклад, може використатися для виявлення аномалій, що допоможе виявити незвичайні дії та моделі. Аналіз посилань може бути використаний щоб простежити віруси до зловмисників. Класифікація може використатися для групування різних кібератак для подальшого попередження нових спроб нападу. Передбачення може бути використано для визначення потенційних атак у майбутньому.

Data Mining також застосовується для виявлення проникнення та аудиту. Архітектра однієї з систем виявлення проникнень з застосуванням Data Mining відображена на рисунку 1.5 .

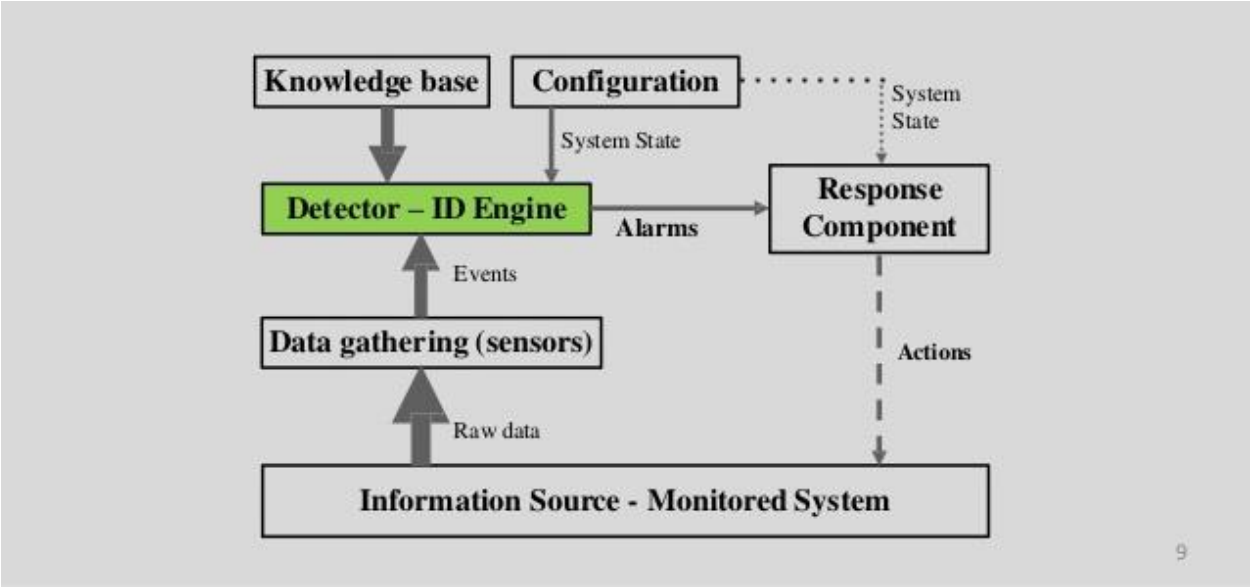


Рисунок 1.5 - Архітектура системи виявлення проникнень

Звичайний підхід до захисту комп’ютерних системи проти кіберзагроз - це проектування таких механізмів, як брандмауери, засоби автентифікації та віртуальні приватні мережі, що створюють захисний щит. Однак ці механізми майже завжди мають уразливості. Вони не можуть захистити від атак, які постійно пристосовуються для використання слабких місць системи, які часто з’являються через недбале проектування та недоліки впровадження. Це створило потребу в впровадженні системи виявлення вторгнень, технологія безпеки, яка доповнює звичайні підходи до безпеки за допомогою систем моніторингу та виявлення комп'ютерних атак. Традиційні методи виявлення вторгнень базуються на обширних знання експертів про сигнатури атак. Сигнатури мають кілька обмежень. Вони не можуть виявити нові напади, тому що хтось повинен переглянути базу даних сигнатур вручну для кожного нового виявленого типу вторгнення. Ці обмеження призвели до зростання інтересу до виявлення вторгнень які базуються на Data Mining [12].

1.4 Висновки за розділом

Таким чином, в розділі розкриті основні поняття об’єкту дослідження, а саме - сутність криптології як науки та її основних розділів – криптографії та криптоаналізу.

Наведено основні етапи розвитку криптографії, показано вітчизняний вклад в розвиток криптографії, пов’язаний з розробкою шрифту «Калина». Вказано, що одним з сучасних напрямків розвитку криптології є застосування відносно нових технологій інтелектуального аналізу та квантових обчислень.

Наприкінці розділу аналізуються задачі інтелектуального аналізу даних та їх застосування у кібербезпеці. Наголошується, що для рішення значної кількості задач кібербезпеки застосовуються методи статистичної обробки, візуалізації, кластеризації, пошуку асоціацій та класифікації, котрі є предметом подальшого дослідження у даній роботі.

РОЗДІЛ 2
ЗАСТОСУВАННЯ МЕТОДІВ КЛАСИФІКАЦІЇ В КІБЕРБЕЗПЕЦІ

2.1 Огляд методів класифікації

Кібербезпека – багатопрофільна дисципліна, в якій застосовуються моделі й методи різних наукових напрямків. Поширені застосування в кібербезпеці моделей й методів статистики, теорії чисел, модульної арифметики, інтелектуального аналізу даних й багатьох інших [13]. Предметом даної роботи є аналіз застосування базових методів одного з напрямків Data Mining, а саме методів класифікації у криптології.

Класифікація – це процес групування об’єктів, котрими є результати дослідження або спостереження відповідно до їх загальних ознак, визначення відношення об’єкту, що розглядається, одному або декільком класам. В результаті розробленої класифікації створюється класифікаційна система

До задач, що вимагають застосування методів класифікації у кібербезпеці відносяться:

- виявлення прихованих кореляцій, зв’язків між подіями;
- дослідження мережних структур, виявлення неправомірних підключень;
- моніторинг соціальних мереж, форумів, блогів, пошук недоброчинного контексту;
- аналіз різноманітних баз даних, пошук нехарактерних записів;
- виявлення спільної участі суб’єктів у проведенні групових дій;
- виявлення поведінкових тенденцій та аномалій;
- обробка текстових, графічних, звукових файлів аналіз вмісту;
- розпізнавання обличь та біометрична ідентифікація.

Стандартна постановка завдання класифікації полягає в наступному [14]. Досліджується деяка множина об’єктів D. Об’єкти цієї множини описуються деякою системою ознак. Передбачається, що множину D можна

представити у вигляді об’єднання непересічних підмножин (класів) $K_1, \dots K_i$. Крім того, нехай є скінченний набір об’єктів $S_1, \dots S_m : \{S_i\} \in D$, і відомо, яким класам вони належать. Набір об’єктів S_i називається прецедентами або навчальними об’єктами. Потрібно по введеному набору значень ознак об’єкта визначити, до якого класу він належить.

Якщо інформація цілочисельна й кількість припустимих значень кожної ознаки незначне, успішно застосовуються методи, засновані на комбінаторному аналізі ознакових описів об’єктів. При конструюванні цих методів використовується апарат дискретної математики, булевої алгебри, теорії диз’юнктивних нормальних форм, булевих і цілочисельних матриць. Особливістю процедур класифікації є можливість отримання результату за відсутності інформації про функції розподілу значень ознак і за наявності малих навчальних вибірок.

Методи класифікації лежать на стику двох областей – машинного навчання (machine learning, ML) та інформаційного пошуку (information retrieval, IR) [15-17].

Слід поширених та найбільш часто застосовних моделей рішення задач класифікації слід назвати бінарну та лінійну моделі, метод байєсовської логістичної регресії, метод опорних векторів.

Байєсовська модель. ЇЇ застосування у кібербезпеці вперше описав Клод Шенон в історичній роботі «Теорія зв'язку в секретних системах» [18]. У статті Шеннона вперше були визначені фундаментальні поняття теорії криптографії. До них відноситься, наприклад, доказ досконалої криптостійкости шифру Вернама. Необхідна і достатня умова для того, щоб система була цілком таємною, записується за допомогою теореми Байєса. Вважається, що саме з появою цієї статті криптографія почала розвиватися як наука. Поняття відстані єдності, ідея створення шифрів на основі декількох циклів заміни і перестановки, що є базою симетричних алгоритмів - в основі кожного з перерахованих вище понять лежить теорія Байєса [19]. Зараз Байєсовськи методи в криптографії застосовуються для передбачення атак, виявлення

погроз, визначення ризиків. На основі байєсівського аналізу в кібербезпеці прогнозують події, фільтрують сильно зашумлені дані, в яких є сигнали певної форми, оцінюють параметри, порівнюють моделі [20].

Другий напрямок – застосування методу опорних векторів, або Support vector machines (SVM), описаний в роботах В. Н. Вапник [21]. Метод опорних векторів - призначено для розв'язання задач класифікації й є, по-суті, математичним методом побудови моделі поведінки користувачів та виявлення можливих порушників з можливістю отримання функції, яка описує цей процес [22]. Метод опорних векторів застосовується при виявленні аномальної поведінки, виділення сигнатур атак, в системах антивірусного захисту [23]. Метод добре зарекомендував себе й в задачах біометричної ідентифікації при розпізнаванні обличь. Є приклади його застосування в задачах текстової класифікації для розпізнавання документів й ідентифікації особи. Метрична віддаленість від геометричного центру векторів-ознак подій комп'ютерної мережі - одна з характеристик, яка застосовується для визначення небажаного або зловмисного програмного забезпечення з використанням цього методу [24].

У другій частині розділу розглянуто особливості проведення семантичного аналізу й класифікаторів машинного навчання для оцінювання якості систем захисту інформації різного рівня.

Третій пункт розділу – застосування задач класифікації для виявлення проникнень

Потужним інструментом для виявлення кібератак є аналітика великих даних, котра неможлива без застосування алгоритмів класифікації.

При сучасних технологіях і швидкості кібератак виникає гостра потреба передбачати атаки і розпізнавати їх по найбільш раннім ознаками. Threat Intelligence - одна з таких технік, що дозволяє дізнаватися про погрози до того, як вони реалізувалися і спричинили шкоду. Цей напрямок носить назву відстеження загроз, являє собою знання про загрози, отримані

в результаті аналізу та інтерпретації даних. Напрямок Threat Intelligence описано в п'ятій частині даного розділу.

2.1.1 Байєсова модель

Байєсова модель вважається ймовірнісним методом класифікації. Оцінюється ймовірність, яка є умовною, того, що об’єкт належить до класу C, водночас цим, він має ознаки $F_1, \dots, F_n$:

$$P(C|F_1, \dots F_n).$$

І, за теоремою Байєса:

$$P\left(C\middle|F_{1,} \dots, F_n\right) = \frac{P(C)P(F_1,\dots,F_n|C)}{P(F_1,\dots,F_n)}.$$

За визначення ймовірності (при $P(F_1, \dots, F_n) \equiv 1$):

$$P(C|F_1, \dots, F_n) = P(C)P(F_1, \dots, F_n|C) = P(c)P(F_1|C)P(F_2, \dots, F_n|C, F_1)$$
$$= P(c)P(F_1|C)P(F_2|C)P(F_3, \dots, F_n|C, F_1, F_2).$$

За байєсовим підходом передбачається, що F_i, F_j є незалежними для будь-яких $i \neq j$:

$$P\left(F_i\middle|C, F_j\right) = P(F_i|C).$$

Відповідно:

$$P(C|F_1, \dots, F_n) = P(C)P(F_1|C) \cdot \dots \cdot P(F_n|C) = P(C)\prod_{i=1}^{n} P(F_i|C).$$

При класифікації об’єктів, у разі бінарної класифікації ймовірність Байеєса визначається за формулою:

$$P(D|C) = \prod\prod P(w_i|C).$$

За теоремою Байеса:

$$P(C|D) = \frac{P(C)}{P(D)}P(D|C).$$

Якщо класифікація відбувається лише за двома класами, наприклад, C і $\bar{C}$, то за формулою Байєса, отримаємо:

$$P(C|D) = \frac{P(C)}{P(D)}P(w_i|C),$$

$$P(C|D) = \frac{P(C)}{P(D)} P(w_i|\bar{C}).$$

Критерієм, який використовується для розуміння того, що об’єкт має приналежність до категорії, використовується відношення ймовірності, неприналежності і приналежності до класу С, яке розглянуте нижче.

$$\frac{P(C|D)}{P(\bar{C}|D)} = \frac{P(C)}{P\bar{C}} \prod_i \frac{P(w_i|C)}{P(w_i|\bar{C})}.$$

Але на практиці частіше відбувається використання логарифму відношення ймовірності:

$$\ln \frac{P(C|D)}{P(\bar{C}|D)} = \ln \frac{P(C)}{P(\bar{C})} + \sum \ln \frac{P(w_i|C)}{P(w_i|\bar{C})}.$$

Особливості застосування методу класифікації Байєса будуть продемонстровані у третьому розділі.

2.1.2 Метод опорних векторів

Найчастіше зараз використовується метод опорних векторів, який відноситься до граничних методів класифікації. Його суть полягає в тому, що визначається приналежність об’єктів за допомогою меж областей. В нашому випадку розглядатиметься лише бінарна класифікація. Нехай, кожний об’єкт класифікації буде вектором в N-вимірному просторі, а кожна векторна координата являється деякою ознакою , і чим більше ознака виражена в об’єкті, тим більша його величина.

З використанням лінійного класифікатора можна легко вирішувати задачі класифікації. Відбувається пошук гіперплощини в N-вимірному просторі, який займається відокремленням всіх точок одного класу від точок іншого. У випадку, коли вдається знайти таку пряму, завданням класифікації стає визначення взаємних розташувань точок і прямих. Якщо точка лежить зверху гіперплощини, то вона є частиною класу С, якщо знизу – іншого класу.

До недоліків цього методу класифікації можна віднести:

- неможливість знаходження поділяючої смуги у більшості випадків;
- лише граничні точки мають значення при пошуку поділяючої смуги;

- трапляються випадки з малою кількістю параметрів для налаштування;

- відсутність чітко сформованих критеріїв вибору ядра;

- система класифікації навчається доволі повільно;

В той же час, до переваг можна віднести наступні твердження:

- є кращим методом на тестах з масивами документів;

- якщо обирати різні ядра, можна користуватися іншими підходами;

- підсумкове правило вбирається за допомогою деяких цільових функцій, а з використанням експериментальної евристики [25].

2.1.3 Лінійна та бінарна класифікація

У бінарній класифікації може існувати лише дві категорії, які, при цьому, не перетинаються. За допомогою цієї класифікації розв'язується велика кількість задач, наприклад, класифікація за множиною критеріїв $C = \{c_1, \dots, c_M\}$розбиваємо на M бінарних класифікацій $\{c_i, \overline{c_i}\}$

Є доволі частим використання ранжування, при якому множиною значень цільової функції є відрізок [0, 1]. Важливим моментом бінарної класифікації є те, що два класи звичайно не симетричні як за обсягом відмінних наборів даних з кожного класу, так і за наслідками помилкової класифікації. При ранжуванні об'єкт може відноситися відразу до декількох категорій з різним ступенем приналежності, а не тільки до однієї. При цьому категорії можуть перетинатися між собою.

Задача класифікації є предметом розгляду в машинному навчанні методом навчання з учителем. Задача навчання з учителем полягає у визначенні відомих категорій для нових спостережень. Коли таких категорій всього дві, то це статистична бінарна класифікація.

Для автоматизованого вирішення задач бінарної класифікації часто застосовують такі методи, як, наприклад, дерево рішень, random forest, баєсову мережу, опорні вектори, штучну нейронну мережу, логістичну регресію [26 - 28].

Якість класифікатора залежить від предметної області та від кількості спостережень, розмірності вектору ознак, шуму в даних та багатьох інших факторів.

Бінарний класифікатор можна назвати лінійним класифікатором, якщо він приймає рішення про приналежність документа класу за допомогою порівняння лінійної комбінації ознак з визначеним граничним значенням. При відображенні на площині лінійним класифікатором є пряма лінія. Загальний функціональний вигляд лінійних класифікаторів такий: $w_1x_1 + w_2x_2 = b$. Правило класифікації за допомогою лінійного класифікатора полягає в тім, що документ відноситься до класу c, якщо $w_1x_1 + w_2x_2 > b$, і до класу $c^\wedge$, якщо $w_1x_1 + w_2x_2 \leq b$. Тут $(x_1, x_2)^T$ - двовимірне векторне представлення об'єкта, а $(w_1, w_2)^T$ — вектор параметрів, що разом з числом b визначають поділяючу межу.

На перший погляд, лінійна класифікація виглядає тривіальною. Однак навчання лінійного класифікатора пов'язане із значними складнощами. До лінійних методів, відносяться такі, як метод Роккіо і наївний байєсівський метод [29].

2.2 Семантичний аналіз в кібербезпеці

Модель зрілості виявлення кіберзагроз була запропоновано Райаном Стілліонсом. Модель DML (рис. 2.1) наголошує на зростанні рівню абстракції при виявленні кібератак, де передбачається, що спеціалісти з малим досвідом і вмінням зможуть виявляти атаки до того як ті встигнуть нанести великої шкоди мережі, але при цьому не маючи розуміння технічних подробиць і методів з допомогою яких атака була проведена. З іншого боку, передбачається що спеціалісти з високою досвідом роботи та навичками зможуть за допомогою технічних спостережень виявити тип атаки, використані методи та, можливо, особу зловмисника .

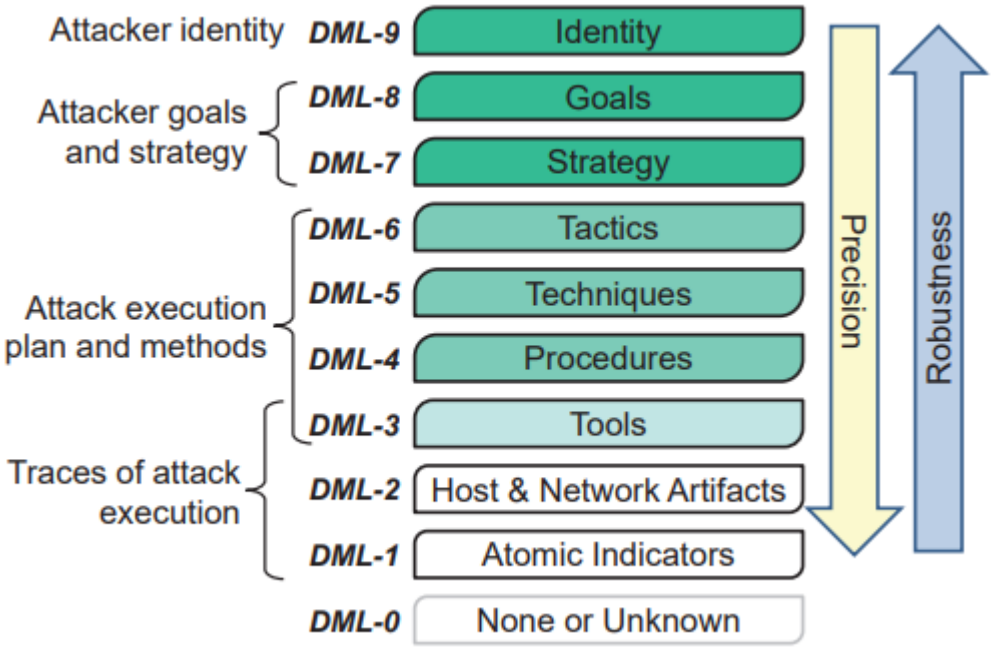


Рисунок 2.1 - Модель DML

При цьому DML-0 означає «Немає або невідомий» - відсутність команди реагування на інциденти.

DML-1 означає «Показники компрометації» - це елементарні частини артефактів хосту та мережі, які могли бути отримані від інших сторін. значення атомних показників компромісу обмежене через коротку «термін зберігання» цього типу інформації.

«Артефакти хосту та мережі» DML-2. Це тип інформації, який може бути зібраний мережею та датчиками кінцевої точки. При високій пропускній здатності посилань кількість зібраної інформації може бути приголомшливою і вимагає хороших аналітичних інструментів для аналізу та розуміння нападу на вищих рівнях абстракції.

«Інструменти» DML-3. Зловмисники встановлюють і використовують інструменти всередині мережі жертв. Інструменти часто змінюються, так що інструменти виявлені та проаналізовані під час попереднього інциденту безпеки може бути подібними, але не зовсім однаковими у нових атаках. DML-3 означає, що захисник може надійно виявити інструменти зловмисника, незалежно від незначних змін функціональних можливостей інструменту, або

відмінності в артефактах та показниках компрометації, залишених інструментом.

«Процедури» DML-4. Виявлення процедури означає виявлення послідовності двох або більше кроків, які використав зловмисник. Тут мета - ізолювати дії, які зловмисник виконує послідовно, два або більше разів під час інциденту.

«Методи» DML-5. Методи - це специфічні способи виконання окремих кроків атаки.

«Тактика» DML-6. Виявити тактику означає зрозуміти як розроблено та здійснено атаку, тобто знати методи, процедури та інструменти, що були використані.

«Стратегія» DML-7. Це нетехнічний високорівневий опис запланованої атаки. Є кілька різних способів за допомогою яких зловмисник може досягти своїх цілей, і стратегія визначає, який підхід слід застосовувати.

«Цілі» DML-8. Мотивація нападу може бути описана як мета. Залежно від того, як зловмисник організований, ціль може бути невідомою для команди, яка виконує атаку, команда може отримати лише стратегію, якої слід дотримуватися.

«Ідентифікація» DML-9. Особою зловмисника або агентом загрози, може бути ім'я особи, організації або держави. Іноді ідентичність може бути лише пов'язана з іншими атаками без будь-яких інших ознак хто вони або звідки вони працюють. Особистість зловмисника може не мати значення для захисника, якщо він хоче лише вивести зловмисника з мережі. Однак часто буває важливим мати можливість прив’язати кілька атак до одного і того самого виконавця, щоб передбачити стратегію, тактику, методи та процедури, які можуть бути використані.

Завдання полягає у використанні спостережуваних ознак атаки, виявлених на низьких рівнях, для визначення похідних причин на більш високих рівнях. Припустимо, що дана компанія В має за мету перемогти компанію А на відкритому ринку. Ця мета може змусити компанію В

використовувати неетичні засоби зі стратегією викрадення секретної інформації у компанії А з метою вдосконалення власної продукції та позиції на ринку. Тактикою компанії В може бути отримання доступу на внутрішні сервери компанії А на основі плану атаки з використанням методів, процедур та інструментів. Нарешті, виконання плану призводить до того, що сліди нападу залишаються в мережі жертви А.

Команда реагування на кібернетичні події спочатку виявляє сліди, звідти треба спробувати з'ясувати, що сталося і тоді прийняти відповідні дії. Сліди – є індикаторами, і завдання полягає в тому, щоб визначити, що насправді сталося, мати розуміння причин викрадення, тому можна використати індикатори як класифікатори для визначення характеру та походження нападу. Більшість команд реагування на аварії сьогодні працюють на рівнях DML-1 та DML-2. Деякі працюють на DML-3 і частково DML-6. Однак чим далі ви заходите, тим рідше отримуєте машиночитані результати від аналізу і іншої виконаної роботи, яка проводилась. Визначення семантичних моделей для типу інформації, зібраної на вищих рівнях моделі DML і відносини між ними дозволять більшій кількості команд підвищити рівень їх зрілості. Обмін інформацією також буде сприяти такому розвитку подій.

Виявлення справжньої природи загрози з урахуванням набору даних або інформації, яка вимагає семантичної моделі, щоб представити всі аспекти загроз без місця для неоднозначного результату. Чим далі ви підіймаєтесь по моделі DML, тим точніше можна зробити ідентифікацію. Чим далі вгору, тим дорожча спроба втручання для зловмисника і тим надійніший висновок ідентичності може стати. Обидва аспекти корисні для різних ролей та ситуацій протягом надзвичайного випадку. Інструменти управління інцидентами безпеки та управління подіями зазвичай використовують семантичне представлення артефактів хосту та мережі на нижніх рівнях моделі DML, але не часто використовують семантику подання аспектів високого рівня. Таким чином, необхідно стандартизувати семантичні подання аспектів високого

рівня у моделі DML. Це дозволить почати використовувати потенціал машинного навчання щоб робити передові аналітичні досліди у кібербезпеці.

Основна увага моделі DML полягає у вказанні рівнів зрілості при виявленні кіберзагроз. Однак та сама модель може бути використаний як основа для розробки класифікаторів кіберзагроз, називається ця нову модель класифікацією семантичних загроз. На рисунку 2.2 показана модель класифікації, яка складається з компактного представлення моделі DML у поєднанні з класифікаторами що представляють аналітичні взаємозв'язки, починаючи від особливостей низького рівня до особливостей високого рівня.

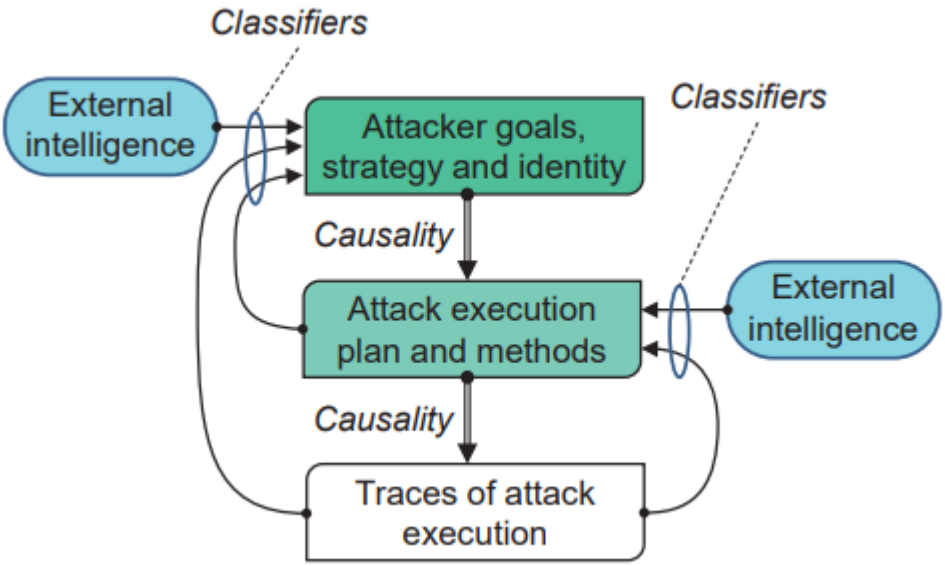


Рисунок 2.2 - Модель семантичної класифікації

Треба звернути увагу, що існують причинно-наслідкові зв’язки функції високого рівня і функцій низького рівня. Отже, класифікатори звикли міркувати в протилежному напрямку до причинно-наслідкових зв’язків.

У машинному навчанні та статистиці класифікатори звикли визначити категорії, до яких належить якесь спостереження, на основі навчального набору даних, що містить спостереження, приналежність яких до категорії відома. Для аналітики кібербезпеки класифікатор може, наприклад бути

використаним для співвідношення набору мережевих артефактів з певною ціллю зловмисника, або, навіть особистістю.

Контекстна інформація також може використовуватися як вхідна інформація показників для класифікаторів. Контекстною інформацією може бути, наприклад, політичні події, що з'являються у ЗМІ. Політичний конфлікт між національними державами може підвищити ймовірність запуску державами конкретних типів кібератак один проти одної

Завдання для розробки надійних класифікаторів полягає у визначенні відповідних семантичних ознак та їх змінних на кожному рівні абстракції та у забезпеченні достатньої кількості і типів даних для того, щоб дати класифікаторам достатнє навчання для надійного виявлення та класифікації.

Класифікатори машинного навчання розроблені в значній мірі залежно від статистичних методів, і автори вказують на важливість математики у кібербезпеці [30].

2.3 Виявлення проникнень з Temporal Logic Based Framework

Автори наступної розробки пропонують базове програмне забезпечення, Logic Based Framework, як основу для виявлення вторгнень. Робота системи базується на моніторингу часу виконання специфікацій часової логіки. Шаблони вторгнень визначено як формули у основі системи.

Система підтримує значення даних та параметризовані рекурсивні рівняння і дозволяє лаконічно виражати атаки безпеки за допомогою складних шаблонів часових подій, а також атаки, підписи яких за своєю суттю є статистичними [31].

При роботі Logic Based Framework використовується алгоритм онлайн-моніторингу. В якості базової ситуації обрана специфікація відсутності атаки. Порушення специфікації викликає сигнал тривоги.

Автори представляють реалізацію системи, яку вони назвали MONID, і демонструють результати, отримані при її застосуванні для виявлення таких

атак, як Smurf attacks, Cookie-Stealing Scenario, Multi-domain Buffer Overflows, Password guessing Attack.

Автори вважають, що їх приклади є загальними і можуть бути використані як шаблон для зазначення великої кількості інших атак.

Планується проведення систематичного дослідження ефективності використання системи, й дослідження сформульованих ідей для прогнозування збоїв безпеки в багатопотокових програмах.

2.4 Big Data в кібербезпеці

Аналітика великих даних швидко стає незамінним інструментом у нашому все більш цифровізованому суспільстві. Вона використовується не лише великими корпораціями для допомоги прийняття рішень, але і для багатьох інших дисципліни, включаючи штучний інтелект, дослідження, пов'язані зі здоров'ям, та безпекою інформації.

Важливість аналізу великих даних пояснюється простими прикладами, для визначення даних про місцезнаходження в режимі реального часу зі смартфона користувачів, скільки покупців було у торгових центрах на чорну п’ятницю чи на початку Різдва. Потім ці дані дозволяють аналітикам оцінити обсяги продажів ще до того, як були зафіксовані фактичні продажі.

Крім того, у поєднанні з алгоритмами машинного навчання великі дані використовуються для створення систем штучного інтелекту, які краще виконують завдання, які раніше могла б зробити тільки людина. Типовий приклад – Watson компанії IBM, який здолав найкращі розуми у грі Загроза в 2012. Інший приклад машинного навчання - автомобілі без водія; хоча ці машини ще не перевершили людей, тести, на певних вибраних дорогах, показують що ці машини освоїли складне мистецтво водіння.

Справа в тому, що аналітика великих даних може надавати потужний інструмент організаціям для прийняття розумніших та кращих рішень, в свою чергу, це може давати кращу картину подій навіть до того, як ця подія сталася.

Це робить аналітику великих даних ідеальним та потужним інструментом для виявлення кібератак.

Під час виступу на конференції з кібербезпеки в 2012 році директор ФБР виступив з цілком незвичне твердження: «Я переконаний, що існує лише два типи компаній: ті, що були зламані, і ті, що будуть. На жаль, це сумна реальність у сучасному оцифрованому світі. Кібератаки стали настільки буденними, що організації навіть не дивуються, коли це трапляється».

Відповідно до звіту про, у 2015 році було виявлено понад 430 мільйонів нових шкідливих програм, а що ще більш неймовірним було в цьому звіті - те, що ця знахідка не стала несподіванкою для дослідників. У звіті про безпеку далі пояснюється цілеспрямовані, витончені та наполегливі напади на державні організації та підприємства різних розмірів зростають і породжують серйозна становити серйозну загрозу національній безпеці та економіці [32].

Кібер-атаки бувають різних розмірів і форм - від поширених вірусів до дуже сильних, складних шкідливих програм, такі як кіберзброя. Найбільш вірогідними джерелами кібератак можуть бути звичайні незадоволені працівники, хактивісти та злочинні синдикати. У галузі інформаційної безпеки це сприймається як належне, з гарними причинами та доказами, що внутрішня загроза (діяльність працівників) представляє найбільшу загрозу (або ризик) для безпеки інформації в будь-якій організації, але останнім чином, як свідчать звіти, це змінюється. У звітах пояснюється, що зараз діяльність зовнішніх зловмисників значно частіше є джерелом загрози, ніж внутрішні загрози.

Зовнішні нападники включають злочинні синдикати, хакерів, що фінансуються державою, хактивістів та хакерів-самотники. Модус дії цих зловмисників включає використання дуже досконалого шкідливого програмного забезпечення, яке неможливо легко виявити навіть за допомогою настільки ж сучасної системи безпеки. Наприклад, під час нападу на Sony повідомлялося, що шкідливе програмне забезпечення, яке використовувалося, могло уникнути більшості мережевих захистів, які існують сьогодні.

З моменту появи Stuxnet, досить підступного та невидимого шкідливого програмного забезпечення, яке використовувалося для атаки на іранські ядерні об'єкти, все більше подібних типів таких шкідливих програм почали з’являтися в cybersphere. До відомих прикладів цих типів стелс-шкідливих програм, окрім Stuxnet, належать Duqu, Flame та Red October, які сумісно називають Virvilis та Gritzalis

Virvilis та Gritzalis описують як такі, що мають такі загальні риси: вони, як правило, спрямовані на конкретні та важливі цілі і, отже, для конкретних операційних систем або платформ; вони зазвичай, мають початковий вектор атаки, такий як зловмисний текстовий документ або знімні накопичувальні пристрої; вони оснащені багатьма методами ухилення від антивірусного програмного забезпечення та системи виявлення вторгнень; частина їхніх методів ухилення включає шифрування трафіку їх мережі, вони використовують викрадені, але законні цифрові сертифікати, що обманюють цільові системи.

Ці особливості дуже ускладнюють роботу з виявлення навіть загартованих і складних систем. Таким чином, їх виявлення в значній мірі залежить від проведення ручних розслідувань та досвіду людських аналітиків.

Було запропоновано використовувати аналітику великих даних для виявлення кібератак. Організації можуть видобувати величезні обсяги даних, які вони збирали під час потенційних подій кібербезпеки, таких як шкідливе програмне забезпечення та спроби фішингу.

Для проведення аналізу великих даних використовується цілий ряд технологій (рис. 2.3). Загальне консенсус серед більшості експертів у цій галузі полягає в тому, що явище великих даних є перспективним методом і, здається, це підтримується цілим набором технологій, які включають зберігання додатків, алгоритми машинного навчання для аналітики та користувальницькі інтерфейси, все це з'являється на ринку вже сьогодні.

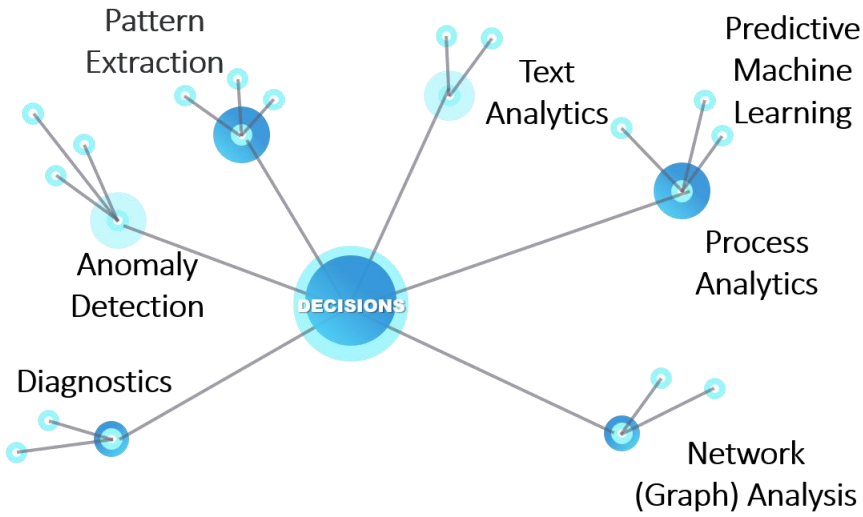


Рисунок 2.3 - Методи аналітики в Big Data

Форум з інформаційної безпеки склав звіт про потенційний позитивний вплив та вдосконалення аналітики великих даних щодо інформаційної безпеки. У звіті зазначено, що організаціям потрібно відійти від реагування на випадки кібератак і рухатись у напрямку виявлення та запобігання подібним інцидентам. Звіт робить висновок, що хоча поточна аналітика великих даних може бути використана для підвищення інформаційної безпеки зменшуючи ризики та підвищуючи швидкість реагування, технологія не зовсім зріла галузі інформаційної безпеки.

З багатьох переваг аналітики великих даних найбільш переконливою є операційна ефективність. Можна стверджувати, що ця "Операційна ефективність" включає виявлення кібератак, оскільки забезпечення безпеки системи є частиною діяльності організацій. Крім комерційних організацій, аналіз великих даних може бути корисним урядам для виявлення загроз з боку іноземних країн, терористів, хактивістів та злочинних елементів у реальному світі кіберпросторі. Оскільки інформація, отримана від аналітики великих даних має велике значення для організації, яка її отримала, це неминуче буде мішенню для кібератак, але сама аналітика великих даних також може бути використана для запобігання таким атаки. Іншими словами, аналітика великих

даних може використовуватися організаціями для збільшення продуктивності і одночасно роблячи свої системи більш безпечними.

Щоб підвищити ефективність аналітики великих даних, засоби контролю доступу повинні бути віддалені від області мережі і ближче до ресурсу даних, які потребують захисту.

Ідея аналізу виявлення кібератак не є новою, вже протягом багатьох років спільнота інформаційної безпеки здійснює моніторинг мережевого трафіку, аналіз системних журналів та інших джерел даних з метою виявлення загроз та зловмисних дій, але використання аналітики великих даних є кращою альтернативою, вона подолала багато викликів, з якими стикалися традиційні засоби аналізу даних з моніторингу мережевого трафіку, журналів безпеки тощо.

Один із цих викликів полягає в нездатності проводити довгострокову та широкомасштабну аналітику, оскільки це було б не економічно можливо зберігати великі обсяги даних протягом тривалого періоду. Одне з основних нововведень в технології великих даних полягає у сприянні розвитку доступної інфраструктури, такої як зберігання та обслуговування для моніторингу безпеки різними галузями, що робить можливим проведення масштабної аналітики. Незважаючи на значну перспективу аналітики великих даних щодо безпеки даних, існує декілька таких проблем, як закони про конфіденційність, які можуть перешкодити цьому розвитку. Аналітика великих даних не є панацеєю для кібербезпеки а, отже, фахівцям з безпеки доведеться продовжувати досліджувати нові засоби приборкання складних атак [32].

2.5 Threat Intelligence в кібербезпеці

Основне питання, яке слід поставити, коли ми хочемо зрозуміти концепцію відомостей кіберзагроз "Що таке відомості?" Найпоширенішою роботою як посиланням для відповіді на це питання є ключовий документ Міністерством оборони США . На рисунку 2.4 [33], показано взаємозв'язок

між даними, інформацією та відомостями, який може привести до дієвих відомостей. Дієві відомості завжди повинені бути кінцевою метою в життєвому циклі розвідки для поліпшення кібербезпеки. Організаціям потрібно більше вкладати гроші в людських аналітиків, проводити аналіз та виробляти діючі відомості про загрози. Дієві відомості про загрози можуть надати достатньо інформації для прийняття обґрунтованого рішення, за допомогою якого можна вжити найбільш ефективних заходів.

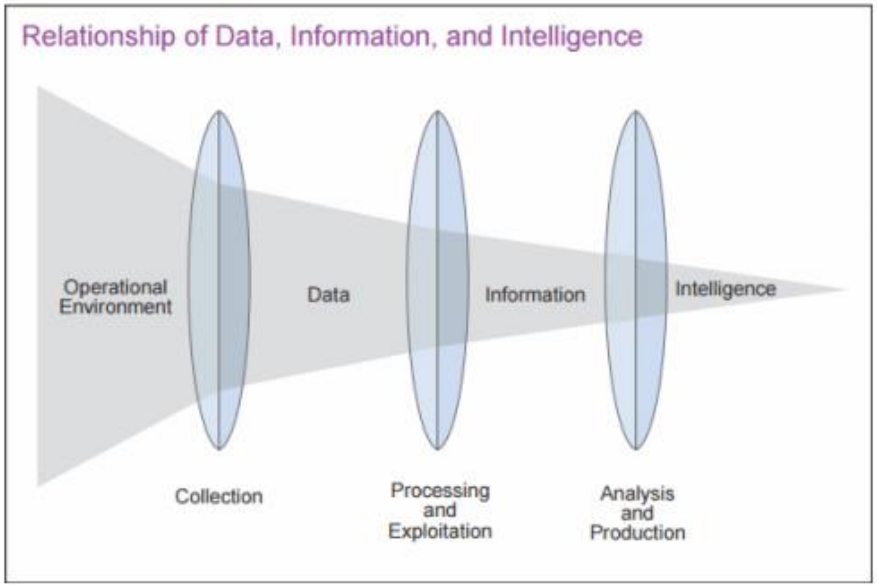


Рисунок 2.4 - Взаємозв'язок даних, інформації та інтелекту.

Існує величезна різниця між шумом, даними про загрози, інформацією та відомостями, розуміння цієї різниці є важливим для отримання максимальної віддачі від розвідувальної платформи загроз.

Дані складаються з основної, нерафінованої та, як правило, нефільтрованої інформації, яка зазвичай знаходиться в формі символів та сигналів, які можна зчитати. Символи включають слова (текстові та / або словесні), цифри, схеми, та зображення (нерухомі та / або відео), які є будівельними блоками комунікації. Тим часом сигнали включають датчики та / або сенсорні показання світла, звуку, запаху, смаку та дотику.

Інформація - це підготовлені дані, які були оброблені, узагальнені та організовані у більш зручний для людей формат, який забезпечує більше контекстів і корисна для певної форми аналізу.

Якщо описувати відомості з професійної точки зору як дані, які були вдосконалені, проаналізовані та оброблені, тому результати повинні бути відповідними, ефективними та цінними. Ці три вимоги можуть бути досягнуті шляхом проведення людиною логічного та аналітичного процесу, який може надати контекстні дані і мають корисний результат.

У контексті інформаційної безпеки, відомості описуються як діюча інформація або продукт життєвого циклу моделі відомостей, що включає декілька видів діяльності, таких як планування, збір, аналіз та розповсюдження даних. Однак більша частина організацій сьогодні в першу чергу зосереджується щодо збору даних та приділенні меншої уваги іншим заходам життєвого циклу відомостей. Основною метою відомостей є підтримка прийняття рішень або оперативних дій, таких як виявлення, запобігання та реагування.

Інструменти та канали даних самі по собі не можуть надати відомості про загрози без втручання людини для отримання відомостей з інформації та даних, відомості будь-якого типу вимагає аналізу. Аналіз проводиться людьми. Автоматизація, аналітика та різні інструменти можуть суттєво підвищити ефективність аналітиків, але вони завжди повинні бути аналітиками, які беруть участь у процесі.

Підсумовуючи взаємозв'язок даних, можна сказати, що дані, зібрані з оперативного середовища обробляються та вдосконалюється для отримання інформації. Потім інформація аналізується і перетворюється у дієвий формат, який називається відомостями.

В останні роки відомості про кіберзагрози (CTI) стала актуальною темою інформаційної безпеки (ІБ) але відсутність огляду літератури щодо роз'яснення концепції змушують, як правило, використовувати своє власне визначення і може призвести до певної неясності. Існує багато різних

визначень для пояснення цього терміну. Як би неоднозначно це не було, відомості про кіберзагрози (CTI) можна комплексно визначити як доказові знання, які включають контекст, механізми, показники, наслідки та дієві поради, про існуючу або виникаючу загрозу, які можуть бути використані для інформування щодо прийняття рішень суб'єкта на цю загрозу чи небезпеку. У визначенні зазначено, що організація може приймати рішення щодо своїх дій у стратегічному, оперативному та тактичному рівнях за допомогою збору інформації, що містить деталі поточної чи нової загрози.

У той же час, інші спеціалісти пропонують кілька інших визначень для CTI, які базуються на операціях, аналізі та домені. Таким чином, вони визначили операції CTI як дії, вжиті кіберпростором для компрометації, захисту захищеної інформації та можливостей, доступних у цьому домені. В той же час часом, аналіз CTI – це аналіз цих дій, діючих обличь, інструментів та методів.

На основі Клопперта, CTI - це не лише фокус на державі, яка пов’язана з деякими техніками впливу на національну політику, воно більше стосується технічного аспекту, такого як інструменти та методи.

На противагу цьому Лі запропонував визначення поняття CTI, як процес і продукт, отриманий в результаті інтерпретації вихідних даних в інформацію, яка відповідає вимогам, що стосуються супротивника, який маює намір, можливість і здатність заподіяти шкоду. Зі свого дослідження Лі згадав що CTI включає процес перетворення даних на інформацію, що стосується супротивника.

На підставі розглянутих визначень, можна бачити, що визначення, дане Клоппертом, інтерпретує CTI не у вигляді використання для отримання переваги над супротивником, але цей противник також використовує його для отримання перевага перед захисником. Дане визначення також стосується більш технічних аспектів, таких як інструменти та методи. Порівняно з Лі, дане визначення стосується намірів і можливостей завдати шкоди.

Аналіз літератури показав, що для CTI не існує загальноприйнятого визначення. Дослідники схильні визначати цей термін, базуючись на своєму особистому робочому середовищі. Однак є кілька ключових моментів, які ми можемо отримати з будь-якого визначення, а саме контекст та елементи CTI. Контекст є опорою CTI. Без контексту CTI може легко стати некерованим потоком оповіщень. Контекст може дозволити аналітику безпеки зрозуміти тип загрози чи ідентифікувати особистість атакуючого, тому він може сформулювати відповідний план дій. Є три основні елементи CTI – ревелантність, своєчасність та дієвість. Повне визначення CTI повинне охоплювати ці три елементи, щоб переконатися, що зібрані відповіді дані про загрози, дані аналізуються та обробляються своєчасно, а результат дає дієву допомогу для сприяння прийняттю рішень.

Щоб полегшити та пришвидшити обмін розвідувальними даними між організаціями, потрібна структурована автоматизована система обміну інформацією. Завдяки цьому відбувається підвищення кількості розробок стандартів для передачі CTI, наприклад, CybOX, STIX та TAXII. Також значного розвитку зазнали системи автоматичного поширення CTI, наприклад, MISP, OTX [34]. На сьогоднішній день STIX розглядається як фактичний стандарт для опису даних CTI та широко використовується для обміну розвідувальними даними [35].

Існує безліч стандартів, які організація може адаптувати залежно від її конкретних потреб. MITER розробив три стандарти (CybOX, STIX, TAXII) як пакет, розроблений для роботи разом, кожен для різної потреби, в системі управління ІТК. CybOX - це скорочення від Cyber Observable eXpression XML. CYBOX характеризує хронологію та часовий діапазон між подіями. Схема XML CybOX використовується для представлення спостережень STIX, які описують кіберартефакти або події, такі як адреси IPv4, з декількома пов’язані об’єкти [36]. STIX - використовує словниковий запас CybOX описуючи інформації про кіберзагрози, щоб її можна було послідовно використовувати, зберігати та аналізувати.

Архітектура, що використовується в STIX, складається з дев'яти конструкцій, таких як спостереження, індикатори, інциденти, тактика, техніка та процедури, експлуатація цілі, напрямки дій, кампанії, учасники загрози та звіти. Найчастіше використовують такі індикатори, як IP-адреси для командних і консольних, та хеші шкідливого програмного забезпечення [37]. TAXII - це протокол з відкритим джерелом та спеціалізовані на тому, щоб дозволити обмінюватися CTI між організації. TAXII користується можливостями CTI, надаючи загальні, відкриті специфікації для передачі інформаційних повідомлень про кіберзагрози, з такими можливостями, як шифрування, автентифікація, адресація, оповіщення та запити, між системами в безпечному та автоматизованому способі [38].

MILE також розробив три стандарти як пакет, що складається з опису об'єкта інциденту та Формат обміну (IODEF), структурованої інформації про кібербезпеку (IODEF-SCI) та Мережевий захист у реальному часі (RID). IODEF, призначений RFC 5070, для нормалізації даних з різних джерел для людського аналізу та реагування на інциденти. Хоча IODEF-SCI виступає як розширення стандарту IODEF, що додає підтримку додаткові кількості даних та включає RID, який може використовуватися як стандарт зв'язку в CTI.

Mandiant також представив систему Open Indicators of Compromise (OpenIOC), яка може характеризувати статичну інформацію.

Тоді (VERIS), розроблений Verizon, дозволяє організаціям обмінюватися даними про події та бути частиною загальної вибірки даних кібератак.

З боку організацій та фахівців з безпеки зростає інтерес до збору даних розвідки про загрози та визначення способу обробки цих даних.. Однак без допомоги інструментів CTI, дані про загрози можуть стати некерованим потоком інформації. Через це багато компаній розробили інструменти, які можуть допомогти організаціям та спеціалістам керувати розповсюдженням інформацією про загрози.

Є два інструменти, які можна використовувати для номенклатури та словника, CPE для апаратного забезпечення та CCE захисту конфігурацій програмного забезпечення.

REN-ISAC представив систему колективного інтелекту (CIF) як систему клієнт / сервер для обміну даними CTI. CIF включає серверний компонент, який збирає та зберігає дані. Даними можуть бути IP-адреси, номери ASN, адреси електронної пошти, доменні імена та інші атрибути.

Alien Vault випустив Open Threat Exchange (OTX) для досліджень і розслідувань відкритих у загальному доступі. OTX може очищати, агрегувати та перевіряти щоб ділитися останніми даними, тенденціями та методами загроз.

McAfee Threat Intelligence Exchange представила послугу «витягування» описання, визначення вірусу або DAT-файлу, який містить актуальні вірусні сигнатури та іншу інформацію, яку використовують антивірусні продукти McAfee для захисту комп'ютерів Linux, Windows або Mac від шкідливого програмного забезпечення. Нові загрози з'являються кожен день, і McAfee постійно випускають нові DAT-файли.

Нарешті, є проект Центру реагування на комп'ютерні інциденти Люксембургу (CIRCL). Розроблена платформа обміну інформацією MISP [39]. Основна мета цієї надійної платформи полягає в тому, щоб дозволити збирати та обмінюватися важливими показниками цілеспрямованих атак, інформацією про загрози, такою як вразливості або фінансові показники, що використовуються у випадках шахрайства.

2.6 Машинне навчання в кібербезпеці

Алгоритми машинного навчання класифікується як контрольоване навчання або виявлення шаблону [40]. У навчанні під наглядом, там завжди є цільова змінна, значення яке модель машинного навчання вивчає, щоб передбачати події, використовуючи різні навчальні алгоритми, наприклад, на

основі розташування IP-адреси, частот веб-запитів та часу запитів. Модель машинного навчання може передбачити, чи була вказана IP-адреса частиною DDOS атаки.

До контрольованого навчання потрапляють наступні алгоритми машинного навчання: лінійна та логістична регресія, дерево рішень та SVM [41]. З іншого боку, у процесі навчання без нагляду немає передбачення цільової змінної, більш схоже на те, що некеровані алгоритми вчяться знаходити цікаві асоціації або шаблони в наборах даних, наприклад, ідентифікація комп'ютерних програм, таких як шкідливі програми з подібними операційними / поведінковими моделями з використанням алгоритмів кластеризації та асоціації.

Окрема галузь, в якій спостерігається широке поширення машинного навчання є кіберзлочинність та кіберзахист, де знайдеться багато завдань, які може вирішувати ця технологія, таких як аналіз логів, та шкідливого програмного забезпечення.

Зі зростанням загрози кібербезпеки дослідження зосереджують уваги на машинному навчанні, його широкому наборі інструментів та методах виявлення, зупинки та реагування на складні кібератаки. Машинне навчання можна використати в різних сферах кібербезпеки для забезпечення аналітичних підходів до виявлення та реагування на атаки[42].

Це може також покращують процеси безпеки шляхом автоматизації рутинних завдань і полегшити аналітикам безпеки швидку роботу з напівавтоматизованими завданнями.

Алгоритми машинного навчання можуть бути реалізовані в програмах для виявлення та реагування на кібератаки. Зазвичай це досягається за допомогою моделі розробленої шляхом аналізу великих даних, наборів подій безпеки та виявлених моделей дій зловмисників[43]. Як результат, коли виявляються подібні дії, вони виконуються автоматично.

Моделі набору навчальних даних зазвичай складаються з попередньо виявлених та зареєстрованих показників IOC, які потім використовуються для

побудови моделей і систем, які можуть контролювати, виявляти та реагувати на загрози в реальному часі.

Крім того, з наявністю наборів даних IOC, ми можемо використовувати алгоритми класифікації машинного навчання для ідентифікації різні типи поведінки шкідливих програм у наборах даних, та класифікують їх відповідно. Дослідження проводяться на поведінковій системі основи аналізу, яка використовують машинним навчанням щоб класифікувати та кластерізувати поведінки тисяч шкідливих програм. Це дає можливість використовувати вивчені моделі для автоматизації процесу виявлення та класифікації нових шкідливих програм[44]. Це може допомогти аналітикам з безпеки або інших автоматизованих систем, швидко виявити та класифікувати новий тип загрози та дати на неї відповідні контрзаходи. Наприклад, за використання історичного набору даних, що містять детальний опис події атаки вірусу Petya, модель машинного навчання може навчитися ідентифікувати подібні атаки, тим самим даючи можливість автоматизувати процес ідентифікації та реагування на подібні атаки.

Прийоми машинного навчання також можуть бути використані у класифікації трафіку IP, що допоможе автоматизувати процес виявлення вторгнень, які можуть використовуватися для виявлення поведінкових контрольних зразків, як у випадку з DDOS-атаки [45]. Зі збільшенням числа різних рішень для машинного навчання, дослідження були зосереджені на використанні декількох рішень машинного навчання для виявлення вторгнень в системи, включаючи одиночні, гібридні та ансамблеві[46].

Також машинне навчання може використовуватись у оцінці мережевих ризиків. Це стосується використання кількісних показників для оцінки ризику проникнення в різні розділи мережі, тим самим допомагаючи організаціям надавати пріоритет розподілу ресурсів під час побудови систем кіберзахисту. Машинне навчання може бути використано для автоматизації цього процесу шляхом аналізу історичних наборів даних про кібератаки та визначення, які області мережі в основному брали участь у певних видах атак.

Використання машинного навчання вигідне в тому сенсі, що отримані оцінки базуватимуться не лише на знаннях домену мереж, але найголовніше, можна буде отримати числову оцінку ризиків у вигляді певних балів. Ці бали можуть допомогти кількісно визначити ймовірність та вплив атаки на дану область мережі та можуть допомогти організаціям зменшити ризик стати жертвами нападів.

Машинне навчання може бути використано для автоматизації повторюваних завдань, що виконуються аналітиками безпеки під час роботи. Це можна зробити за допомогою аналізу записів або звітів про минулі дії, здійснені аналітиками з питань безпеки. Успішно виявивши та зреагувавши на певні атаки можна використати ці знання для побудови моделі, яка допоможе ідентифікувати подібні атакує і відповідно реагувати без участі людини.

Хоча важко автоматизувати повний процес безпеки і замінити людських аналітиків безпеки, є деякі аспекти аналізу, які машинне навчання може автоматизувати, включаючи виявлення шкідливого програмного забезпечення, аналіз журналу мережі та оцінки вразливості, таких як аналіз мережевого ризику.

З експоненціальним зростанням штучного інтелекту ми бачимо зростаючу кількість автоматизованих завдань, спокусливо думати, що штучний інтелект буде підвищувати автоматизацію певних завдань, які в даний час виконує людина. Це може здійснитися вже зараз, однак є чисельні випадки, коли поєднання штучного інтелекту та інтелекту людини дають набагато кращі результати, ніж кожен сам по собі. Саме з цієї причини зараз спостерігається зростання компаній зі штучним інтелектом з акцентом не тільки створення продуктів штучного інтелекту для автоматизації завдань, але й створення продуктів, що підвищують і доповнюють продуктивність аналітиків. Відомий приклад такої компанії є Palantir, який створює продукти, що полегшують аналітику для збору та використання величезних обсягів даних [47]. Для посилення діяльності аналітиків з безпеки, були проведені дослідження з використанням алгоритмів машинного навчання, таких як

генетичні алгоритми, які намагається створювати програми, що генерують правила класифікації мережі з'єднання [48].

Інші підходи стосуються реалізації когнітивної архітектури для створення автоматизованої системи кіберзахисту, системи прийняття рішень на експертного рівня, натхненна тим як люди міркують і вчяться. Аналітикам з кібербезпеки як правило, доводиться витрачати час, відповідаючи на кілька подій, які іноді включають помилкові спрацьовування, які здебільшого обертаються порожньою втратою час [49]. Проведені дослідження показали, що класифікатори машинного навчання можна тренувати за попередніми даними для виявлення та розрізнення помилкових спрацьовувань, тим самим даючи можливість створити автоматизовану система, яка буде попереджувати аналітиків лише про сценарії які включають справжні спроби атак [50].

2.7 Висновки за розділом

У другому розділі наведено огляд методів класифікації та можливості їх застосування в кібербезпеці. Зокрема, це байєсовська модель, яка застосовується для передбачення атак, при виявлені загроз і визначенні ризиків. Другий – метод опорних векторів, який допомагає при виявленні аномальної поведінки сигнатур атак і біометричній ідентифікації. Крім того, розглянуто метод лінійної та бінарної класифікації, згадано метод Rocchio.

Розглянуто особливості застосування методів класифікації при оцінюванні якості систем захисту інформації, виявленні проникнень, аналіз великих даних з виявлення кібератак, розв’язання задач передбачення виникнення атак.

Наприкінці розділу проаналізовано особливості застосування машинного навчання при рішенні задач оцінки мережевих ризиків та аналізу трафіку, класифікації атак в залежності від величини нанесеної шкоди і вірогідності їх реалізації.

РОЗДІЛ 3
ОПИС РОЗРОБКИ ІНСТРУМЕНТУ ДОСЛІДЖЕННЯ

Зі зростанням загрози атак кібербезпеки ми спостерігаємо зростання аналітики безпеки, і такі системи, як Splunk, QRadar та HPE Arcsight використовуються для збору, аналізу та виявлення загроз. Зазвичай людські аналітики використовуються для осмислення створених попереджень, але часто вони все більше перевантажені кількістю попереджень та можливими загрозами. Таким чином, машинне навчання може бути використано для осмислення попереджень та їх співвіднесення між собою, а потім передавання результатів аналітикам.

Для машинного навчання (ML), як правило, є дві основні фази: навчання та тестування, із загальним набором етапів визначення ознак та класифікації наборів даних про навчання. Наступний підклас атрибутів призначений для класифікації та моделі навчання, застосованої тренування даних. За допомогою моделі навчання решта даних потім відновлюється та визначається рівень успіху. Основні елементи, які ми маємо при застосуванні машинного навчання у кібербезпеці:

- джерела інформації, що передбачає визначення джерел інформації, які потрібні для отримання правильної інформації;
- інструменти збору даних, які передбачають створення програмних агентів, необхідних для отримання необхідних даних;
- попередня обробка даних. що передбачає обробку даних у форматі, готовому для аналізу;
- визначення ключових особливостей, які потребували б механізми аналізу;
- механізм аналізу передбачає створення механізму, який враховує особливості та створює оцінку для оцінки ризиків.

- двигун прийняття рішень приймає бальні системи з етапу аналізу та приймає обґрунтоване рішення щодо рівня ризику.

Два основних підходи, що використовуються під час виявлення загроз - це виявлення сигнатур, які співпадають з добре відомими зразками шкідливої поведінки, або використовуємо виявлення аномалій, де визначено нормальний шаблон поведінки, а потім виявляємо відхилення від нього. Для машинно-орієнтованих загроз, таких як віруси та хробаки, найкраще підходять сигнатурні методи але для виявлення зосереджених на людині загроз нульового дня, наприклад, для шахрайства та крадіжки даних, методи виявлення аномалій зазвичай працюють найкраще.

В рамках машинного навчання часто бувають дві основні фази: навчання та тестування. Це передбачає визначення атрибутів класу (ознак) та класів на основі даних навчання, а потім їх зведення до підмережі, яка може бути використана в процесі класифікації. Потім з навчальним набором створюється модель, де модель використовується на повному наборі даних, щоб зрозуміти рівень успіху. Цей результат може бути представлений у формі метрики або рішення. У випадку з рішенням, як правило, використовується підхід матриці плутанини, де порівнюються передбачувані значення з фактичними значеннями. Наприклад, можна мати систему виявлення, яка контролює та класифікує логіни користувачів, тоді складається матриця плутанини, яка зображена на рисунку 3.1 щоб відобразити показники успіху [51].

		Predicted		
		Valid user	**Scripted user**	**Non-valid user**
Actual class	**Valid user**	7	1	0
	Scripted user	3	5	1
	Non-valid user	0	2	10

Рисунок 3.1 - Матриця плутанини

В рамках механізму прийняття рішень часто використовується поняття правильних та неправильних припущень. Отже, правильне припущення - це випадок, коли визначено, що подія була правильно виявлена, тоді як неправильне припущення - це те, коли справжня подія не була виявлена і, отже, пропущена системою. В системі IDS (системи виявлення вторгнень) часто доводиться дотримуватися рівноваги при налаштуванні систем, щоб користувачі не були завалені занадто великою кількістю помилкових попереджень (помилкових спрацьовувань) або занадто великою кількістю фальшивих попереджень.

Splunk - це один із найуспішніших пакетів аналітики кібербезпеки та визначає сім основних елементів машинного навчання :

- попередня обробка, яка визначає спосіб масштабування даних для отримання правильного діапазону (типовим методом є StandardScalar);
- вилучення функцій визначає метод вилучення ключових функцій, необхідних машині для навчання. (типовими методами є PCA та TFIDF);
- аналіз даних, який передбачає аналіз співвідношень між даними. (типові методи включають ACF та PACF);
- класифікація включає класифікацію даних за групами (типові методи включають: SVM та RandomForestClassifier);
- групові події, які зазвичай передбачають кластеризацію. (типові методи - Kmeans та BIRCH);
- виявлення викидів, де визначаються аномалії в наборах даних. (типовим методом є OneClassSVM);
- прогнозування визначає метод прогнозування майбутніх значень даних з історії даних. (типовими методами є ARIMA та KalmanFilter);

Прогнозування робить прогнози щодо даних із заданим набором відомих вхідних даних і можуть бути чисельним прогнозуваннями (наприклад, за

допомогою лінійної регресії, випадкової регресії лісу, ласо та регресії дерева рішень) або категоріальним (наприклад, з логістичною регресією).

3.1 Обрання інструменту для написання програмного продукту

Для написання програмного коду розробки було обрано такий потужний інструмент як Anaconda. Anaconda являє собою дистрибутив таких мов програмування як Pyton та R. Інструмент включає в себе ряд бібліотек з вільним доступом, які, в основному направлені на вирішення таких питань як наука про дані і Machine Learning. Ціль, яку переслідували розробники, було створити такий продукт, який буде здатний надати користувачу швидкий доступ до найбільш використовуваних модулів, тобто Astropy, Numpy, SciPy, та деяких інших.

Розглянемо інструмент більш детально. Після загрузки продукту, який розповсюджується на безкоштовній основі, та може бути знайдений на офіційному сайті anaconda.com (рис. 3.2), проводиться процес інсталяції, під час якого можуть бути обрані деякі додаткові налаштування.

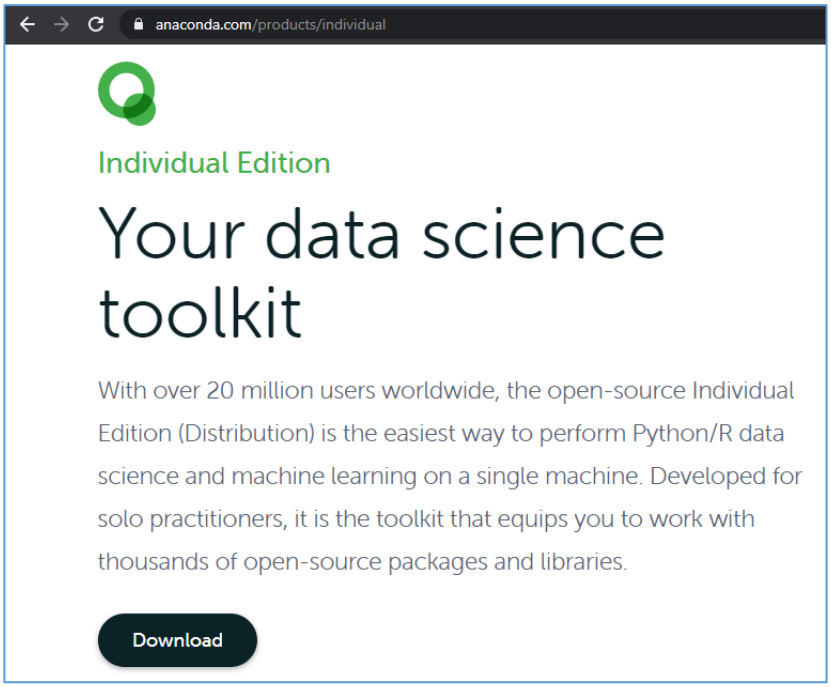


Рисунок 3.2 - Сторінка загрузки продукту на сайті **anaconda.com**

В тому числі, місце розташування папки дистрибутиву та інтегрування інструменту у процес провідника для швидкого доступу до певних можливостей продукту (рис. 3.3).

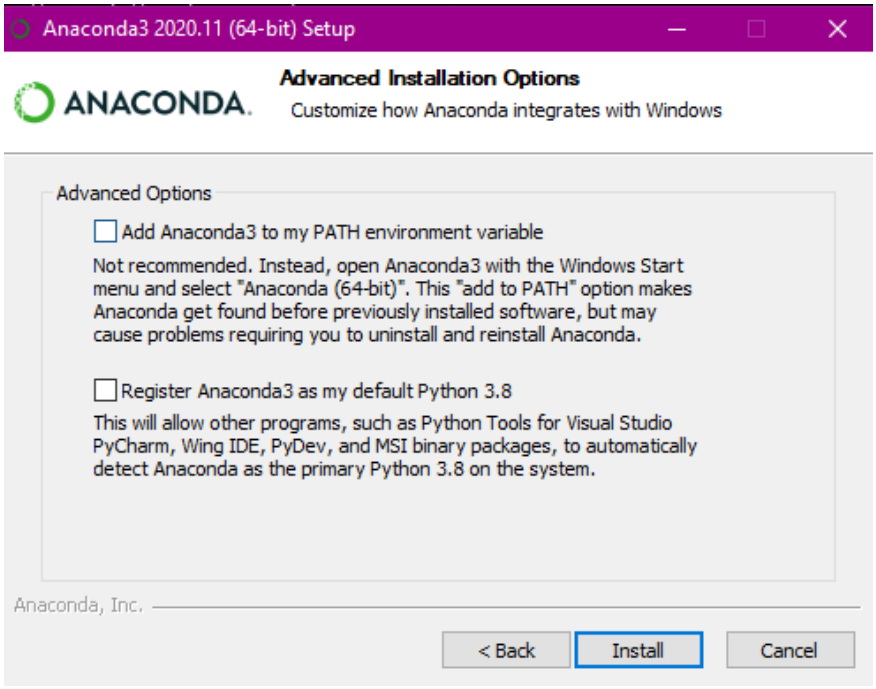


Рисунок 3.3 - Вікно інсталяції

Після того, як програма була інстальована на пристрій доступ до неї можна здійснити через меню «пуск», чи ярлик на робочому столі.

Інтерфейс програми представляє з себе так званий «навігатор» у якому представлено 8 модулів призначених для вирішення конкретних завдань (рис. 3.4). В тому числі мається модуль Orange 3, який надає користувачу потужний інструмент для роботи у середовищі Data Mining.

У проекті робота ведеться за допомогою модулю JupyterLab, розширене середовище для інтерактивних і відтворюваних обчислень заснованих на Jupyter Notebook і Architecture.

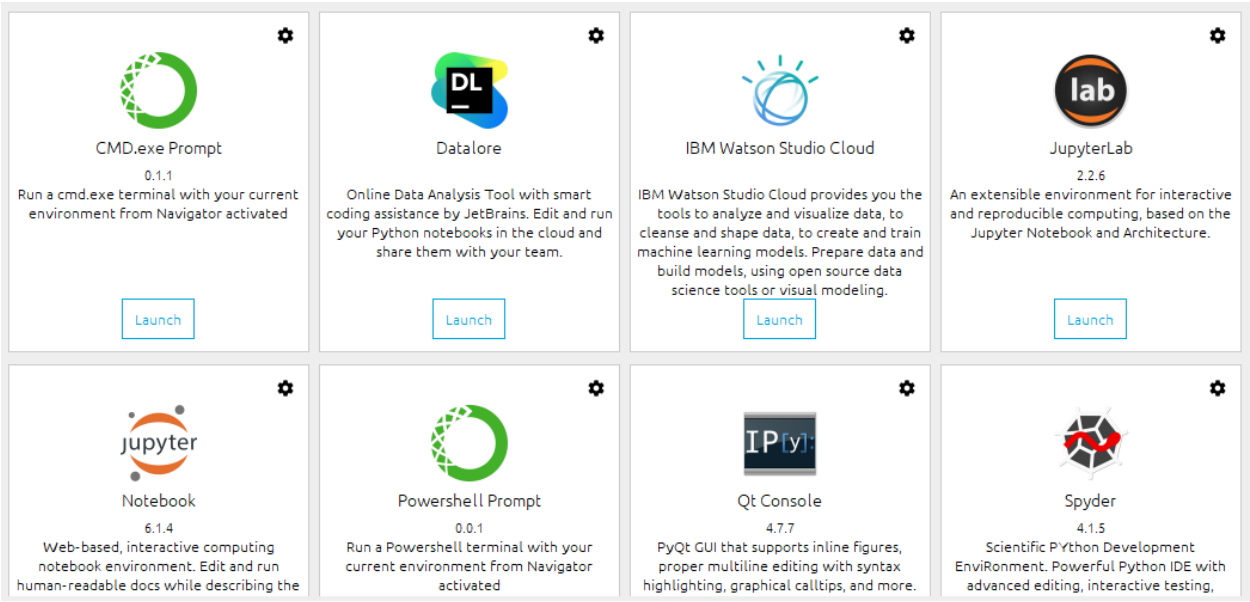


Рисунок 3.4 - Початкове вікно в Anaconda

JupyterLab це користувацький інтерфейс нового покоління основаного на web системі для роботи в середовищі Python.

3.2 Огляд та обрання методу класифікації

Метод класифікації Байєса базується на теоремі Байєса і стосується незалежної природи предикторів (не пов'язаних між собою ознак). Для цього ми маємо P (A | B), і яка є ймовірністю події A, заданою B; $P\,(B \mid A)$, яка ймовірність події B з урахуванням A; $P\,(A)$ ймовірність події A; і $P\,(B)$ ймовірність події B. Потім теорема визначає:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}.$$

Позначаємо вектор змінних $D = (d_i), i = 1,2,\dots,n$ представляємо документ, де d відповідає літері, слову чи інші атрибути якогось тексту, та набір $\mathrm{C} = (\mathrm{c}, \mathrm{c}, \dots,)$ визначено заздалегідь класи. Класифікація тексту полягає у призначенні мітки класу $c_j, \quad j = 1,2,\dots,k$ від C до документа. Класифікатор Байєса по суті є гібридною моделлю ймовірності параметрів:

$$P\left(C\middle|F_{1,}\dots,F_n\right) = \frac{P(C)P(F_1,\dots,F_n|C)}{P(F_1,\dots,F_n)}.$$

Де $P\ (c_j)$ - попередня інформація про ймовірність появи класу, це інформація з спостережень, що є знаннями з самого тексту, який підлягає класифікації, та $P\ (D|c_j)$– це ймовірність розподілу документа D у просторі класів. Класифікатор Байєса полягає у інтеграції цієї інформації і обчисленні окремо апостеріорні документи D, які потрапляють до кожного класу c_j, і призначити документ до класу з найбільшою ймовірністю, тобто:

$$c^*(D) = \arg\max P(c_j|D).$$

Припустимо, що компоненти D незалежні один від одного, оскільки умовна ймовірність $P\left(D\middle|c_j\right)$ неможливо обчислити безпосередньо на практиці. Таким чином:

$$P\left(D\middle|c_j\right) = \prod P\ (d_i|c_j).$$

Модель з наведеним вище припущенням називається наївною моделлю Байєса, і дорівнює:

$$P\left(c_j\middle|D\right) = \frac{P(c_j)\prod P(d_i|c_j)}{P(D)}.$$

Оскільки зразок інформації $P(D)$ ідентичний кожному класу $c_j,\ j\ =\ 1,2,\ldots,k$, рівняння стає

$$c^*(D) = \arg\max P(c_j)\prod P\left(d_i|c_j\right).$$

3.3 Опис роботи алгоритму

З метою розв’язання завдань даної кваліфікаційної роботи було вирішено створити програмний інструмент, за допомогою якого можна розрахувати вірогідності атаки на певну систему з використанням методу Байєса.

Вхідними даними для роботи алгоритму є кількість зафіксованих атак різного типу на обрані об’єкти системи.

Інструмент розроблено з урахуванням, що кількість видів атак і кількість об’єктів системи є необмеженими.

На початку робочого алгоритму формується структура таблиці для виконання подальших розрахунків та заповнення.

Завдяки прості алгоритму і малої кількості використаних модулів, алгоритм може бути легко адаптований під особливості певної системи.

Блок схема алгоритму розробленого продукту відображено на рисунку 3.5.

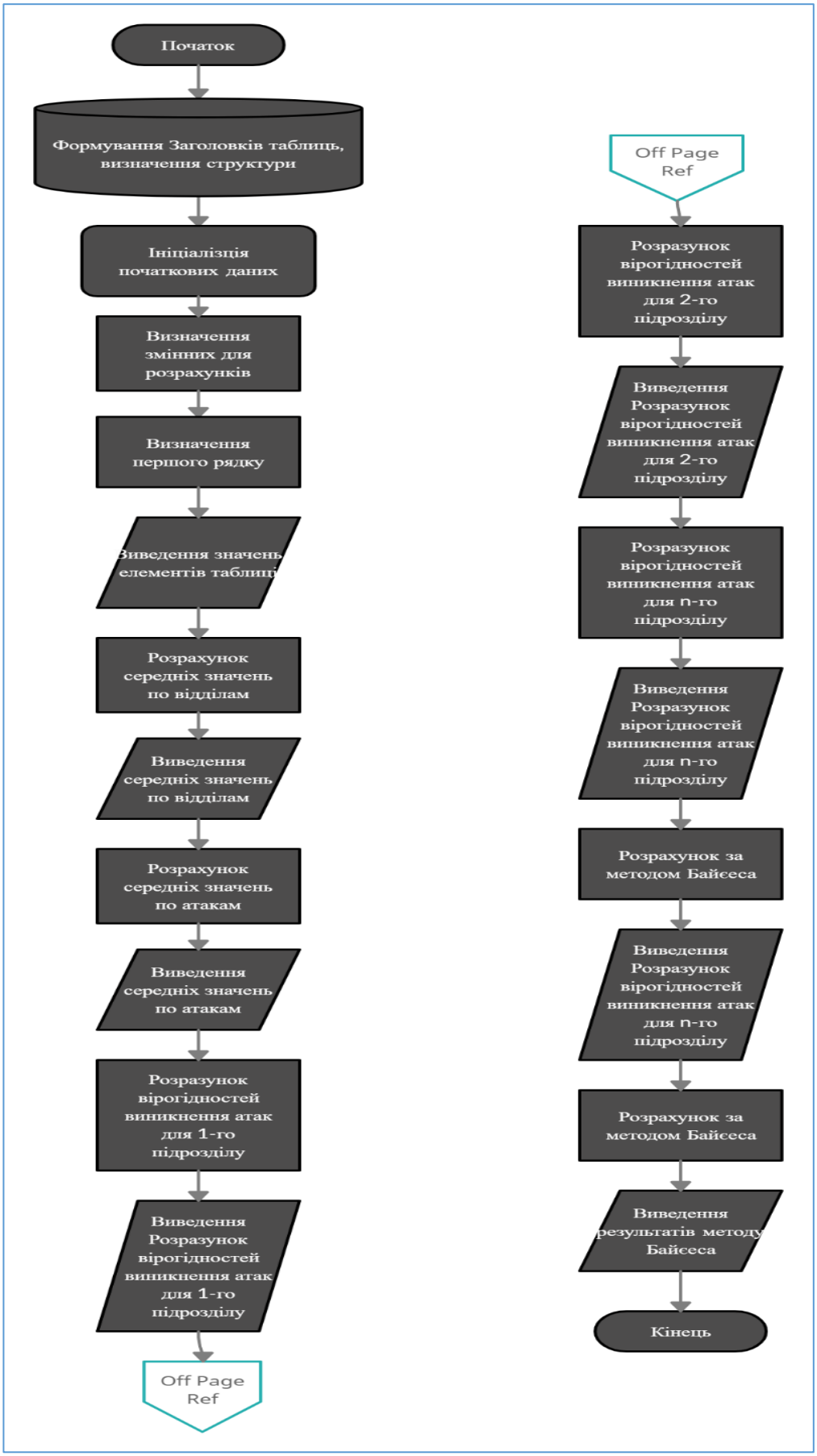


Рисунок 3.5 - Блок схема алгоритму розрахунку за методом Байєса

Алгоритм формує і заповнює табличну структуру, виконує розрахунки за формулою Байєса. Рядки таблиці характеризують системи, колонки – види виявлених атак. Кількість рядків та стовбців не обмежено.

3.4 Опис програмної реалізації

В процесі програмної реалізації застосовані описані нижче змінні та параметри.

Вхідні параметри:

A – масив назв об’єктів;

B – масив виявлених атак;

np.array – масив частот появи атак конкретного виду;

N_Accounting, N_HRD, N_Technical – назви об’єктів;

N_Phishing, N_Crypto, N_Network – види атак.

Робочі параметри:

P_Accounting, P_HRD, P_Technical – середні значення кількості атак;

P_Phishing, P_Crypto, P_Network – середня кількість реалізованих атак за видами;

P_S_givenP, P_S_givenC, P_S_givenN, P_P_givenP, P_P_givenC, P_P_givenN, P_R_givenP, P_R_givenC, P_R_givenN – вірогідність виникнення атак для підрозділів.

Результати:

P_Phish_givenAccounting, P_Phish_givenHRD, P_Phish_givenTechnical – результуючі змінні.

Програма написана на мові програмування Python, має лінійну структуру і призначена для формування і заповнення матриці визначення вірогідностей події з застосування методу Байєса за попередньо описаною математичною моделлю.

3.5 Висновки за розділом

На початку розділу проаналізовано існуючий інструментарій котрий використовується для збору аналізу і виявлення загроз. Застосовуються поняття машинного навчання і його використання з метою виявлення та передбачення порушень. Виділено основні елементи при застосуванні машинного навчання. Наведено поняття «матриці плутанини».

Далі в розділі розглянуто інструменти для розробки програмного продукту, надано опис системи Anaconda.

З точки зору програмної реалізації обґрунтовано обрання методу класифікації Байєса.

Наведено алгоритм розробленого програмного інструменту для виконання розрахунків. Описана загальна структура програми.

У наступному розділі опишемо тестування працездатності інструменту та проведемо аналіз результатів дослідження.

РОЗДІЛ 4
АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

4.1 Тестування працездатності програмного продукту

З метою виконання завдань кваліфікаційної роботи було виконано огляд та аналіз методів класифікації інформації. За результатами дослідження виявлено, що метод Байєса є необхідним та достатнім методом для виконання попереднього етапу аналізу. Загальний інтерфейс програми-інструменту дослідження наведено на рисунку 4.1.

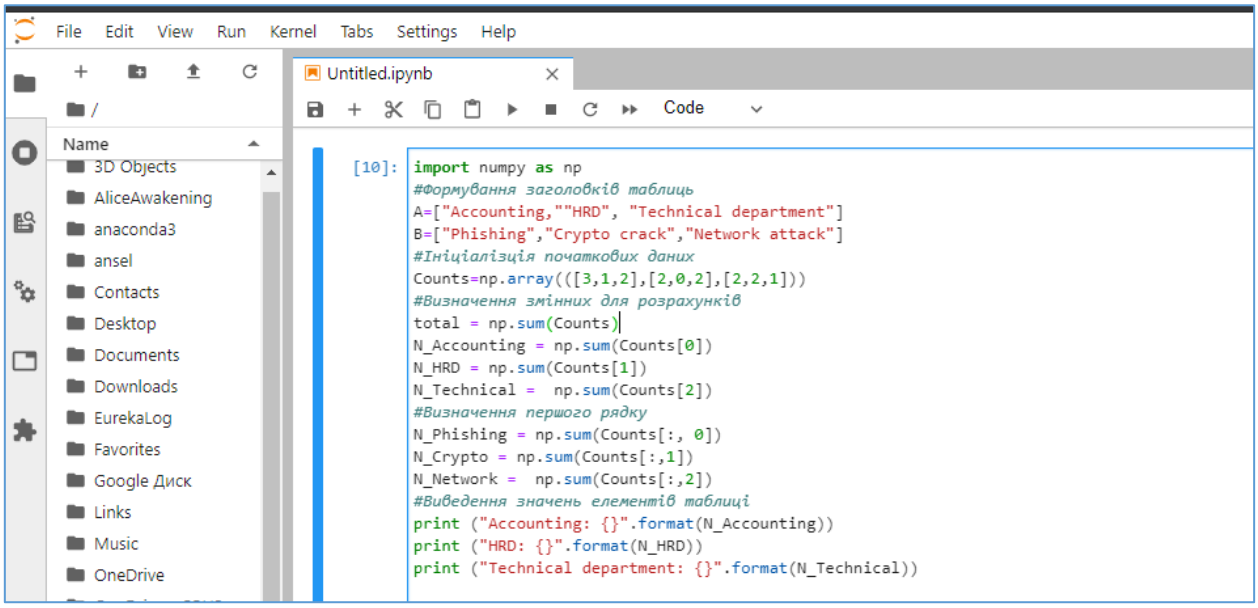


Рисунок 4.1 - Інтерфейс середовища програмування

Це є консольний додаток на мові Python з застосуванням стандартних бібліотек, операторів та режимів пакету.

Тестування працездатності програмного продукту підтверджено методом білої скриньки при запуску розробки, що видно на рисунку 4.2.

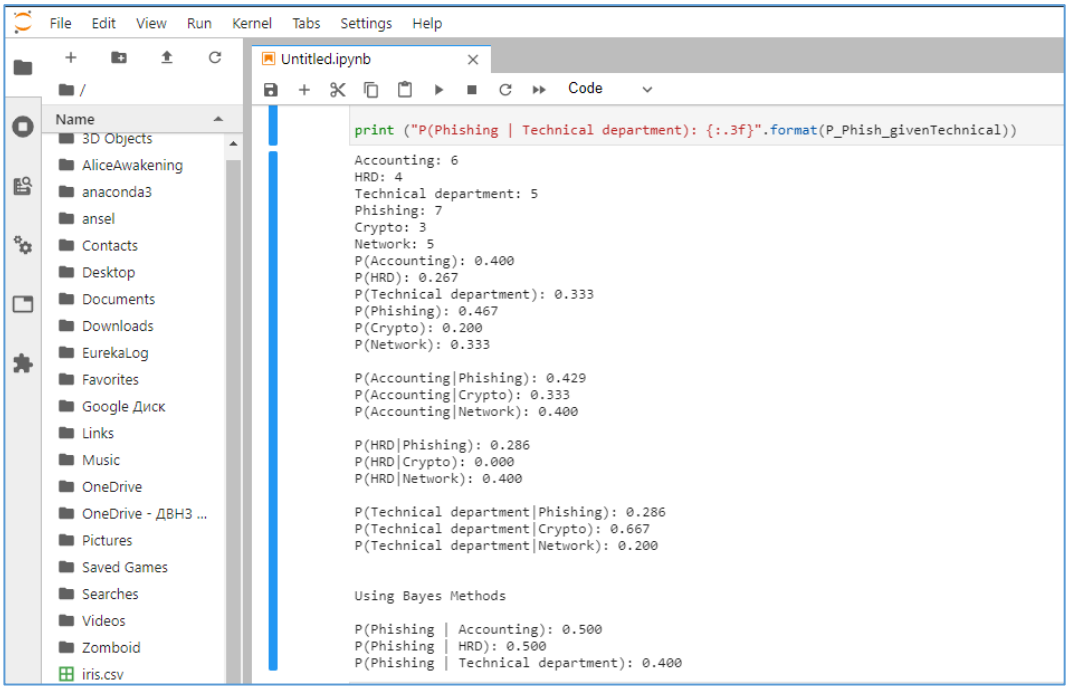


Рисунок 4.2 - Результати роботи програми

4.2 Вхідні дані для експерименту

Опишемо вхідні дані експерименту. Наприклад, відстежуємо системи (A) і виявляємо види вірусних атак (B), як показано в таблиці 4.1.

Таблиця 4.1 – Перелік систем та виявлених атак

Системи	Втручання
Відділ кадрів	Фішинг
Відділ кадрів	Атака мережі
Відділ кадрів	Фішинг
Відділ кадрів	Атака мережі
Технічний відділ	Атака мережі
Технічний відділ	Крипто атака
Технічний відділ	Крипто атака
Технічний відділ	Фішинг
Технічний відділ	Фішинг
Бухгалтерія	Фішинг
Бухгалтерія	Атака мережі
Бухгалтерія	Фішинг
Бухгалтерія	Крипто атака
Бухгалтерія	Фішинг
Бухгалтерія	Атака мережі

В якості вхідних даних обрана інформація отримана у відділі служби комп’ютерного забезпечення підприємства шахта «Центральна». Цими даними є результати зафіксованих атак системи, у тому числі мережевих та крипто атак.

Для проведення експерименту обрано 15 атак, які зафіксовані за даними підприємства проходження переддипломної практики (таблиця 4.2). По-перше, ми можемо створити таблицю частот для атак на наші системи:

Таблиця 4.2 – Дані для експерименту 1

Системи	Фішинг	Крипто атаки	Атаки мережі	P(A)
Бухгалтерія	3	1	2	0.4
Відділ кадрів	2		2	0.267
Технічний відділ	2	2	1	0.333
P(B)	0.467	0.2	0.333	

Графічне відображення надано на рисунку 4.3.

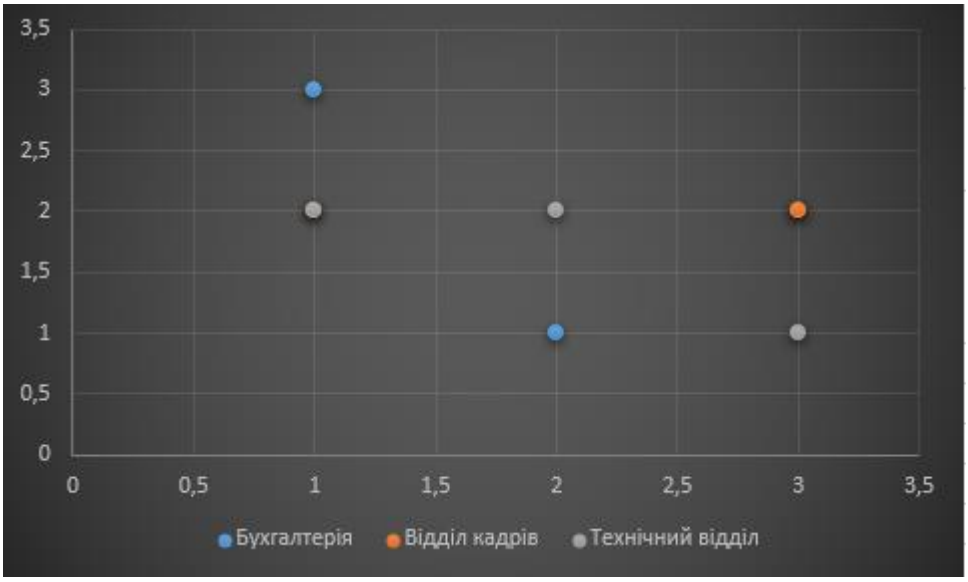


Рисунок 4.3 - Частоти атаки на системи

4.3 Заміри та експерименти

Тепер ми можемо бачити, що P (Бухгалтерія) = 0,467 (7/15), P (Відділ кадрів) = 0,267 (4/15) і P (Технічний відділ) = 0,333 (5/15), а P (фішинг) = 0,64, P (Крипто атака) = 0,18 і P (Атака мережі) = 0,45. Отже, ми маємо ймовірність того, що наш сервер продажів буде зламаний протягом 46,7% випадків, а ймовірність того, що це мережева атака, становить 33,3% часу. Далі ми можемо визначити ймовірність того, що A (Система) відбудеться з урахуванням B (Тип атаки), а це P (A | B).

Для цього ми просто беремо кожну атаку, а потім ділимо на загальну кількість цих атак (таблиця 4.3):

Таблиця 4.3 – Етап перший

Системи	Фішинг	Крипто атаки	Атаки мережі
Бухгалтерія	0.429	0.333	0.4
Відділ кадрів	0.286	0	0.4
Технічний відділ	0.286	0.667	0.2

У цьому випадку бачимо:

$$P(\text{Бухгалтерія}|\text{Фішинг}) = \frac{3}{7} = 0.429,$$

$$P(\text{Відділ кадрів}|\text{Фішинг}) = \frac{2}{7} = 0.286,$$

$$P(\text{Технічний відділ}|\text{Фішинг}) = \frac{2}{7} = 0.286.$$

Таким чином, ймовірність того, що саме сервер бухгалтерії потрапив, якщо ми знаємо, що маємо фішинг-атаку, становить 0,429. Якщо ми знаємо, що це крипто-атака, між сервером бухгалтерії і сервером технічного відділу існує шанс 50/50. Сума наших ймовірностей знання B (атаки) для визначення P (A | B) повинна дорівнювати одиниці.

Тепер ми будемо використовувати логіку Байєса для визначення P (B | A) і де ми зможемо визначити ймовірність типу атаки (A) для сервера (B). Таким чином для:

$$P(\text{Крипто атаки}|\text{Продажі}) = =$$

$$\frac{P(\text{Бухгалтерія}|\text{Крипто атаки})\cdot P(\text{Крипто атаки})}{P(\text{Бухгалтерія})},$$

$$P(\text{Крипто атаки}|\text{Бухгалтерія}) = \frac{0.333\cdot 0.214}{0.429} = 0.166.$$

Результати наступного етапу розрахунку відображено в таблиці 4.4.

Таблиця 4.4 – Результати проведених розрахунків, етап другий

Атака	Бухгалтерія	Відділ кадрів	Технічний відділ
Фішинг	0.501	0.5	0.401
Крипто атака	0.167	0	0.401
Атака мережі	0.333	0.499	0.2

Після проведення іншого дослідження з більшою кількість даних, отримали наступні результати зображені на рисунку 4.4.

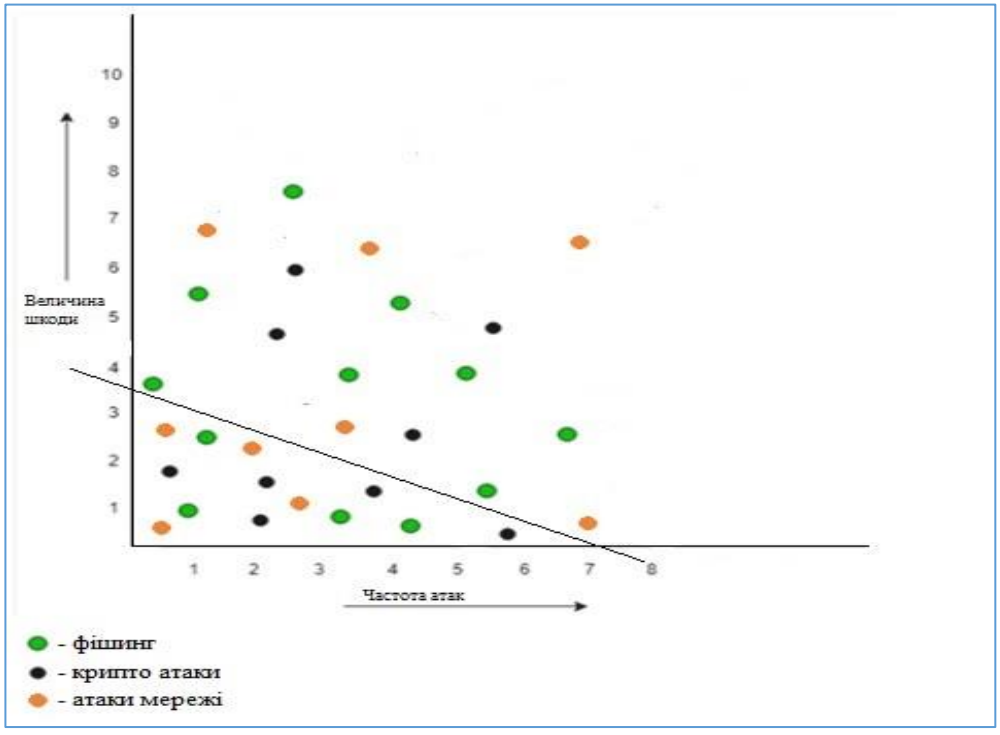


Рисунок 4.4 - Ймовірность атаки на систему

При побудові графіку для формування графіку застосовані наступні значення параметрів за осями X та Y.

Вісь Y це значення уразливості відносно можливої шкоди, котру зазнає підприємство в результаті здійсненої атаки (таблиця 4.5).

Таблиця 4.5 - Значення уразливості в залежності від шкоди

Значення вразливості	Опис шкоди
0	Розкриття інформації принесе незначний моральний збиток фірмі
1	Розкриття інформації принесе незначний моральний і фінансовий збиток фірмі
2	Збиток від атаки є, але він незначний, основні фінансові операції фірми на ринку не порушені
3	Збиток від атаки є, фінансове положення фірми на ринку все ще стабільне
4	Фінансові операції не ведуться протягом деякого часу, фірма зазнає збитків, але її положення на ринку і кількість клієнтів змінюються мінімально
5	Фінансові операції не ведуться, фірма зазнає збитків, її положення на ринку змінюються помітно
6	Значні втрати на ринку і в прибутку.
7	Від фірми йде відчутна частина клієнтів
8	Втрати дуже значні, фірма на період до року втрачає становище на ринку.
9	Для відновлення положення фірми на ринку потрібні великі фінансові позики.
10	Фірма припиняє існування

Для формування осі X застосовано значення атак, яке представляється невід'ємним числом у відповідності, наприклад, з наступною таблицею 4.6:

Таблиця 4.6 - Ймовірність атаки

Ймовірність	Середня частота появи
0	даний вид атаки відсутній
1	рідше, ніж раз на рік
2	близько 1 разу на рік
3	1 раз на півроку
4	рідше, ніж 1 раз на півроку
5	близько 1 разу на квартал
6	близько 1 разу на місяць
7	близько 1 разу на тиждень
8	практично щодня

У Байєсі нам потрібна сильна незалежність між подіями A та B.

У рамках scikit-learn ми можемо використовувати три наївні ймовірнісні розподіли Байєса [51]:

- Бернуллі визначає базову двійкову класифікацію щодо наявності ознаки чи ні;
- багаточлена визначає дискретний показник міцності об’єкта;
- Гаусову, яка визначає як середнє значення, так і дисперсію сили об’єкта.

Таким чином розроблені структури аналітичних таблиць та створений інструмент підтверджують працездатність створеного програмного інструменту, який побудовано з застосуванням методу Байєса й можливість його застосування для виконання класифікації криптографічних атак.

4.4 Висновки за розділом

На початку розділу продемонстровано працездатність розробленого інструменту, наведено зображення, які зображують частину програмного коду та результати його роботи.

Далі в розділі розглянуто вхідні дані, взяті з реально існуючого підприємства. Інформація була оброблена і зведена до зручної у використанні таблиці, а також зображена на діаграмі розсіювання.

Були зроблені розрахунки, які продемонстрували вірогідність певного виду атаки на певну систему. Після проведення необхідних обчислень, результати були занесені до таблиць.

Наприкінці розділу продемонстровано діаграму розсіювання, на якій зображені результати проведення іншого досліду з використанням більшої кількості даних для більш наглядної демонстрації роботи алгоритму класифікації Байєса.

ВИСНОВКИ

Методи класифікації є одним з основних інструментів, які застосовуються в сфері захисту даних для вирішення таких задач, як попередження атак, розрахунок ризиків атак на окремі системи та класифікації втручання в роботу системи.

Кваліфікаційна робота пропонує перелік та аналіз методів Data Mining, зокрема методів класифікації та приклади їх застосування при захисті систем.

В результаті виконання кваліфікаційної роботи вирішено наступні задачі:

1) проаналізовано основи інформаційної безпеки та проблем, які вона вирішує;
2) знайдено приклади застосування методів Data Mining в захисті інформації;
3) вдалося систематизувати методи класифікації інформації відносно застосування в криптології;
4) визначено критерії обрання методів класифікаціїї для розв’язання конкретних задач кібербезпеки;
5) показана можливість розподілу атак з визначенням найбільш критичних.

Розроблені структури аналітичних таблиць для аналізу та створений інструмент, який допомагає в проведенні досліджень з застосуванням методу Байєса.

В майбутньому створений інструмент може бути застосований службою кібербезпеки підприємства для попередження та реальної класифікації виявлених атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук - Луцьк: Вежа-Друк, 2014. - 164 с.

2. Тилборгван Х. Основы криптологии. Профессиональное руководство и интерактивный учебник, — М.: Мир, 2006, - 471 с.

3. Gustavus J. Simmons: Cryptology, [Електроний ресурс]. - Режим доступу: www.britannica.com/topic/cryptology

4. Arnold Abrams, David Kahn: Historian of Secret Codes, in Newsday (Sept. 19, 2004), [Електронний ресурс]. - Режим доступу: https://web.archive.org/web/20050913030949/http://hnn.us/roundup/comments/7460.html

5. Al-Vahed A., Sahhavi H., An overview of modern cryptography, World Applied Programming, Vol (1), No (1), April 2011. 55-61, ISSN: 2222-2510

6. AES encryption, [Електронний ресурс]. – Режим доступу: https://aesencryption.net/

7. Горбенко, І. Д. Перспективний блоковий симетричний шифр «Калина»: основні положення та специфікації / І. Д. Горбенко, В. І. Долгов, Р. В. Олейніков [та ін.] // Прикладна радіоелектроніка. - 2007. - Т. 6, № 2. – 195-208 с.

8. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Review of Modern Physics. - 2002. - V. 74. - 145-195 с.

9. Василиу Е.В., Воробиенко П.П. Проблемы развития и перспективы использования квантово-криптографических систем // Наук. праці ОНАЗ ім. О.С. Попова. - 2006, № 1. - 3-17 с.

10. Role of Data Mining in Cyber Security P. Santhosh Raj , G. Silambarasan M.Phil Scholar, [Електроний ресурс]. - Режим доступу:https:/ijesc.org/upload/acabab661bea8652d8a277ba30e6d866.Role%20of%20Data%20Mining%20in%20Cyber%20Security.pdf

11. Data Mining for Security Applications : Bhavani Thuraisingham, Latifur Khan, Mohammad M. Masud, Kevin W. Hamlen

12. P. Santhosh Raj, G. Silambarasan, M.Phil Scholar, Role of Data Mining in Cyber Security, International Journal of Engineering Science and Computing, July 2017, P 13932 -13935, URL

13. Кузнецов Г. В. Математичні основи криптографії Навч посібник / Г. В. Кузнецов, В. В. Фомичов, С. О. Сушко, Л. Я. Фомичова - Дніпропетровськ Національний гірничий університет, 2004.- 391 с.

14. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. - К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. - 297 с.

15. Лившиц Ю. Курс лекций “Алгоритмы для Интернета”, [електронний ресурс], режим доступу: // https://logic.pdmi.ras.ru/~yura/internet.html

16. Rocchio, J. Relevance feedback in information retrieval // In G. Salton ed., The SMART Retrieval System: Experiments in Automatic Document Processing, Englewood Cliffs, New Jersey, Prentice-Hall, 1971. - 313 - 323 с.

17. Sebastiani F. Machine Learning in Automated Text Categorization, [Електроний ресурс]. – Режим доступу: https://www.nmis.isti.cnr.it/sebastiani/Publications/ACMCS02.pdf

18. C. E. Shannon, Communication Theory of Secrecy Systems, Bell Systems Technical Journal, , 1948 - Vol. 28. - 656–715 с.

19. Eli Biham Shannon’s Theory of Secrecy Systems // Lecture. - March 1, 2011, [Електроний ресурс]. - Режим доступу: http://www.cs.haifa.ac.il/~orrd/IntroToCrypto/Spring11/Lecture2.pdf

20. John K. Kruschke «Doing Bayesian Data Analysis: A Tutorial with R and BUGS» Europe’s Journal of Psychology, 7(4), 778-779 p, [Електроний ресурс]. - Режим доступу: https://www.researchgate.net/publication/273368935_Doing_Bayesian_Data_Analysis_A_Tutorial_with_R_and_BUGS

21. Vapnik V. Statistical learning theory. Wiley, New York, 1998.

22. Перегудов С.В. Модель профілювання поведінки користувачів за допомогою методу опорних векторів, [Електроний ресурс]. – Режим доступу: https://ela.kpi.ua/handle/123456789/31320

23. Пархоменко І. І. Застосування методів штучного інтелекту в системах антивірусного захисту / Пархоменко І. І., Молодан Б. О., Нечипорук В.В. // Науково-практичний журнал «Захист інформації» № 2, 2012, 37-41 с.

24. Lashkov P., Schäfer C., Kotenko I. Intrusion Detection in Unlabeled Data with Quarter-Sphere Support Vector Machine, [електронний ресурс], режим доступу www.comsec.spb.ru

25. Иофина Г.В. Эффективные оценки в алгоритмах вычисления оценок // "Штучний інтелект". – № 2'2006. – 155 – 159 с.

26. Nello Cristianini and John Shawe-Taylor. An Introduction to Support Vector Machines and other kernel-based learning methods. Cambridge University Press, 2000.

27. John Shawe-Taylor and Nello Cristianini. Kernel Methods for Pattern Analysis. Cambridge University Press, 2004.

28. Y. Lu and C. Rasmussen (2012). Simplified markov random fields for efficient semantic labeling of 3D point clouds. IROS.

29. Маннинг К.Д., Рагхаван П., Шютце Х. Введение в информационный поиск.— М.: Изд-во «Вильямс», 2020. – 528 с.

30. Siri Bromander, Audun Jøsang, Martin Eian, Semantic Cyberthreat Modelling, [Електроний ресурс]. – Режим доступу: http://ceur-ws.org/Vol-1788/STIDS_2016_A03_Bromander_etal.pdf

31. Prasad Naldurg, Koushik Sen, and Prasanna Thati A Temporal Logic Based Framework for Intrusion Detection, [Електроний ресурс]. – Режим доступу: http://dl.ifip.org/db/conf/forte/forte2004/NaldurgST04.pdf

32. Thomas Oseku-Afful (2016), The use of Big Data Analytics to protect Critical Information Infrastructures from Cyber-attacks, Luleå University of Technology, [Електроний ресурс]. – Режим доступу: https://www.diva-portal.org/smash/get/diva2:1037515/FULLTEXT02.pdf

33. Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin, Robiah Yusof, Cyber Threat Intelligence – Issue and Challenges, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 10, No. 1, April 2018, 371 – 379 p., [Електроний ресурс]. – Режим доступу: https://www.researchgate.net/publication/322939485_Cyber_Threat_Intelligence_-_Issue_and_Challenges

34. Fransen F, Smulders A, Kerkdijk R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. Elektrotechnik & Informationstechnik. 2015 - 18:106–12 с.

35. Sillaber C, Sauerwein C, Mussmann A, Breu R. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. Proc 2016 ACM Work Inf Shar Collab Secur. 2016 - 65–70 с.

36. Casey E, Back G, Barnum S. Leveraging CybOXTM to standardize representation and exchange of digital forensic information. Digit Investig. 2015 - 12(S1):S102–10.

37. Barnum S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIXTM). MITRE Corp July. 2014. - 1–20 с.

38. Connolly J, Davidson M, Schmidt C. The Trusted Automated eXchange of Indicator Information (TAXII TM). 2014 - 1–10 с.

39. Wagner C, Dulaunoy A, Wagener G, Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. Proc 2016 ACM Work Inf Shar Collab Secur. 2016 - 49–56 с.

40. A. Dey. Machine Learning Algorithms: A Review. vol, 7, 1174-1179,2016.

41. S. B. Kotsiantis, I. Zaharakis, and P. Pintelas. Supervised machine learning: A review of classification techniques. Emerging artificialintelligence applications in computer engineering, 160, 2007. - 3-24 с.

42. J. B. Fraley, and J. Cannady. The promise of machine learning in cybersecurity. In SoutheastCon, 2017. - IEEE. 2017, March. - 1-6 с.

43. S. Dolev and S. Lodha, “Cyber Security Cryptography and Machine Learning“, In Proceedings of the First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, 2017.

44. K. Rieck, P. Trinius, C. Willems, and T. Holz. Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4), 2011. - 639-668 с.

45. T. Nguyen, and G. Armitage. A survey of techniques for Internet traffic classification using machine learning. IEEE Communications Surveys and Tutorials. – 2008 - 56-76 с.

46. C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y Lin. Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994-12000, 2009.

47. G. A. Wang, M. Chau, and H. Chen. Intelligence and Security Informatics: 12th Pacific Asia Workshop, PAISI 2017, Jeju Island, South Korea, May 23, 2017, Proceedings. Cham, Switzerland: Springer.

48. C. Sinclair, L. Pierce, and S. Matzner. An application of machine learning to network intrusion detection. In Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual. - IEEE, 1999. - 371-377 с.

49. D. P. Benjamin, P. Pal, F. Webber, P. Rubel, and M. Atigetchi. Using a cognitive architecture to automate cyberdefense reasoning. In Bioinspired Learning and Intelligent Systems for Security, 2008. BLISS'08. ECSIS Symposium on. - IEEE, 2008, August. - 58-63 с.

50. L. Zomlot, S. Chandran, D. Caragea, and X. Ou. Aiding intrusion analysis using machine learning. In Machine Learning and Applications (ICMLA), 2013 12th International Conference on. - IEEE, 2013, December. - Vol. 2, 40-47 с.

51. Introduction to Naïve Bayes in Cybersecurity, Bill Buchanan, [Електроний ресурс]. – Режим доступу: https://billatnapier.medium.com/introduction-to-na%C3%AFve-bayes-in-cybersecurity-9fb19f849f80

Додаток А

Зауваження нормоконтролера

Таблиця А.1 – Зауваження нормоконтролера

Сторінка	Позначення	Зміст зауваження

Додаток Б

Фрагмент лістингу програми

```
import numpy as np
#Формування заголовків таблиць
A=["Accounting,""HRD", "Technical department"]
B=["Phishing","Crypto crack","Network attack"]
#Ініціалізція початкових даних
Counts=np.array(([3,1,2],[2,0,2],[2,2,1]))
#Визначення змінних для розрахунків
total = np.sum(Counts)
N_Accounting = np.sum(Counts[0])
N_HRD = np.sum(Counts[1])
N_Technical =  np.sum(Counts[2])
#Визначення першого рядку
N_Phishing = np.sum(Counts[:, 0])
N_Crypto = np.sum(Counts[:,1])
N_Network =  np.sum(Counts[:,2])
#Виведення значень елементів таблиці
print ("Accounting: {}".format(N_Accounting))
print ("HRD: {}".format(N_HRD))
print ("Technical department: {}".format(N_Technical))

print ("Phishing: {}".format(N_Phishing))
print ("Crypto: {}".format(N_Crypto))
print ("Network: {}".format(N_Network))
```

```
#Розрахунок середніх значень по відділам
P_Accounting=np.sum(Counts[0])/total
P_HRD= np.sum(Counts[1])/total
P_Technical = np.sum(Counts[2])/total
#Виведення середніх значень по відділам
print ("P(Accounting): {:.3f}".format(P_Accounting))
print ("P(HRD): {:.3f}".format(P_HRD))
print ("P(Technical department): {:.3f}".format(P_Technical))
#Розрахунок середніх значень по атакам
P_Phishing=np.sum(Counts[:,0])/total
P_Crypto= np.sum(Counts[:,1])/total
P_Network = np.sum(Counts[:,2])/total
#Виведення середніх значень по атакам
print ("P(Phishing): {:.3f}".format(P_Phishing))
print ("P(Crypto): {:.3f}".format(P_Crypto))
print ("P(Network): {:.3f}".format(P_Network))
#Розразунок вірогідностей виникнення атак для 1-го підрозділу
P_S_givenP = Counts[0][0]/N_Phishing
P_S_givenC = Counts[0][1]/N_Crypto
P_S_givenN = Counts[0][2]/N_Network
#Виведення вірогідностей виникнення атак для 1-го підрозділу
print ("\nP(Accounting|Phishing): {:.3f}".format(Counts[0][0]/N_Phishing))
print ("P(Accounting|Crypto): {:.3f}".format(P_S_givenC))
print ("P(Accounting|Network): {:.3f}".format(P_S_givenN))
#Розразунок вірогідностей виникнення атак для 2-го підрозділу
P_P_givenP = Counts[1][0]/N_Phishing
```

```
P_P_givenC = Counts[1][1]/N_Crypto
P_P_givenN = Counts[1][2]/N_Network
#Виведення вірогідностей виникнення атак для 2-го підрозділу
print ("\nP(HRD|Phishing): {:.3f}".format(P_P_givenP))
print ("P(HRD|Crypto): {:.3f}".format(P_P_givenC))
print ("P(HRD|Network): {:.3f}".format(P_P_givenN))
#Розразунок вірогідностей виникнення атак для n-го підрозділу
P_R_givenP = Counts[2][0]/N_Phishing
P_R_givenC = Counts[2][1]/N_Crypto
P_R_givenN = Counts[2][2]/N_Network
#Виведення вірогідностей виникнення атак для n-го підрозділу
print ("\nP(Technical department|Phishing): {:.3f}".format(P_R_givenP))
print ("P(Technical department|Crypto): {:.3f}".format(P_R_givenC))
print ("P(Technical department|Network): {:.3f}".format(P_R_givenN))
# Розрахунок за методом Байєеса P(A|B) = P(B|A) * P(A) / P(B)
print ("\n\nUsing Bayes Methods")
P_Phish_givenAccounting = P_S_givenP * P_Phishing/P_Accounting
P_Phish_givenHRD = P_P_givenP * P_Phishing/P_HRD
P_Phish_givenTechnical = P_P_givenP* P_Phishing/P_Technical
#Виведення результатів методу Байєеса
print ("\nP(Phishing | Accounting): {:.3f}".format(P_Phish_givenAccounting))
print ("P(Phishing | HRD): {:.3f}".format(P_Phish_givenHRD))

print ("P(Phishing | Technical department):
{:.3f}".format(P_Phish_givenTechnical))
```

Додаток В

Матеріали презентації

Міністерство освіти і науки України

ДВНЗ «Донецький національний технічний університет»

Аналіз особливостей застосування методів класифікації інформації в криптографії

ст. групи ІПЗІм-19

Дем'яненко Віктор Дмитрович

Науковий керівник

Маслова Наталя Олександрівна

Вступ

Актуальність. Проблема класифікації інформації є актуальною, так як обробка інформації отриманої під час протидії кібератакам є одним із головних елементів забезпечення інформаційної безпеки, а класифікація є важливим інструментом структурування даних для їх подальшого аналізу аналітиками.

Мета. Аналіз застосування методів класифікації інформації в криптології та розробка програмного інструменту аналізу атак.

Об'єкт. Технології застосування методів класифікації для проведення криптографічного захисту інформаційних систем від комп'ютерних атак.

Предмет дослідження. Методи класифікації в захисті інформаційних систем.

Задачі

1) аналіз основ інформаційної безпеки та проблем, які вона вирішує;

2) пошук прикладів застосування методів Data Mining в захисті інформації;

3) систематизація методів класифікації інформації відносно застосування в криптології;

4) визначення критеріїв обрання методів класифікаціїї для розв'язання конкретних задач кібербезпеки;

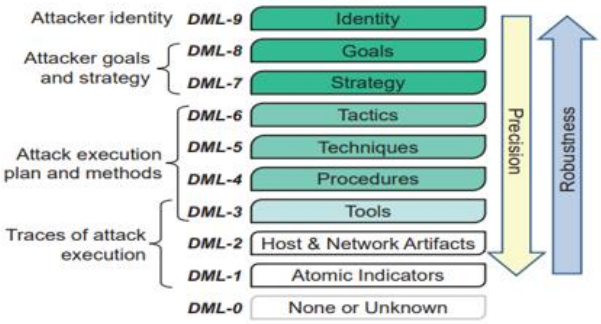
5) оцінка ефективності методів та розробка структури таблиці для аналізу.

Огляд методів класифікації

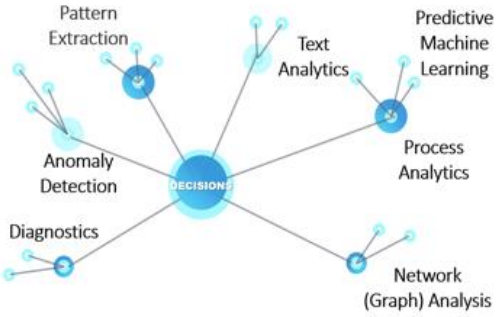
Метод Байєса. На основі байєсівського аналізу в кібербезпеці прогнозують події, фільтрують сильно зашумлені дані, в яких є сигнали певної форми, оцінюють параметри, порівнюють моделі.

Метод опорних векторів. Метод опорних векторів застосовується при виявленні аномальної поведінки, виділення сигнатур атак, в системах антивірусного захисту.

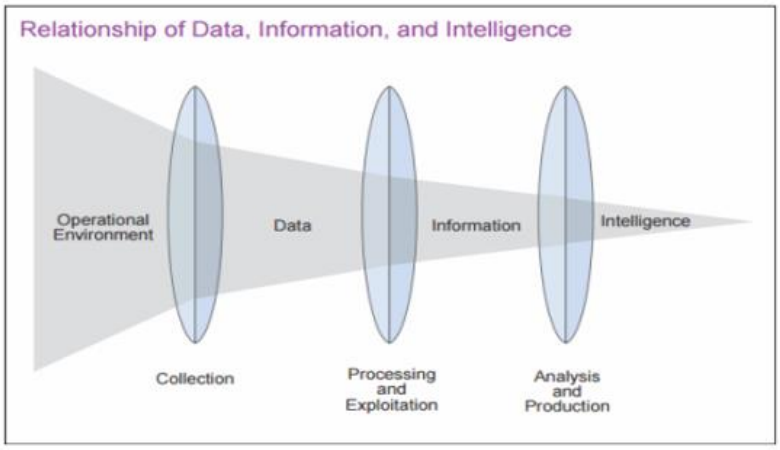
Модель DML



Методи аналітика в Big Data



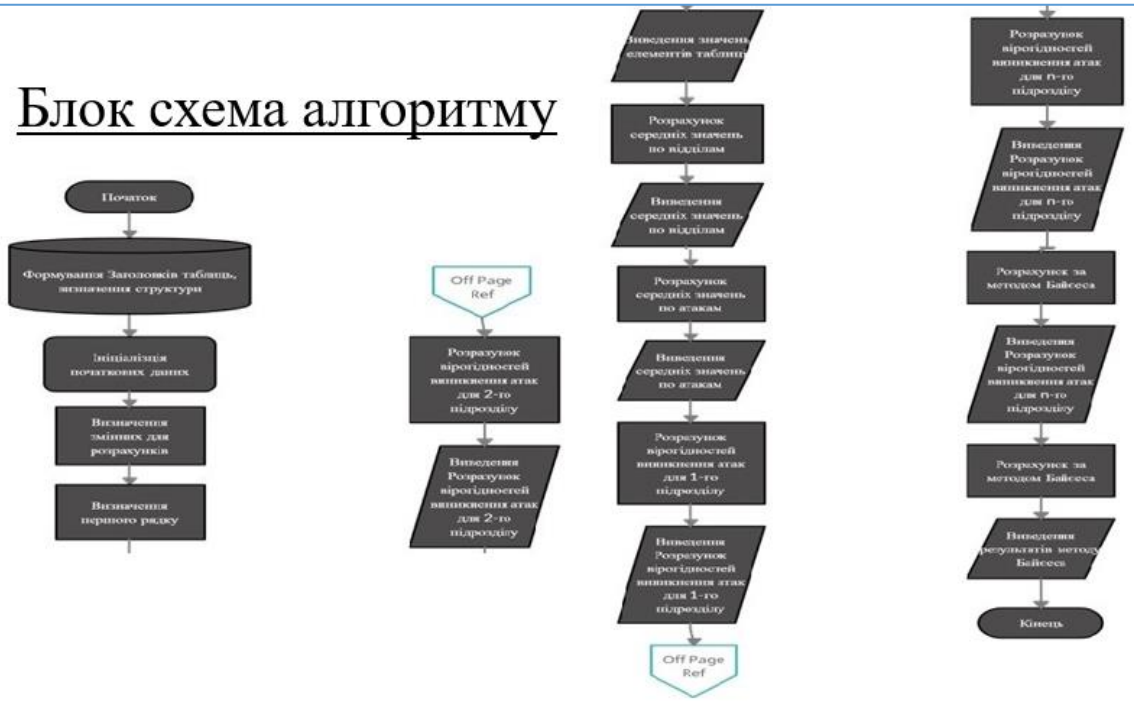
Threat Intelligence



Постановка задачі

Створити інструмент, який дозволяє розміщувати в табличній формі дані про атаки і розраховувати вірогідність реалізації цих атак з використанням формули Байєса.

Блок схема алгоритму



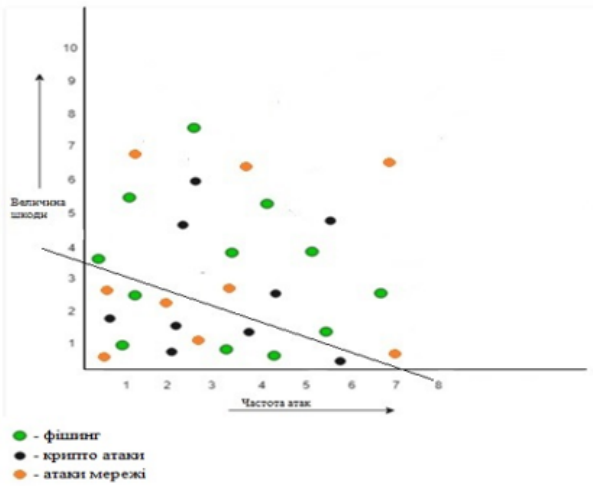
Вхідні дані

Системи	Фішинг	Крипто атаки	Атаки мережі	P(A)
Бухгалтерія	3	1	2	0.4
Відділ кадрів	2		2	0.267
Технічний відділ	2	2	1	0.333
P(B)	0.467	0.2	0.333	

Результати першого експерименту

Атака	Бухгалтерія	Відділ кадрів	Технічний відділ
Фішинг	0.501	0.5	0.401
Крипто атака	0.167	0	0.401
Атака мережі	0.333	0.499	0.2

Результати другого експерименту



Висновки

В результаті виконання кваліфікаційної роботи вирішено наступні задачі:

- проаналізовано основи інформаційної безпеки та проблем, які вона вирішує;
- знайдено приклади застосування методів Data Mining в захисті інформації;
- вдалося систематизувати методи класифікації інформації відносно застосування в криптології;
- визначено критерії обрання методів класифікаціїї для розв'язання конкретних задач кібербезпеки;
- показана можливість розподілу атак з визначенням найбільш критичних.

Розроблені структури аналітичних таблиць для аналізу та створений інструмент, який допомагає в проведенні досліджень з застосуванням методу Байєса.
В майбутньому створений інструмент може бути застосований службою кібербезпеки підприємства для попередження та реальної класифікації виявлених атак.

Дякую за увагу