МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ А.В. Ільєнко

«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.57

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»

Тема: Методи аналізу кіберзагроз в інформаційному просторі

Автор: Ю.І. Фіненко

Науковий керівник: к.т.н., доц. Н.К. Гулак

Нормоконтролер: асист. С.В. Єгоров

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Компютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання магістерської атестаційної роботи

магістранта Фіненка Юрія Івановича

1. Тема: Методи аналізу кіберзагроз в інформаційному просторі
затверджена наказом ректора від 02.10.2019 р. № 2265/ст.
2. Термін виконання з 14.10.2019 р. по 09.02.2020 р.
3. Вихідні дані: вибірка об'єктів, які завідомо до початку дослідження були класифіковані на два різні класи: «не містить кіберзагрозу», «містить кіберзагрозу»; методи аналізу кіберзагроз; методи математичної статистики; методи машинного навчання; програмне середовище «MATLAB».
4. Зміст пояснювальної записки: методи аналізу кіберзагроз; аналіз моделі загроз, моделі порушника на основі нормативно-правового регулювання законодавства України; аналіз математичних моделей методів аналізу кіберзагроз та каналів передачі прихованих кіберзагроз; розробка алгоритму класифікації кіберзагроз, який дозволяє зменшити кількість станів кіберзагроз у каналі зв'язку, що в свою чергу дозволяє зменшити кількість ресурсів на виконання первинного аналізу вхідної інформації.

КАЛЕНДАРНИЙ ПЛАН

виконання магістерської роботи

№ п/п	Етапи виконання магістерської роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	14.10.2019	Виконано
2.	Аналіз літературних джерел	15.10.2019-22.102019	Виконано
3.	Обґрунтування вибору рішення	23.10.2019-30.10.2019	Виконано
4.	Збір інформації	31.10.2019-15.11.2019	Виконано
5.	Дослідження існуючих сучасних методів аналізу кіберзагроз на основі правового-регулювання законодавства України	15.11.2019-10.12.2019	Виконано
6.	Аналіз математичних моделей аналізу даних та каналів передачі прихованих кіберзагроз	10.12.2019-01.01.2020	Виконано
7.	Розробка алгоритму для оцінки наявності прихованої кіберзагрози в каналі зв’язку	02.01.2020-12.01.2020	Виконано
8.	Апробація роботи на науково-технічній конференції Університету «Україна»	13.01.2020	Виконано
9.	Перевірка на антиплагіат	02.02.2020	Виконано
10.	Оформлення і друк пояснювальної записки	04.02.2020	Виконано
11.	Оформлення презентації	05.02.2020	Виконано
12.	Отримання рецензій від рецензента	08.02.2020	Виконано
13.	Захист в ЕК	09.02.2020	Виконано

Магістрант Ю. Фіненко

(підпис, дата)

Науковий керівник Н. Гулак

(підпис, дата)

РЕФЕРАТ

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 96 сторінок основного тексту, 37 рисунків, 6 таблиць, 5 сторінок додатків. Список використаних джерел містить 79 найменувань і займає 7 сторінок. Загальний обсяг роботи 108 сторінок.

Мета роботи. На підставі ретельного аналізу методів кіберзагроз обрати методи аналізу кіберзагроз та їх математичні моделі для розробки алгоритму що дозволив би підвищити ефективність методу за рахунок зменшення кількості станів кіберзагрози.

В роботі проаналізовано існуючі методи аналізу кіберзагроз в інформаційному просторі, проаналізувано математичні моделі аналізу кіберзагроз та канали управління кібератаками; розроблено алгоритм класифікації кіберзагроз, що дозволило зменшити кількість станів кіберзагроз у каналі зв’язку.

Розроблений алгоритм дає можливість пристосування технологій машинного навчання для захисту інформаційно-комунікаційних систем, завдяки скороченню ресурсів для аналізу первинних даних на предмет кіберзагроз.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням моделі і алгоритму та розробка прикладного програмно-технічного забезпечення відповідно до вимог міжнародних стандартів, для більш повноцінного аналізу прихованих кіберзагроз в існуючих та перспективних каналів зв’язку.

Ключові слова: МАШИННЕ НАВЧАННЯ, КІБЕРЗАГРОЗА, ІНФОРМАЦІЙНИЙ ПРОСТІР, КАНАЛ ЗВ’ЯЗКУ, МАТЕМАТИЧНА СТАТИСТИКА, АТАКА НА КІБЕРЗАГРОЗУ, МАТЕМАТИЧНА МОДЕЛЬ, БІНАРНА КЛАСИФІКАЦІЯ КАНАЛІВ ЗВ’ЯЗКУ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце;
ДССЗІ	–	Державна служба спеціального захисту інформації;
ІАД	–	інтелектуальний аналіз даних;
ІБ	–	інформаційна безпека;
ІС	–	інформаційна система;
ПЗ	–	програмне забезпечення;
СУІБ	–	система управління інформаційною безпекою;
ЦВК	–	центральна виборча комісія;
COBIT	–	Цілі управління інформаційними та суміжними технологіями;
CRAM	–	CCTA Аналіз ризиків та управління методами;
DARPA	–	Агентство прогресивних дослідницьких проектів в галузі оборони;
DDoS	–	Відмова в обслуговуванні;
EM	–	максимізація очікування;
JPEG	–	Joint Photographic Experts Group;
IP	–	Internet Protocol Address;
ISMS	–	Система управління інформаційною безпекою;
ISO	–	Міжнародна організація стандартизації;
ITIL	–	Бібліотека IT-інфраструктури;
LSB	–	Найменш значимий біт;
OLAP	–	Онлайн аналітична обробка;
UA-CERT	–	Комп'ютерна команда реагування на надзвичайні ситуації України.

ВСТУП

Актуальність. Протягом останніх років на інформаційно-телекомунікаційні системи деяких об’єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об’єктами критичної інфраструктури, здійснено низку масштабних кібератак, зокрема:

– 21 - 25 травня 2014 відбулися DDoS-атаки і злом сайту ЦВК під час президентських виборів, внаслідок яких на сайті з’явилися помилкові результати. Незважаючи на повідомлення про злом, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні [1];

– у червні 2014 року на серверах приватних компаній України і країн НАТО були виявлені шкідливі програми, які займалися кібершпіонажем. Серед них такі, як Turla/Uroburos/Snake, RedOctober, MiniDuke і NetTraveler [1];

– 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, у використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більше ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п’яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго [1];

– 6 грудня 2015 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, що вивела з ладу ряд комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень [1];

– 15 грудня 2015 року українські хакери на замовлення невстановленої особи із Санкт-Петербурга здійснили DDOS-атаку на сайт Укрзалізниці, внаслідок чого протягом дня була повністю заблокована його робота. Атака була націлена на крадіжку даних про пассажироперевезення [1];

– 17 грудня 2015 року кібератака на підстанцію “Північна” компанії “Укренерго” призвела до збою в автоматиці управління, через що більше години знеструмленими залишалися райони у північній частині правобережного Києва і прилеглі райони області [1];

– у першій половині дня 27 червня 2017 року розпочалася масова кібератака на український державний та комерційний сектор із застосування шкідливого програмного забезпечення – вірусу-шифрувальника файлів Petya Ransomware. Її жертвами стали інформаційно-телекомунікаційні системи “Укрпошти”, аеропорту “Бориспіль”, “Укренерго”, ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС та інших компаній [1].

У комп'ютерній безпеці різні методи машинного навчання давно застосовуються в фільтрації спаму, аналізі трафіку, при виявленні фроду або шкідливого програмного забезпечення. Однак є ще одна не менш важлива задача в сфері захисту інформації, це викриття прихованих кіберзагроз, які можуть завдати непоправної шкоди інформаційно-комунікаційним системам, які здійснюються через відкриті канали зв'язку ззовні, за допомогою методів приховування факту передачі. Аналіз і виявлення таких кіберзагроз та каналів управління ними є пріоритетними напрямками сфери кібербезпеки. Виділити з мільярдів сигналів і величезних масивів різноформатних даних інформацію, яка реально важлива для відбиття атаки, вкрай складно. Людина витратить на такий аналіз занадто багато часу. І, навпаки, система машинного навчання може проводити поведінковий аналіз мільярдів кіберінцидентів кожен день. Це дозволяє значно скоротити час реагування на кіберінциденти. Тому дане дослідження є пріоритетним і затребуваним сьогодні.

Використання методів аналізу кіберзагроз та машинного навчання дозволить ефективніше використовувати обмежені ресурси інформаційного простору. Тому розробка нових аналітичних методів для захисту інформації є актуальною науково-практичною задачею [3].

Для аналізу дослідження були розглянуті методи математичної статистики, за якими було показано різницю між різними каналами передачі кіберзагроз в інформаційному просторі [3].

Мета роботи. На підставі ретельного аналізу методів кіберзагроз обрати методи аналізу кіберзагроз та їх математичні моделі для розробки алгоритму що дозволив би підвищити ефективність методу за рахунок зменшення кількості станів кіберзагрози.

Для забезпечення поставленої мети, потрібно виконати ряд завдань:

– проаналізувати існуючі методи аналізу кіберзагроз в інформаційному просторі на основі нормативно-правового регулювання законодавства України;

– проаналізувати математичні моделі аналізу кіберзагроз та канали управління кібератаками;

– розробка алгоритму класифікації кіберзагроз, що дозволило зменшити кількість станів кіберзагроз у каналі зв’язку.

Галузь застосування. Розроблений алгоритм можливо використовувати в галузі кібербезпеки для підвищення ефективності існуючих методів та систем аналізу та систем захисту від кіберзагроз.

Об’єктом дослідження є процес аналізу та оцінки прихованих кіберзагроз в інформаційному просторі.

Предметом дослідження є канал зв’язку з прихованими кіберзагрозами.

Методи дослідження. Для вирішення означених вище наукових завдань в роботі використані методи системного аналізу, теорії інформаційної безпеки, методи аналізу кіберзагроз, методи математичної статистики та машинного навчання.

Наукова новизна отриманих результатів: На основі поєднання статистичних моделей та моделі кінцевих автоматів для аналізу кіберзагроз, було розроблено алгоритм класифікації кіберзагроз, що дозволило зменшити кількість станів кіберзагроз у каналі зв’язку, що в свою чергу дозволяє

зменшити кількість ресурсів на виконання первинного аналізу вхідної інформації.

Практичне значення отриманих результатів: Результатом дослідження дає можливість пристосування технологій машинного навчання для захисту інформаційно-комунікаційних систем, завдяки скороченню ресурсів для аналізу первинних даних на предмет кіберзагроз.

Апробація результатів.

1. Шматок А.С. Методы анализа критических данных на основе машинного обучения. / А.С. Шматок, Ю.И. Финенко // II міжнар. наук.-практ. конф. «Проблеми кібербезпеки інформаціно-телекомунікаційних систем (PCSITS)», «Київ, 11-13 квітня 3019 р.). – Київ, КНУ ім. Тараса Шевченка, 2019. – С. 21-23.

2. Шматок О.С. Штучний інтелект та машинне навчання в задачах стеганоаналізу даних. / О.С. Шматок, Ю.І. Фіненко, А.Б. Єлізаров, В.А. Телющенко // Всеукраїнська наук.-техн. конф. «Комп'ютерні технології: наука та освіта» (Київ, 13-14 січня 2020 р.) – Київ, Університет «Україна», 2019. С.219-227.

Розділ 1. Кіберзагрози та методи їх аналізу

1.1. Визначення проблеми

Відповідно до частини третьої статті 6 Закону України “Про основні засади забезпечення кібербезпеки України” Адміністрацією Держспецзв’язку розроблено проект постанови Кабінету Міністрів України “Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури” (далі – проект постанови) [4].

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.3015 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для вчинення терористичних актів [4].

Аналіз кіберзагроз свідчить, що кібератаки на комунікаційні системи та системи управління технологічними процесами об’єктів критичної інфраструктури держави таких галузей, як енергетика, хімічна промисловість та інші можуть призвести до виникнення надзвичайних ситуацій техногенного характеру та/або негативного впливу на стан екологічної безпеки держави [4].

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв’язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України [4].

Водночас Закон України “Про основні засади забезпечення кібербезпеки України” визначає, що до Переліку об’єктів критичної інфраструктури (далі – Перелік) можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та

фінансовому секторах; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами потенційно небезпечних технологій і виробництв [4].

Необхідність прийняття постанови зумовлена відсутністю відомостей щодо реального стану інформаційної безпеки на об'єктах критичної інфраструктури та, як наслідок, унеможливлює системний підхід до розв'язання проблеми захисту критичної інфраструктури на загальнодержавному рівні [4].

Проблеми забезпечення належного рівня інформаційної безпеки на об'єктах критичної інфраструктури не можуть бути розв'язані без існування систематизованого підходу до аналізу стану захисту інформації, який базувався би на реальних показниках, отриманих під час проведення незалежного аудиту інформаційної безпеки [4]. Проблема кіберзагроз впливає на різні групи суб'єкти ().

1.2. Основні поняття та визначення

Визначені правові і організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями і принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян в цій сфері, основні принципи координації їх діяльності по забезпеченню кібербезпеки [4].

Індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози [4].

Інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз [4].

Інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [4].

Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [4].

Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та

цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [4].

Кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем (рис. 1.1) [4].

Кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [4].

Кіберзлочинність - сукупність кіберзлочинів [4].

Кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [4].

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [4].

Кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням [4].

Кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням [4].

Кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням. Критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури [4].

Критично важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей [4].

Кіберзахисту підлягають інформаційно-комунікаційні системи усіх форм власності, в яких обробляються національні інформаційні ресурси і які використовуються в інтересах органів державної влади і місцевого самоврядування, правоохоронних органів і військових формувань, в сферах електронного управління, електронних державних послуг, електронної комерції, електронного документообігу, а також об'єкти критичної інформаційної інфраструктури. Перелік вказаних об’єктів має затверджуватися Кабінетом Міністрів України та наразі відсутній. До останніх можуть бути віднесені підприємства, установи і організації незалежно від форми власності: в області енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському і фінансовому секторах; у сферах водо-, газо- і електропостачання, водовідведення, виробництва продуктів харчування, сільського господарства, охорони здоров'я. Також до об'єктів критичної і відносяться комунальні, аварійні і рятувальні служби, стратегічні підприємства, потенційно небезпечні виробництва [4].

Слід зазначити, що дія закону № 3153 не поширюється, зокрема, на: відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або в технологічних системах; діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформації, необхідність захисту якої встановлено законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів; комунікаційні системи, які не взаємодіють із публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем) [4].

1.3. Модель загроз інформаційному просторі

Діяльність всіх осіб, що мають доступ до охоронюваним законом масивів особистої інформації, повинна спиратися на норми, введені «Моделлю». Модель бачить такі види об’єкти кібератак, категорії жертв та методи кібератак (рис. 1.1) [5].

Їх кроки, які посягають на збереження і цілісність захищених масивів відомостей, можуть принести шкоду інтересам особистості, суспільства, держави (рис 1.2) [5].

ДССЗІ розробило модель дій цих типів суб'єктів (рис. 1.3). Зазіхання, за версією документа, можуть відбуватися наступними шляхами [5]:

– перехоплення або знімання інформації, яка направляється по каналах зв'язку, для її копіювання або поширення з будь-якими цілями, такими, що суперечать законодавству [5];

– отримання неправомірного доступу до баз, в яких зберігаються номери паспортів, адреси, медичні історії. Доступ використовується не тільки

для копіювання або неправомірного поширення відомостей, а й для їх зміни, знищення, внесення спотворень в важливі параметри. Для деструктивних впливів використовуються спеціальні програмні та технічні засоби, при цьому оператори часто не мають готових відповідей на виклики, створені з використанням сучасних технологій (рис. 1.1) [5].

Рис. 1.1. Складові частини та жертви кібератаки

Рис. 1.2. Кіберпростір підприємства

Рис. 1.3. Суб’єкти і об’єкти кіберпростору

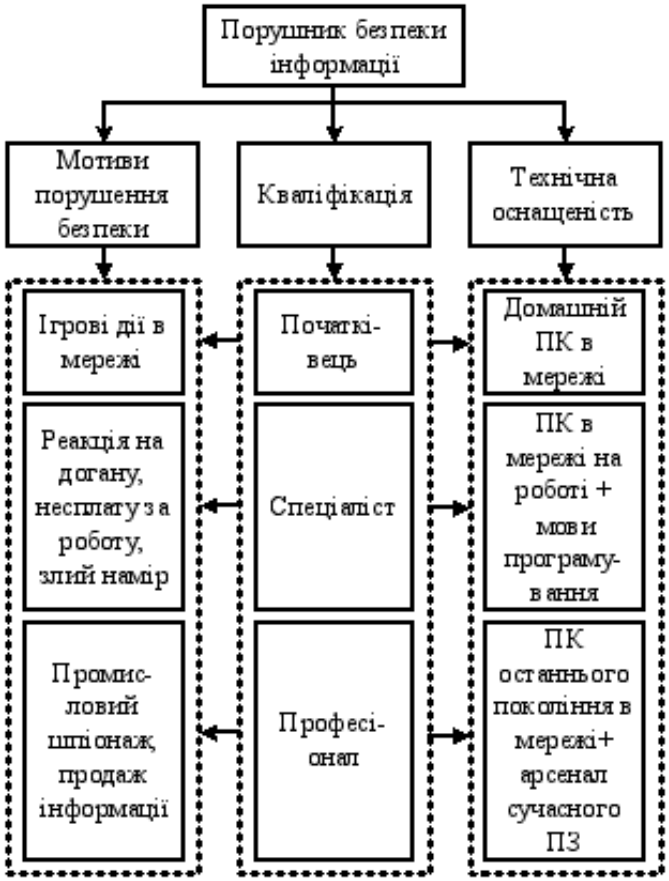


Рис. 1.4. Суб’єкти, які можуть завдати шкоди інформаційним системам

Рис. 1.5. Матеріальні засоби зберігання і обробки, яке необхідно захищати.

ДССЗІ, розробляючи свою модель загроз, було впевнено в тому, що з її допомогою кожен конкретний оператор зможе розробити власні методики захисту від загроз в інформаційному просторі власних підприємств. Для цього потрібно правильно використовувати матеріальні засоби зберігання і передачі (рис. 1.5) [5].

Відповідальність за працездатність і захищеність обладнання і мереж несуть їх власники [5].

Завдання, які вирішуються «Моделлю загроз»

Будь-який суб'єкт ринку, який потрапив до реєстру, повинен не тільки в будь-який момент бути готовим пройти перевірку ДССЗІ, але і вирішувати завдання, не передбачені чинною на поточний момент нормативною документацією, що стають новими викликами. До таких завдань відносяться [5]:

– розробка власних моделей загроз, актуальних для кожного конкретного особи, яка здійснює обробку персональних даних. Абсолютно різні цілі можуть бути в осіб, які зазіхають на інформацію, пов'язану з особистостями державних службовців, і тих злочинців, які цікавляться медичними картами пенсіонерів [5];

– аналіз і моніторинг поточної ситуації із захистом баз персональних даних від зовнішнього проникнення [5];

– розробка власної системи захисту баз даних і нейтралізації потенційних загроз, заснованої на пропонованих для кожної окремої системи методах і рекомендаціях [5];

– систематичне проведення заходів, які повинні виключити несанкціоноване проникнення до баз даних порушників - третіх осіб, яким не оформлений допуск до вивчення і обробці цієї інформації [5];

– організація технічної системи захисту засобів обробки даних, яка повинна виключити будь-який вплив на них, що може спричинити їх пошкодження або руйнування [5];

– постійний контроль якості захисту [5].

Модель загроз пропонує вивчити основні вразливі точки систем захисту, актуальні види загроз, доступні способи забезпечення інформаційної безпеки. UA-CERT проводить постійний моніторинг знову з'являються видів загроз, вносячи зміни в свої рекомендації [5].

Класифікація загроз (рис 1.6):

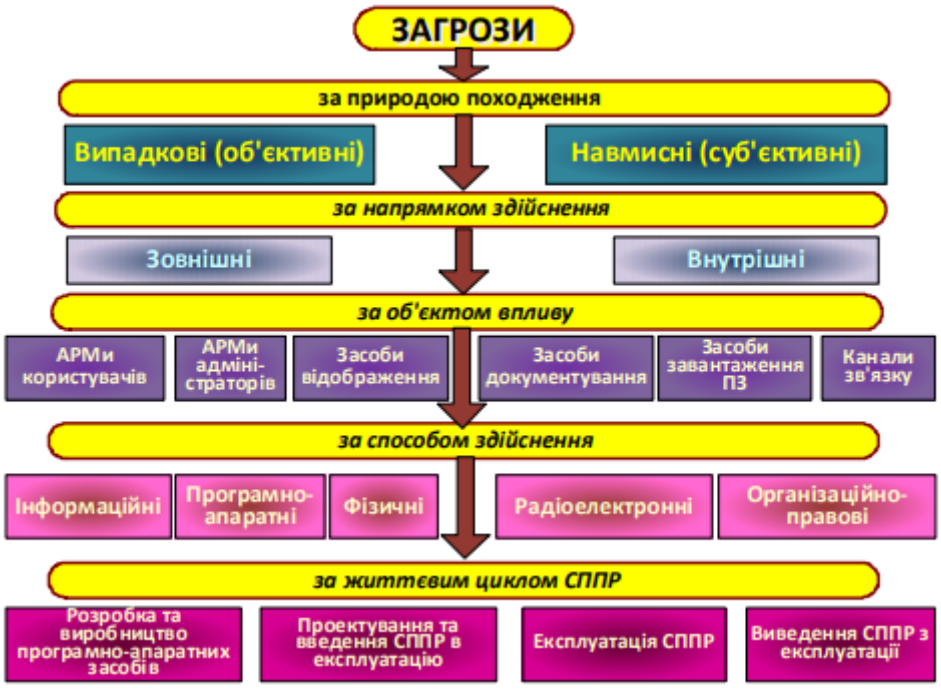


Рис. 1.6. Класифікація загроз

Неможливо боротися з будь-якими загрозами, якщо не розуміти їх походження, ступеня серйозності, інших параметрів. Вирішенню цього завдання допоможе запропонована класифікація загроз. Відомство в моделі пропонує наступне визначення загрози: це сукупність зовнішніх і внутрішніх факторів або умов, які дозволяють зловмисникам навмисно або ненавмисно отримати доступ до охоронюваної інформації, завдяки чому стає можливим її несанкціоноване [5]:

– знищення (стирання з пам'яті комп'ютера);
– блокування доступу до неї;
– поширення серед обмеженого або широкого кола осіб;
– зміна;
– копіювання;
– будь-які інші дії, не передбачені встановленими правилами обробки відомостей в інформаційних системах персональних даних [5].

Ризики можуть носити як особистісний, пов'язаний з наміром третіх осіб, так і знеособлений, техногенний, характер, пов'язаний з помилками або необережністю обслуговуючого персоналу. Сукупність факторів і умов для кожної окремої системи матиме індивідуальний характер, який складається з характеристик конкретної ІС, середовища та шляхів поширення інформаційних сигналів, технічних та інших можливостей, наявних у джерел потенційних загроз [5].

Характеристики ІС, які впливають на появу нових загроз і ризиків [5]:

– обсяг і зміст відомостей, наявних в базі;
– структура та конфігурація системи;
– наявність підключення системи до мереж передачі інформації загального користування або мереж, за якими проводиться транскордонне спілкування;
– наявність і якість систем захисту;
– режим, в якому обробляються персональні дані;

– наявність різнорівневої системи доступу осіб з різним обсягом повноважень і завдань до даних;

– фізичне місцезнаходження технічних пристроїв, режим їх захисту від протиправного посягання [5].

При цьому властивості середовища поширення сигналів враховуються з різних точок зору, часто отримати доступ до охоронюваним відомостями можна, використовуючи лінії підключення до електричних мереж, шляхом знімання інформації про зміну електромагнітного випромінювання [5].

Повністю досі не виключена можливість підслуховування і збереження звукової інформації за допомогою пристроїв звукозапису [5].

При аналізі джерел загроз необхідно вивчити такі їх типи, як можливості, що виникають у зв'язку з використанням службового становища, технічні, програмні, фізичні. Будь-яка загроза отримує свою реалізацію на практиці в той момент, коли між суб'єктом, що має намір здійснити протиправну дію, і об'єктом, що охороняється виникає канал доступу, що призводить до можливості виникнення несанкціонованого, усвідомленого або випадкового доступу до об'єкта [5].

Аналізуючи загрози, що виникають при обробці персональних даних, спираючись на багатогранність можливостей отримання доступу до інформації, модель виділяє такі їх класи [6]:

– внутрішні, інсайдерські – ризики викрадення або зміни відомостей виникають при реалізації можливостей внутрішнього користувача, доступ до інформаційних систем він отримує внаслідок свого службового становища, роботи в компанії або держструктурі [6];

– зовнішні - суб'єкт загроз отримує можливість несанкціонованого доступу до об'єкта захисту, використовуючи можливості мереж загального користування [6];

– технічні - виникають при використанні можливостей апаратних закладок і програм, призначених для розкрадання електронних відомостей [6].

Всі ці типи загроз вимагають серйозного аналізу особистостей співробітників, що мають доступ до чутливої інформації, і підвищеної уваги до технічної захищеності засобів зберігання і обробки даних з використанням спеціалізованих програмних засобів, DLP-систем, SIEM-систем, а також засобів захисту інформаційних ресурсів [6].

Також в моделі дається класифікація, заснована на різних типах використовуваного обладнання [6]:

– загрози безпеці тим даних, які обробляються співробітником на його робочому місці (АРМ), що не підключеному до мереж Інтернет [6];

– загрози відомостями, які обробляються співробітником на його робочому місці, підключеному до мереж Інтернет [6];

– погрози тим інформаційним масивам, які обробляються в локальних мережах, які не підключені до мереж Інтернет [6];

– погрози тим масивам, з якими працюють в локальних мережах підприємств і організацій, що мають вихід в Інтернет [6];

– загрози безпеці тих даних, які обробляються в розподілених мережах операторів і підключених, і не підключених до мереж міжнародного інформаційного обміну (Інтернет) [6].

Також в моделі загроз безпеки пропонується класифікація, пов'язана з різними типами технічних засобів, завдяки яким здійснюється доступ до охоронюваним масивів інформації [6]:

– використання шкідливих програм, вірусів, хробаків і аналогічних, що створюються з свідомо протиправними цілями;

– втрати даних з технічних і фізичних каналах витоку;

– інших спеціальних впливів [6].

За типами уразливості засобів захисту і технічних засобів, встановлених у конкретного оператора, модель загроз виділяє наступні [6]:

– пов'язані з уразливістю системного програмного забезпечення [6];

– пов'язані з використанням недоліків прикладного ПО [6];

– пов'язані з можливостями застосування апаратних закладок [6];

– пов'язані з використанням засобів зв'язку та протоколів передачі інформації [6];

– пов'язані із застосуванням технічних каналів передачі даних (наприклад, телефонних мереж, мереж електроживлення) [6].

Для виявлення цих точок уразливості необхідне проведення регулярного аудиту безпеки і систем захисту інформації. Крім аналізу можливостей доступу передбачуваних порушників режиму конфіденційності до засобів комп'ютерної обробки відомостей, необхідно мати на увазі, що практично будь-який офісне технічний засіб може стати потенційним джерелом загрози. Модель безпеки класифікує їх так [6]:

– АРМ;

– виділені засоби обробки (принтери, копіювальні апарати, звукозаписна апаратура, засоби відеоспостереження;

– мережі зв’язку [6].

Технічні канали витоку

Практика показує, що більша частина території, що охороняється інформації витікає з технічних каналам передачі даних. Сигнал поширюється в певній фізичному середовищі, він може бути акустичним або електромагнітним, його перехоплення здійснюється за допомогою закладних пристроїв і іншими шляхами. Пристрої можуть перехоплювати дані електромагнітного випромінювання, акустичну та візуальну інформацію. Захист від цього способу перехоплення здійснюється шляхом обмеження доступу на об'єкт, що охороняється [6].

Несанкціонований доступ

Дуже рідко організація може повністю захистити дані від дій власних співробітників. Для заподіяння шкоди даними можуть використовуватися [6]:

– штатне програмне забезпечення, що дозволяє потрапити в операційну середу;

– створення позаштатних умов роботи, що дозволяє використовувати одержувані спотворення для модифікації даних;

– шкідливі програми;

– загрози, пов'язані з віддаленим доступом;

– комбіновані загрози [6].

Для боротьби з ними необхідні установка захисного ПЗ, регулярний моніторинг функціонування робочих станцій. Крім того, ДССЗІ та UA-CERT проводять перевірки відповідності готовності технічних систем операторів і видає розпорядження, що дозволяють збільшити ступінь захищеності. Не завжди для цього потрібні серйозні фінансові кошти. Стандартні заходи безпеки і дотримання інструкцій допомагають забезпечити до 90% збереження даних [6].

1.4. Модель порушника

Якщо існує інформаційна система, у якій циркулює інформація з обмеженим доступом та конфіденційні дані, то знайдеться особа (порушник), метою якої буде ознайомлення з інформацією, її модифікація чи знищення. Для того, щоб розробити комплекс заходів по забезпеченню захищеності інформаційних ресурсів, необхідно побудувати модель можливого порушника. Ця модель може бути побудована з урахування різних критеріїв [5].

Модель порушника розробляється для того, щоб отримати відповіді на наступні питання [5]:

– від кого захищати інформацію?

– яка мета порушника?

– якими знаннями володіє порушник?

– які повноваження в системі має потенційний порушник?

– якими методами і засобами користується порушник?

– яка обізнаність порушника щодо об’єкта інформаційної діяльності і системи охорони [5]?

Інформація – відомості про об’єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які зменшують наявну про них ступінь невизначеності, неповноти знань [5].

Теоретична інформатика розглядає інформацію як концептуально зв’язані між собою відомості, дані, поняття, що змінюють уявлення про явище або об’єкт навколишнього світу. Поряд з інформацією в інформатиці часто використовують поняття дані. Дані можуть розглядатися як ознаки або записані спостереження, які з будь яких причин не використовуються, а тільки зберігаються. У тому випадку, якщо з’являється можливість використати ці дані для визначення невизначеності будь-чого, дані перетворюються в інформацію. Тобто інформація – це дані, які використовуються [5].

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники - це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп’ютерної системи. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть працювати в даній системі. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації; порушники пропускного режиму [5].

При розробці моделі порушника необхідно визначитись, що і у якій мірі має відображати отримана модель. Для цього необхідно визначитись з необхідним ступенем деталізації моделі порушника [5].

Можна запропонувати наступні ступені деталізації [5]:

– змістовна модель порушників - відображає причини й мотивацію дій порушників, переслідувані ними цілі і загальний характер дій у процесі підготовки і здійснення порушення інформаційної безпеки. Побудувавши змістовну модель, адміністратори безпеки можуть визначити мету порушника, його рівень знань, кваліфікацію, розташування та т.п [5].

– сценарії впливу порушників - визначають класифіковані типи порушень з конкретизацією алгоритмів і етапів, а також способи дії на кожному етапі. Розробивши сценарії впливу, адміністратори безпеки отримають можливу послідовність дій зловмисника для нанесення збитків інформаційним ресурсам [5].

– математична модель впливу порушників представляє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що параметрично характеризують результати дій, і функціональних (аналітичних, числових чи алгоритмічних) залежностей, які описують процеси взаємодії порушників з елементами об’єкту і системи охорони. Цей вид моделі слід використовувати для кількісних оцінок вразливості об’єкту і ефективності охорони [5].

Для того, щоб модель порушника найбільш точно і детально характеризувала порушників, алгоритм їх дій і давала кількісні оцінки вразливості об’єкту і ефективності охорони рекомендується розробляти комплексну модель з урахуванням усіх ступенів деталізації [5].

Способи класифікацій порушників

Під час побудови моделі порушника спочатку необхідно проаналізувати усіх користувачів системи, розподілити їх за категоріями та визначити найбільш критичні. Користувачі таких категорій будуть прийняті як можливі внутрішні порушники системи. Далі необхідно визначитись, які категорії відвідувачів можуть бути зовнішніми порушниками [5].

Усіх можливих порушників необхідно класифікувати за різними показниками для того, щоб надалі скласти модель порушника. Нижче наведені можливі види класифікацій [5]:

– Класифікація порушників інформаційної безпеки за метою порушення. Класифікація за метою порушення проводиться для визначення мотивів порушника. Дії порушника в залежності від мети можуть бути спрямовані як на інформацію, так і на матеріальні носії інформації. Знаючи мету порушника, адміністратори безпеки будуть орієнтуватись, на захист якого ресурсу необхідно приділити більше уваги першочергово [5].

– Класифікація порушників інформаційної безпеки за рівнем знань про автоматизовані системи. Кожен порушник має певний рівень кваліфікації та поінформованості відносно організації функціонування лабораторії зовнішніх та внутрішніх мереж інформаційного комп'ютерного комплексу. В залежності від рівня знань, якими володіє порушник, може бути нанесений певний рівень збитків інформаційним ресурсам організації. В класифікації враховуються знання можливого порушника та його практичні навички у роботі з комп'ютерними системами та інформаційними технологіями [5].

– Класифікація порушника за місцем дії. Ця класифікація проводиться для визначення розташування порушника відносно організації під час здійснення спроби несанкціонованого доступу до інформаційного ресурсу [5].

– Класифікація порушників за методами і способами, якими вони користуються. Порушник може отримати конфіденційну інформацію та інформацію з обмеженим доступом, користуючись при цьому різними методами та засобами. Порушення може бути скоєне або з використанням певних засобів для отримання інформації, або без них. Методи можуть бути різними, як дозволеними, так і забороненими. Дозволеним вважається отримання інформації без порушення прав власності. Як приклад можна привести використання методів соціальної інженерії [5].

– Класифікація порушників за рівнем можливостей, які надані їм засобами автоматизованої системи та обчислювальної техніки. Внутрішніх порушників можна класифікувати за наданим рівнем повноважень у системі. Адже чим більше повноважень, там більше можливостей доступу до інформації з обмеженим доступом [5].

– Класифікація порушників за мотивом порушень. Зловмисники можуть порушувати інформаційну безпеку з різних причин. Порушення можна розбити на дві групи - навмисні та ненавмисні. Особи, які ненавмисно наносять збитків інформаційним ресурсам, порушуючи конфіденційність, цілісність або доступність інформації, не складають плану дій, не мають мети та спеціальних методів та засобів реалізації запланованого порушення. Ненавмисні порушення частіше всього здійснюються в результаті недостатньої кваліфікації, неуважності персоналу. Порушники, які наносять збитків інформаційним ресурсам навмисно, мають певну мету, готують план реалізації атаки на інформаційний ресурс. Навмисні порушення інформаційної безпеки здійснюються для нанесення збитків організації (матеріальних чи моральних), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів [5].

1.5. Сучасні кіберзагрози інформаційному простору

Виділяють наступні сучасні кіберзагрози [7]:

– соціальна інженерія та фішинг;

– вірусне програмне забезпечення;

– використання неактуальних версій програмного забезпечення;

– інсайдерські загрози;

– відсутність політик і процедур щодо поводження з інформаційними ресурсами [7].

Соціальна інженерія і фішинг.

Соціальна інженерія базується на експлуатації людських слабкостей. В результаті успішного психологічного підстроювання до жертви досвідчений зловмисник може виявити багато базових моментів в роботі організації для планування злому, викрадення інформації. Це і робота системи контролю фізичного доступу, робота охорони, графік роботи прибиральниць, місцезнаходження принтерів, сміттєвих кошиків, наявність шредерів і т. д. Підготовка до проникнення в інформаційну систему організації починається саме з такої роботи [7].

Фішингові атаки є продовженням соціальної інженерії. Багатьма фахівцями вони визнаються найбільш масовим і ефективним засобом злому і подальшого доступу до ресурсів підприємств і організацій всіх форм власності. За різними оцінками, до 90% всіх успішних кібератак відбуваються з використанням даного методу. Метод, по суті, дуже простий і являє собою розсилку підроблених листів електронної пошти, текст яких спонукає передбачувану жертву запустити вірусну програму, замасковану, наприклад, під офісний додаток, або перейти по посиланню на підроблений сайт, на якому вам запропонують ввести свій логін і пароль до пошти або інших ресурсів [7].

Вірусне програмне забезпечення.

Це найважливіша зброю зловмисників, для захисту від якого необхідно мати актуальну версію антивірусного програмного забезпечення. Не існує антивірусного ПЗ, яке б захищало від всіх вірусів однаково добре. Як показує практика, дуже корисний обмін інформацією між фахівцями про початок атак і появі нових вірусів, а також використання служб з аналізу підозрілих файлів і посилань на предмет виявлення черв'яків, троянів і всіляких шкідливих програм (рис. 1.7, рис. 1.8.) [7].

Рис. 1.7. Етапи злому інформаційної системи

Рис. 1.8. Механізм роботи кіберзагроз на інформаційні системи

Неактуальні версії програмного забезпечення.

По суті, ця вразливість інформаційної системи, коли Ви пропустите установку необхідних оновлень ПЗ. Регулярне оновлення ПЗ необхідно з багатьох причин, одна з яких - підвищення рівня безпеки та захист від нововиявлених вразливостей і загроз. Потрібно працювати з персоналом в цьому напрямку, робити регулярні розсилки і нагадування для співробітників, показувати на прикладах, до чого може привести використання неактуальною версії ПЗ [7].

Інсайдерські загрози.

Це велика група загроз, джерелом яких є власні співробітники. поширена в організаціях, де відсутній контроль за наданням прав доступу високого рівня, а також розмежування з прав доступу до інформаційних ресурсів. Дуже добре, якщо регулярно проводиться хоча б мінімальна оцінка лояльності співробітників при прийомі на роботу, в процесі роботи і при звільненні. Персонал - це завжди найслабша ланка в системі безпеки і з ним потрібно постійно працювати. Не дарма британські та американські фахівці з безпеки будують свою роботу саме з розвитку культури безпеки [7].

Відсутність політик і процедур щодо поводження з інформаційними активами.

Політики і процедури - це встановлені правила роботи в інформаційній системі організації, а також розподіл ролей і відповідальності. Без них настає хаос, можливі фінансові втрати через неефективне використання ресурсів, виникає підвищений ризик помилок персоналу, ненавмисна витік та втрата інформації. При їх наявності, навпаки, користувач може сам вирішувати багато питань і працювати в чітко окресленому полі. При успішно працюючій процедурі надання прав доступу виконується одна з базових правил інформаційної безпеки - доступ тільки до того, що необхідно по роботі [7].

При наявності правильно працюють політик безпеки не виникає питань, хто за що відповідає, які ресурси слід захищати в першу чергу, до кого звертатися в разі настання інцидентів кібербезпеки і скільки часу організація

може працювати без серйозних втрат в разі тимчасової зупинки тих чи інших процесів. Все це можна розрахувати заздалегідь в ході виконання процедури оцінки ризиків та аналізу наслідків інцидентів для бізнесу [7].

За інноваційними аналітичними моделями DARPA кіберзагрози поділяються [7]:

– загрози підключення до каналів зв’язку;
– загрози наявності недокументованих можливостей;
– загрози зняття інформації в момент передачі по мережі;
– загрози підміни інформації в каналі управління;

Загроза підключення до каналів зв’язку [7].

Цифрова обробка сигналів дає можливість копіювання («відгалуження») трафіку в межах комунікаційної мережі без яких би то не було демаскуючих ознак. Факт копіювання неможливо відстежити, він не викликає зміни в каналі зв’язку, ні спотворень, пов'язаних з задержкою передачі. Це є якісною відмінністю сучасних інформаційних систем і мереж [7].

Загрози наявності недокументованих можливостей.

Недокументовані можливості самих систем (в особливості IP-мереж) є ще однією загрозою для конфіденційності інформації в системах, які захищаються. Програмне забезпечення систем обробки інформації являє собою складний програмний комплекс, в т.ч. який реалізує стек протоколів TCP / IP, і може містити [7]:

– недокументовані можливості, внесені розробниками з метою тестування або на певних етапах розробки нових функціональних можливостей систем [7];
– помилки в реалізації, наприклад, що призводять до уразливостей класу «переповнення буфера», і дозволяють отримати повний контроль над програмним забезпеченням системи до її перезавантаження [7].

Загрози зняття інформації в момент передачі по мережі.

Різні варіанти реалізацій загроз прослуховування трафіку традиційні для комп'ютерних мереж, що використовують у своїй структурі широкомовні

сегменти (Ethernet, в т.ч. комутований, радіо-Ethernet і т.п.), і створюють ще один рівень можливих атак на системи IP-мереж. При відсутності шифрування трафіку на мережевому або більш високих рівнях моделі OSI існує кілька варіантів порушення конфіденційності переданих повідомлень [7].

При отриманні зловмисником адміністративних прав на комутуюче або маршрутизуючого обладнання (наприклад, в результаті атаки на комп'ютер адміністратора або при перехопленні його пароля, що передається у відкритому вигляді) у нього з'являються набагато могутніші засоби перехоплення IP-трафіку [7].

Методика централізованого управління IP-пристроями та комп’ютерами містить ще один можливий шлях прозорого для абонентів перехоплення їх даних. У момент встановлення IP-з'єднання початковий обмін інформацією, що містить їх імена, технічні можливості систем і т.п., в т.ч. IP-адреси кінцевих пристроїв, йде між серверами IP-мереж. На цьому етапі можлива підміна (засобами атак мережевого рівня) інформації про один або обох IP-адреси з метою впровадження противника в ланцюжок передачі трафіку за принципом прозорого проксі-сервера [7].

Подібний клас атак залишається абсолютно непомітним на прикладному рівні, тому що користувачу зазвичай не видно мережеві координати віддаленого абоненту, а стек протоколів не здатний показати факт підміни, і може бути виявлений тільки за допомогою спеціалізованого моніторингу мережевого трафіку [7].

1.6. Методи аналізу моделей кіберзагроз

Аналіз загроз інформаційній безпеці дозволяє виділити складові сучасних комп'ютерних загроз - їх джерела і рушійні сили, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріальної, так і нематеріальної, і вироблення адекватних заходів протидії [8].

При аналізі загроз інформаційній безпеці використовуються наступні методи (рис. 1.9) [8]:

Рис. 1.9. Класифікація методів аналізу кіберзагроз

Розглянемо наведені методи докладніше [8]:

Пряма експертна оцінка. Метод експертних оцінок заснований на тому, що параметри загроз задаються експертами. Експерти визначають переліки параметрів, що характеризують загрози інформаційній безпеці, і дають суб'єктивні коефіцієнти важливості кожного параметра [8].

Статистичний аналіз - це аналіз інформаційних загроз на основі накопичених даних про інциденти інформаційної безпеки, зокрема, про частоту виникнення загроз певного типу, їх джерела та причини успіху чи неуспіху реалізації. Наприклад, знання частоти появи загрози дозволяє визначити ймовірність її виникнення за певний проміжок часу. Для ефективного застосування статистичного методу потрібна наявність досить великий за обсягом бази даних про інциденти. Потрібно відзначити ще одну вимогу: при використанні великого об’єму інформації необхідні інструменти узагальнення даних і виявлення в базі вже відомої та нової інформації [8].

Аналіз заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тим або іншим негативним наслідкам. Такими факторами можуть бути наявність привабливих для кіберзлочинців інформаційних активів, уразливості інформаційної системи, високий рівень вірусної активності в зовнішньому середовищі і т.д. Оскільки на сучасні

інформаційні системи впливають безліч чинників, зазвичай використовується багатофакторний аналіз [8].

При аналізі загроз інформаційній безпеці найбільш ефективно застосовувати комплекс різних аналітичних методів. Це значно підвищує точність оцінки [8].

Методів інтелектуального аналізу

Технології аналізу даних, що базуються на застосуванні класичних статистичних підходів, мають низку недоліків. Відповідні методи ґрунтуються на використанні усереднених показників, на підставі яких важко з'ясувати справжній стан справ у досліджуваній сфері. Методи математичної статистики виявилися корисними насамперед для перевірки заздалегідь сформульованих гіпотез та «грубого» розвідницького аналізу, що становить основу оперативної аналітичної обробки даних (OLAP). Окрім того, стандартні статистичні методи відкидають (нехтують) нетипові спостереження – так звані піки та сплески. Проте окремі нетипові значення можуть становити самостійний інтерес для дослідження, характеризуючи деякі виняткові, але важливі явища [8].

Ці недоліки статистичних методів спонукали до розвитку нових методів дослідження складних систем, які останнім часом все частіше застосовуються для вирішення практичних завдань – методів інтелектуального аналізу даних. Інтелектуальний аналіз даних (далі ІАД) – виявлення прихованих закономірностей або взаємозв'язків між змінними у великих масивах необроблених даних [8].

Сфера застосування ІАД нічим не обмежена – вона скрізь, де є якісь дані. Але насамперед методи ІАД сьогодні зацікавили комерційні підприємства, що розгортають свої проекти на основі інформаційних сховищ даних (Data Warehousing). ІАД являють собою велику цінність для керівників і аналітиків у їх повсякденній діяльності. Ділові люди усвідомили, що за допомогою методів ІАД вони можуть одержати відчутні переваги у конкурентній

боротьбі. Досвід багатьох підприємств показує, що віддача від використання ІАД може сягати 1000 % [8].

В англомовній літературі замість терміна «інтелектуальний аналіз даних» зазвичай використовується термін Data Mining (дослівний переклад – «видобуток даних»). «Data Mining – це процес виявлення в сирих даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для ухвалення рішень в різних сферах людської діяльності» [8].

В основу інтелектуального аналізу покладена концепція шаблонів (паттернів), що відбивають фрагменти багатоаспектних взаємин у даних. Ці шаблони являють собою закономірності, властиві підвибіркам даних, які можуть бути компактно виражені у зрозумілій людині формі. Пошук шаблонів проводиться методами, не обмеженими апріорними припущеннями про структуру вибірки, та видами розподілів значень аналізованих показників. Важливе положення інтелектуального аналізу – нетривіальність розшукуваних шаблонів. Це означає, що знайдені шаблони повинні відбивати неочевидні, несподівані регулярності в даних, що становлять так звані приховані знання. До суспільства прийшло розуміння, що сирі дані містять глибинний шар знань, за грамотного «розкопування» якого можуть бути виявлені справжні «самородки» [8].

Розглянемо основні задачі, які вирішуються методами Data Mining:

– класифікація – віднесення об'єктів (спостережень, подій) до одного з заздалегідь відомих класів [9];

– регресія (в тому числі задачі прогнозування) – встановлення залежності безперервних вихідних від вхідних змінних [9];

– кластеризація – угруповання об'єктів (спостережень, подій) на основі даних (властивостей), що описують сутність цих об'єктів, у кластери. Об'єкти всередині кластера повинні бути «схожими» один на одного і відрізнятися від об'єктів, що ввійшли в інші кластери. Чим більше схожі

об'єкти всередині кластера і чим більше відмінностей між кластерами, тим точніша кластеризація [9];

– асоціація – виявлення закономірностей між пов'язаними подіями. Прикладом такої закономірності служить правило, яке вказує, що з події X слід подія Y. Такі правила називаються асоціативними. Вперше ця задача була запропонована для знаходження типових шаблонів покупок, що здійснюються в супермаркетах, тому іноді її ще називають аналізом ринкової корзини (market basket analysis) [9];

– послідовні шаблони – встановлення закономірностей між пов'язаними в часі подіями, тобто виявлення залежності, що якщо відбудеться подія X, то через заданий час відбудеться подія Y [9];

– аналіз відхилень – виявлення найбільш нехарактерних шаблонів.

Інтелектуальний аналіз даних може допомогти у вирішенні проблем інформаційної безпеки шляхом пошуку моделей, асоціацій, кореляцій, які приховані в інформації, що зберігається в базах даних або передаються по каналам зв’язку [10, 11, 12].

1.7. Система управління інформаційною безпекою

Система управління інформаційною безпекою (Information Security Management System, ISMS) – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов’язки, процедури, процеси і ресурси [6].

Найбільш значущою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації [6].

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов’язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей [6].

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки на підприємстві. Слід зазначити, що тут перераховано не повний список (рис. 1.10) [6].

Рис. 1.10. Система управління інформаційною безпекою.

Побудова СУІБ дозволяє чітко визначити, як взаємопов’язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування, і т.д [6].

Основні функції системи управління інформаційною безпекою:

– виявлення та аналіз ризиків інформаційної безпеки;

- планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;
- контроль цих процесів;
- внесення в процеси мінімізації інформаційних ризиків необхідних коригувань [6].

Якісне управління інформаційною безпекою базується на наступних принципах [6]:

- комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;
- узгодженість з бізнес-задачами і стратегією підприємства;
- високий рівень керованості;
- адекватність інформації, яка використовується і генерується;
- ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;
- безперервність управління;
- процесний підхід – зв’язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв’язку між етапами [6].

Одним з ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 31801.

Міжнародний стандарт ISO 31801 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків. СУІБ забезпечує вибір адекватних і пропорційних методів і засобів контролю та захисту інформації і, тим самим, довіру зацікавлених сторін [6].

Проте слід брати до уваги й інші стандарти в сфері інформаційної безпеки. На даний момент у світовій практиці використовується велика кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад ISM3, COBIT, ITIL / ITSM, BSI-100-3, ISO13335-4, CRAMM, ISO15408. Але варто відмітити, що всі вони сумісні з ISO 31801, а також подобні до нього [6].

1.8. Висновок до розділу

В даному розділі на основі Закону України «Про основні засади забезпечення кібербезпеки України» розглянуто перелік загроз і рекомендацій щодо їх усунення, на які не завжди керівники і власники бізнесу, керівники державних організацій звертають належну увагу. Хоча важливість цих загроз, від яких захищаються далеко не завжди технічними заходами, складно переоцінити.

Багато хто намагається сховатися за технологією, ігноруючи роботу з людьми і процедури. Потрібно приділяти достатню увагу всієї тріаді безпеки: люди, процедури, технології. Кібергігієна вже давно широко застосовується в ефективно працюючих компаніях всього світу. Знаючи свої ризики, необхідно працюйте з людьми, впроваджувати технології та регулювати правила роботи з політиками і процедурами.

При досліджені різних видів кіберзагроз основною і часто надважливою складовою є канал зв’язку жертви в інформаційній системі і системи управління зловмисника, або інсайдера з його кураторами. Часто даний канал зв’язку є прихований. Тому дослідження даних каналів зв’язку є найважливішим з етапів дослідження кіберзагроз в цілому.

Розділ 2. Аналіз кіберзагроз, машинне навчання

2.1. Моделі аналізу кіберзагроз

На основі аналізу літератури по системам виявлення і аналізу кіберзагроз, наведені методи як правило не мають достатнього математичного опису. В основному вони формалізовані у вигляді способів і функцій засобів виявлення кіберзагроз, які використовуються в інструментальних засобах попередження і виявлення кіберзагроз [2, 4]. Проблемні питання протидії комп'ютерним кіберзагрозам в сучасній літературі самостійного відображення не знайшли, тому аналіз розглянутих методів здійснено для відомих методів виявлення та аналізу кіберзагроз. Методи виявлення та аналізу несанкціонованих впливів на ресурс інформаційної системи можна розділити на (рис. 2.1):

- методи сигнатурного аналізу,
- методи евристичного аналізу.

Методи сигнатурний аналізу призначені для виявлення відомих кіберзагроз, що засновані на контролі програм і даних в ІС, еталонних послідовностей символів, подій в мережі з базою даних сигнатур кіберзагроз. Вихідними даними для застосування методів служать відомості з системних журналів загального і спеціального програмного забезпечення, баз даних і ключові слова мережевого трафіку ІС. Перевагою даних методів є незначні вимоги до обчислювальних ресурсів ІС, збереження високої оперативності виконання технологічного циклу управління (ТЦУ) в ІС і достовірності виявлення і аналізу кіберзагроз. Недоліком методів сигнатурного аналізу є неможливість виявлення нових (модифікованих) кіберзагроз без суворої формалізації ключових слів мережевого трафіку і оновлення бази даних сигнатур кіберзагроз [66, 67].

Методи евристичного аналізу призначені для виявлення невідомих кіберзагроз. Принцип їх дії полягає в тому, що виявляється аномальна поведінка ІС відмінне від типового і на підставі цього факту приймається рішення про можливу наявність кіберзагрози. Евристичний аналіз в мережі

здійснюється за ознаками комп'ютерних кіберзагроз, таким як рідкісні типи стеків протоколів (інтерфейсів) для запиту інформації, довгі пакети даних, пакети з рідкісними розподілами символів, нестандартна форма запиту до масиву даних.

Для застосування методів евристичного аналізу і зменшення числа помилкових спрацьовувань необхідні чіткі знання про регламентах обробки даних і вимогах до забезпечення безпеки інформації (встановленому порядку адміністрування), оновлення контрольованих програм, тощо [68, 69].

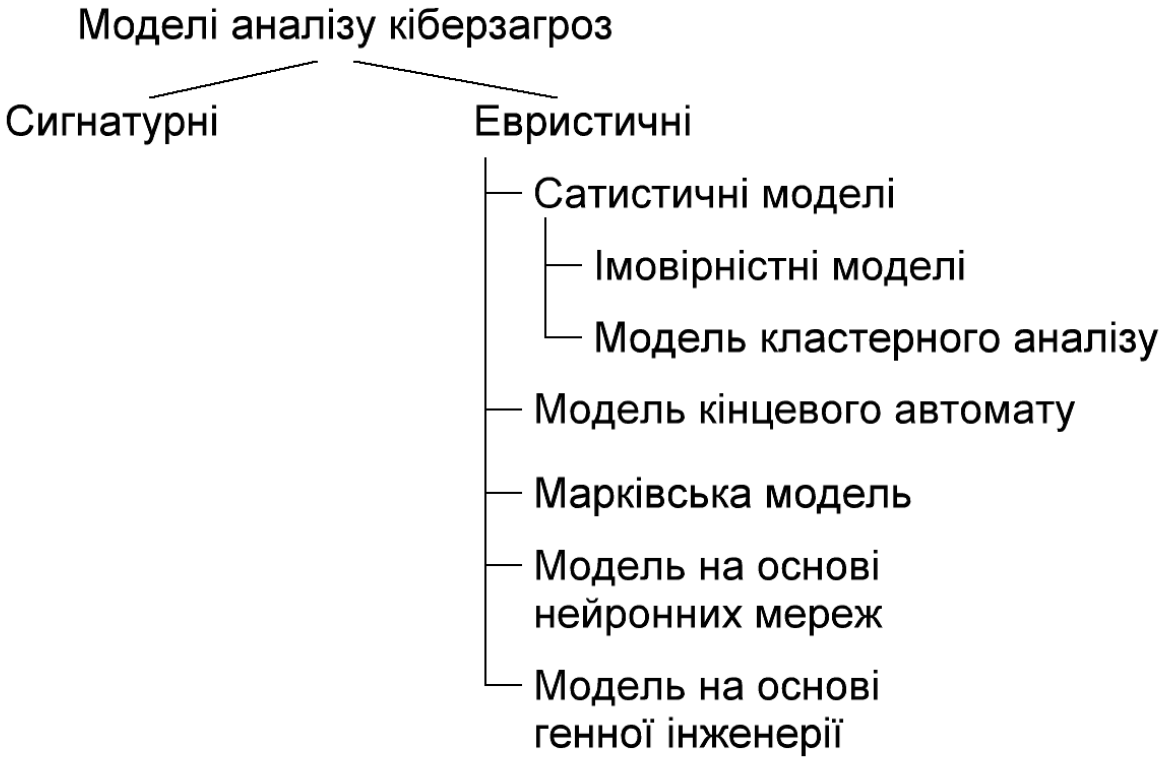


Рис. 2.1. Класифікація моделей аналізу кіберзагроз

2.1.1. Статистична модель

У методі виявлення аномальних відхилень, в якому використовуються статистичні моделі, виявлення аномальної активності здійснюється за допомогою порівняння поточної активності мережевого трафіку ІС з заданими вимогами до технологічного шаблону (профілем нормального поведінки).

Складність прийняття рішення за відсутності математичних моделей призводить до того, що при оцінці і виборі альтернативи необхідно використання і обробка якісної експертної інформації. Перспективний напрямок в даному випадку застосування математичної статистики та теорії ймовірності на основі експериментальних даних, які мають строго певну точність і достовірність [66, 67].

В якості основного показника в імовірнісних моделях виявлення комп'ютерних кіберзагроз використовується:

– ймовірність появи нової форми пакета передачі даних відмінною від еталонної;

– математичне очікування і дисперсія випадкових величин, що характеризують зміну джерела і споживача інформації.

Статистичні методи дають хороші результати на малому підмножині комп'ютерних кіберзагроз зі всієї безлічі можливих кіберзагроз. Недолік статистичних моделей виявлення аномальних відхилень полягає в тому, що вони не дозволяють оцінити обсяг переданих даних і не здатні виявити вторгнення кіберзагроз з перекрученими даними. Вузьким місцем методів є можливість переповнення буфера порогових перевірок «спамом» помилкових повідомлень.

Для ефективного використання статистичних моделей в методі виявлення аномальних відхилень необхідні строго задані вирішальні правила і перевірка ключових слів (порогів спрацьовування) на різних рівнях протоколів передачі даних. В іншому випадку частка помилкових спрацьовувань, за деякими оцінками, становить близько 40% від загального числа виявлених кіберзагроз.

2.1.2. Кластерний аналіз

В основі моделей кластерного аналізу лежить побудова профілю нормальних активностей (наприклад, кластера нормального трафіку) і оцінка відхилень від цього профілю за допомогою обраних критеріїв, ознак

(класифікатора головних компонентів) кіберзагроз і обчисленні відстаней між кластерами на безлічі ознак кіберзагроз. У моделях кластерного аналізу використовується двоетапний алгоритм виявлення кіберзагроз. На першому етапі здійснюється збір інформації для формування безлічі даних кластерів аномального поведінки ІС на нижчих рівнях протоколів передачі даних. На другому етапі виконується порівняльний аналіз отриманих кластерів аномального поведінки ІС з кластерами опису штатного поведінки системи. Імовірність розпізнавання кіберзагроз моделями кластерного аналізу становить в середньому 0,9 при виявленні вторгнень тільки по заголовкам пакетів передачі даних без семантичного аналізу інформаційної складової пакетів. Для отримання достовірних даних з використанням моделей кластерного аналізу необхідний аналіз порядку ідентифікації і аутентифікаціі, реєстрації абонентів, системних переривань, доступу до обчислювальних ресурсів в декількох системних журналах ІС: аудиту, реєстрації, ресурсів, що призводить до затримки часу на прийняття рішень. Така затримка часто унеможливлює застосування моделей кластерного аналізу в системах квазіреалістичного масштабу часу [68, 69, 70].

2.1.3. Модель кінцевих автоматів

Виявлення кіберзагроз з використанням моделі кінцевих автоматів засноване на моделюванні кінцевими автоматами процесів інформаційної взаємодії абонентів ІС по протоколам передачі даних. Кінцевий автомат описується множинами вхідних даних, вихідних даних і внутрішніх станів. Кіберзагрози фіксуються по «аномальним» переходам ІС зі стану в стан. Передбачається, що в ІС «штатні» переходи системи зі стану в стан визначено, а невідомі стану і переходи в ці стану реєструються як аномальні. Перевагою цієї моделі є спрощений підбір класифікаційних ознак для ІС та розгляд малого числа переходів зі стану в стан. Модель дозволяє виявляти кіберзагрози в потоці обробки даних мережевими протоколами в режимі близькому до реального масштабу часу. До недоліків моделі слід віднести

необхідність розробки великого числа складних експертних правил для порівняльного аналізу необхідних і аномальних станів і переходів системи. Експертні правила оцінки станів ІС взаємопов'язані з характеристиками мережевих протоколів передачі даних [71, 72].

2.1.4. Марківська модель

Методи виявлення аномальних відхилень на основі марковських моделей засновані на формуванні марковської ланцюга нормально функціонуючої системи і функції розподілу ймовірностей переходу з одного стану в інше. Ці відомості використовуються як навчальні дані. Виявлення аномалій здійснюється за допомогою порівняння марковских ланцюгів і відповідних функцій розподілу ймовірностей аномального і нормального функціонування ІС за значеннями порога ймовірностей настання подій. На практиці ця модель найбільш ефективна для виявлення комп'ютерних кіберзагроз, заснованих на системних викликах операційної системи, і вимагає додаткових метрик умовної ентропії для використання в системах квазіреальність масштабу часу [73, 74].

Так, марківська модель загрози безпеки системи захисту інформації представлена у вигляді процесів з дискретним станом і безперервним часовим проміжком для орграфа загрози інформаційній безпеці. Створюється за допомогою загрози двох атак:

– в першій використовуються загрози першої і другої уразливості;
– в другій використовуються загрози першої і третьої уразливості.

Тут система з відмовами і відновленнями характеристики безпеки, граф системи станів випадкових процесів представлений на рисунку 2.2.

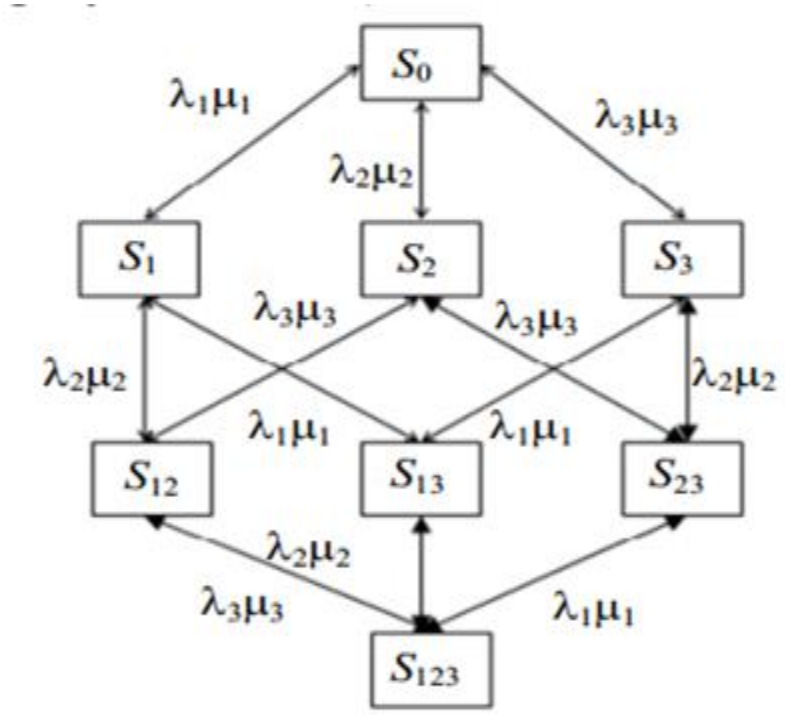


Рис. 2.2. Марківська модель загрози інформаційної безпеки, де S_0 – початковий стан системи, S_1 – в системі виявлена і не усунена одна із загроз, S_2 – в системі виявлені і не усунені дві загрози, S_3 – в системі виявлені і не усунені всі три загрози

На підставі даного графа відбувається моделювання залежності загроз за ступенем їх вразливості. Завдяки використанню даної моделі, будується система диференціальних рівнянь Колмогорова для ймовірностей станів. При вирішенні якої, розраховується ймовірність того, наскільки готова інформаційна система до безпечної експлуатації. Тут обґрунтовується коректність використання марківських процесів моделювання характеристик безпеки інформації, виявляються відмінності в постановці і вирішенні задач моделювання комплексної системи захисту інформаційної системи

2.1.5. Метод «теорії ігор»

Крім марківської моделі оптимізації комплексної системи захисту інформації важлива роль відводиться і методологічного апарату теорії ігор, яка передбачає наявність покупця і продавця, взаємозв'язок між якими визначена у вигляді платіжної матриці (табл. 2.1) [73, 74].

Таблиця 2.1.

Загальний вигляд платіжної матриці статистичної гри

	S_1	S_2	…	S_j
A_1	w_{11}	w_{12}	…	w_{1j}
A_2	w_{21}	w_{22}	…	w_{2j}
…	…	…	…	…
A_i	w_{i1}	w_{i2}	…	w_{ij}

В даному випадку рядок матриці буде виглядати так: A_1, A_2 ..., A_i - це стратегія особи приймаючої рішення, а стовпці матриць S_1, S_2, ..., S_j - відображають стан навколишнього середовища, w_{ij} =i =j - очікувана нагорода при використанні тієї чи іншої стратегії А в разі знаходження середовища в стані S_j.

Для того, щоб прийняти вірне рішення, в основному управління здійснюють на підставі критерію Вальда і критерію Гурвіца. Завдяки критерію Вальда здійснюється вибір так званої, обережною стратегії в сторону песимістичного плану. Тобто, для кожного прийнятого рішення вибирають найгіршу ситуацію з пошуком гарантованого максимального ефекту.

На підставі цього обраний варіант повністю виключає ризик небажаного варіанту подій.

Коли застосовується критерій Вальда, то рішення здійснюється за наступним сценарієм:

– виявляються можливості зовнішнього прояву нічого невідомого природного стану S_j;

– проводиться облік прояви того чи іншого зовнішнього стану S_j;

– рішення використовується одноразово з виключенням будь-якого було ризику.

2.1.6. Метод використанням нейронних мереж

Методи виявлення кіберзагроз на основі нейронних мереж застосовують для попередньої класифікації аномалій в ІС. Вони базуються на ідентифікації

нормального поведінки системи за функцією розподілу отримання пакетів даних (виконання заданих команд оператора), навчанні нейронної мережі і порівняльного аналізу подій за навчальною вибіркою [75, 76].

Аномальне відхилення в ІС виявляється тоді, коли ступінь довіри нейромережі своїм рішенням лежить нижче заданого порогу. Передбачається, що застосування моделі нейронних мереж для реалізації механізмів захисту інформації ІС від кіберзагроз передує навчання цих мереж заданим алгоритмам нормального функціонування. Недоліками методів виявлення кіберзагроз з використанням нейронної мережі є складний математичний апарат, який недостатньо ефективно працює в системах квазіреального масштабу часу, і складність навчання мережі для виявлення невідомих кіберзагроз.

Щоб використовувати нейро-нечітку мережу для оцінки ризиків інформаційної безпеки, необхідно визначити, які дані слід подавати на вхід системи. З визначення ризику інформаційної безпеки слід, що величина ризику R є функція від потенційно можливого збитку (вартості інформації, ресурсу або активу) A, загрози інформаційній безпеці T і уразливості інформаційної системи [77, 78].

Таким чином, вхідними факторами будуть служити експертні оцінки трьох нечітких змінних («загроза», «збиток», «вразливість»), описаних лінгвістичними терм-множини {дуже низький, низький, середній, високий, дуже високий} (табл. 2.2).

Крім експертних оцінок, додатково слід використовувати і дані системи виявлення вторгнень, антивірусів, міжмережевих екранів про потенційно небезпечної активності, загальний рівень мережевої активності і навантаження на ту чи іншу ділянку автоматизованої системи.

Таблиця 2.2.

Стани загроз

Рівні шкали	Загрози	Збиток	Уразливість
1	2	3	4
Дуже низький	Подія практично ніколи не відбувається	Незначні втрати матеріальних засобів та ресурсів, які швидко заповнюються, або незначний вплив на репутацію	Уразливість, якою можна знехтувати
Низький	Подія відбувається рідко	Більш помітні втрати матеріальних активів, більш істотний вплив на репутацію або ущемлення інтересів	Незначна уразливість, що яку легко усунути
Середній	Подія можлива тільки при певному збігові обставин	Достатні втрати матеріальних активів або ресурсів або достатній шкоди репутації та інтересам	Помірна вразливість

Продовження табл. 2.2.

1	2	3	4
Високий	Велика ймовірність, що подія настане при організації атаки	Значної шкоди репутації та інтересам, що може становити загрозу для продовження діяльності	Серйозна вразливість, ліквідація якої можлива, але пов'язана зі значними витратами
Дуже високий	Подія вірогідніше настане під час атаки	Руйнівні наслідки і неможливість ведення діяльності	Критична вразливість, яка ставить під сумнів можливість її усунення

В результаті на виході системи буде отримана оцінка рівня ризику інформаційної безпеки, яку можна описати розширеним лінгвістичним терм-множиною, приміром:{Нехтує низький, дуже низький, низький, нижче середнього, помірний, вище середнього, високий, дуже високий, критичний}.

В цьому випадку шкала вимірювання рівень інформаційних ризиків буде виглядати наступним чином:

– можна знехтувати низький - ризиком можна знехтувати;

– дуже низький - необхідно визначити, чи існує необхідність у коригувальних діях, або є можливість прийняти цей ризик;

– низький - рівень ризику дозволяє працювати, але є передумови до порушення нормальної роботи,

– нижче середнього - необхідно розробити і застосувати план корегуючих дій протягом прийнятного періоду часу;

– помірний - рівень ризику не дозволяє стабільно працювати, є нагальна необхідність у коригувальних діях, що змінюють режим роботи в сторону зменшення ризику;

– вище середнього - система може продовжувати роботу, але коригувальний план дій необхідно застосувати якомога швидше;

– високий - рівень ризику такий, що бізнес-процеси знаходяться в нестійкому стані;

– дуже високий - необхідно негайно вжити заходів щодо зменшення ризику;

– критичний - рівень ризику дуже великий і є неприпустимим для організації, що вимагає припинення експлуатації системи і прийняття радикальних заходів щодо зменшення ризику.

Розглянемо приклад застосування нейро-нечіткої мережі для оцінки інформаційних ризиків в автоматизованій системі. Для наочності на рис. вказані три вхідні змінні (загрози, збитки, уразливості). Виходом є ризик інформаційної безпеки [79].

Блок, позначений на схемі як NNclass (шар L1) (рис. 2.3), призначений для вирішення завдання кластеризації, тобто завдання функцій належності вхідних даних п'яти нечітким класами [79].

Застосування нейронних мереж для оцінки кіберзагроз дозволяє вирішити проблему явної неповноти інформації про складові ризику і їх неоднозначних властивостей. При застосуванні нейронних мереж відсутня необхідність створення детальної моделі автоматизованої системи для здійснення аналізу інформаційних ризиків. Система дозволяє агрегувати дані з різних джерел і добре пристосована для ітераційного безперервного аналізу ризиків інформаційної безпеки [79].

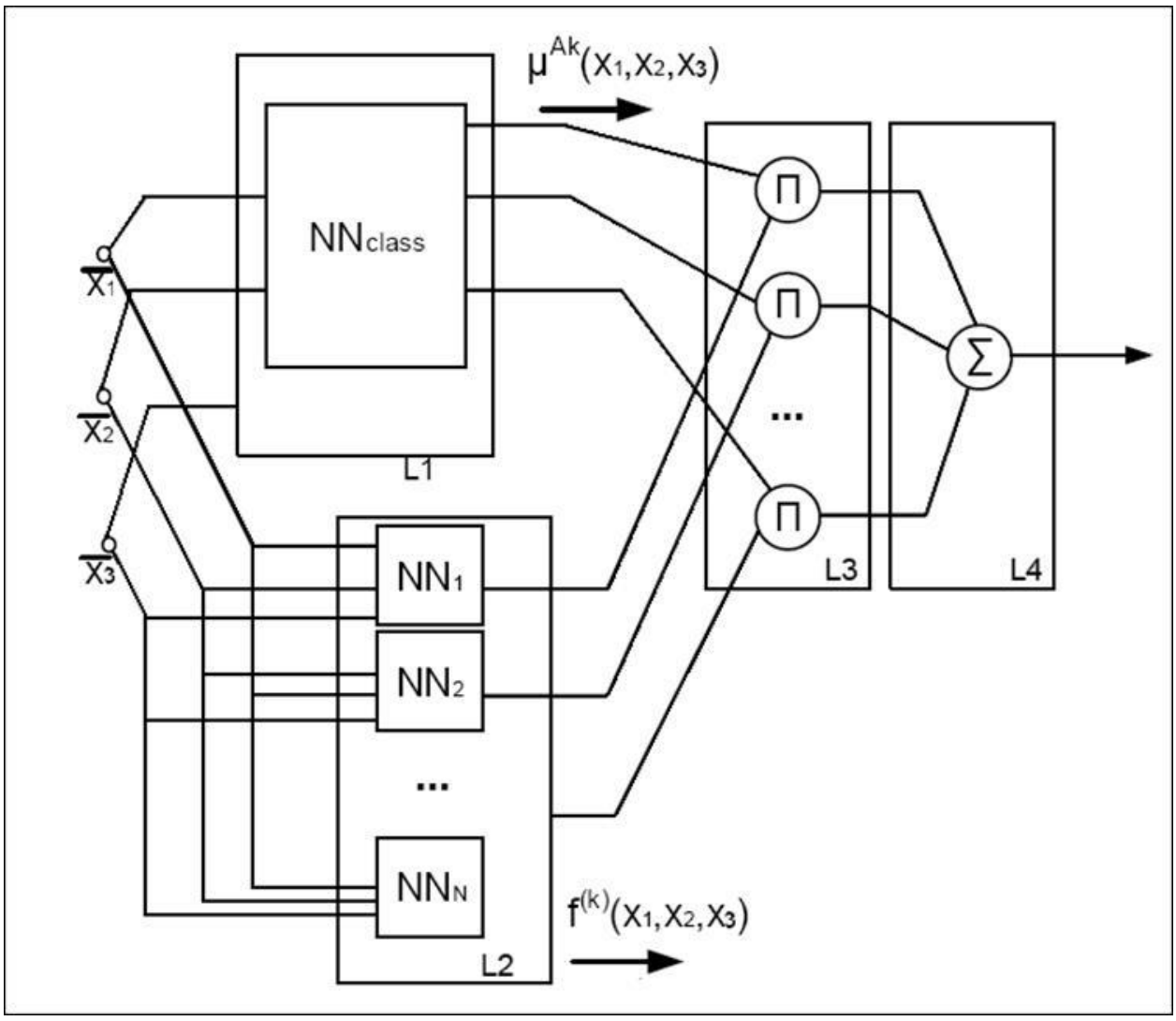


Рис. 2.3. Нейро-нечітка мережа для оцінки інформаційних ризиків в АС

2.1.7. Переваги та недоліки евристичних методів

Таким чином, перевагою методів виявлення аномальних відхилень є можливість аналізу динамічних процесів функціонування ІС і виявлення в них нових типів кіберзагроз. Методи дають можливість апріорного розпізнавання аномалій шляхом систематичного сканування вразливих місць.

До недоліків цих методів можна віднести необхідність збільшення навантаження на трафік в мережі, складність реалізації і більш низька вірогідність виявлення комп'ютерних кіберзагроз в порівнянні з сигнатурним аналізом.

Обмеженням методів виявлення та аналізу кіберзагроз є необхідність детальної інформації про застосування протоколів (стеків протоколів)

передачі даних в ІС на всіх рівнях еталонної моделі взаємодії відкритих систем.

2.2. Машинне навчання

Машинне навчання являє собою підрозділ штучного інтелекту, що стоїть на стику таких дисциплін, як математика, статистика, теорія ймовірностей, теорія графів і вивчає алгоритми, які здатні самостійно навчатися на основі досвіду (рис. 2.4) [9, 14, 15, 16].

Рис. 2.4. Класифікація методів машинного навчання

При навчанні з учителем для кожного прецеденту задана пара «ситуація, рішення». Завдання такого навчання полягає в пошуку залежно прийнятого рішення від заданої ситуації і побудові алгоритму, здатного прийняти на вхід опис ситуації, а на виході передбачити для неї рішення [14].

При навчанні без учителя на вхід подаються тільки описи об'єктів без прийнятого рішення по цій ситуації, а завдання полягає в пошуку залежностей між представленими об'єктами [14].

Часткове навчання є проміжною ланкою між навчанням з учителем і без учителя, так як кожен прецедент задається парою «ситуація, рішення», однак відповіді відомі лише для частини цих ситуацій [14].

Існують різні алгоритми машинного навчання, на основі яких будується модель системи. Багато в чому вибір відповідного алгоритму залежить від характеристик набору даних, таких як обсяг, структура і якість. Також на вибір алгоритму впливає бажаний результат (двокласова або багатокласова класифікація, регресія або фільтрація викидів), необхідна точність передбачення і час, необхідний для навчання моделі [14].

При навчанні з підкріпленням не існує «правильних відповідей» для кожної ситуації, алгоритм шукає оптимальну стратегію поведінки, спираючись на реакцію зовнішнього середовища [14].

2.2.1. Регресійна модель

Як правило, для передбачення значень змінної використовується регресійний аналіз. Його мета - розробити статистичну модель, що дозволяє прогнозувати значення залежної змінної, або відгуку, за значеннями, принаймні однієї, незалежної, або пояснює, змінної [14].

Для ілюстрації залежності між змінними X і Y використовувалася діаграма розкиду. На ній значення змінної X відкладалися по горизонтальній осі, а значення змінної Y - по вертикальній. Залежність між двома змінними може бути різною: від найпростішої до вкрай складної.

Труднощі, пов'язані з регресійним аналізом [38 ,39,40, 41, 42, 43]:

– Ігнорування умов застосовності методу найменших квадратів.

– Помилкова оцінка умов застосовності методу найменших квадратів.

– Неправильний вибір альтернативних методів при порушенні умов застосовності методу найменших квадратів.

– Застосування регресійного аналізу без глибоких знань про предмет дослідження.

– Плутанина між статистичної та причинно-наслідкового залежностями.

2.2.1. Критерій згоди «χ^2-квадрат Пірсона»

Розподіл χ^3 використовується для перевірки узгодженості набору даних з фіксованим розподілом ймовірностей. У критерії згоди частоти, що належать певній категорії, порівнюються з частотами, які є теоретично очікуваними, якби дані дійсно мали зазначений розподіл [44, 45, 46, 47, 48, 49].

Перевірка за допомогою критерію згоди χ^3 виконується в кілька етапів. По-перше, визначається конкретний розподіл ймовірностей, яке порівнюється з вихідними даними. По-друге, висувається гіпотеза про параметри обраного розподілу ймовірностей (наприклад, про її математичне сподівання) або проводиться їх оцінка. По-третє, на основі теоретичного розподілу визначається теоретична ймовірність, відповідна кожної категорії. На закінчення, для перевірки узгодженості даних і розподілу застосовується тестова χ^3 – статистика (2.1) [44, 45, 46, 47, 48, 49]:

$$\chi^3_{k-p-1} = \sum_k \frac{(f_0 - f_e)^3}{f_e} \quad (2.1)$$

де f_0 - спостережувана частота, f_e - теоретична, або очікувана частота, k - кількість категорій, що залишилися після об'єднання, p - кількість оцінюваних параметрів.

Критерій χ^3 для перевірки гіпотези від дисперсії або стандартного відхилення вважається класичною параметричної процедурою. При перевірці гіпотези про дисперсії генеральної сукупності або стандартного відхилення передбачається, що вихідні дані мають нормальний розподіл. Нажаль, χ^3 - критерій досить чутливий до порушення цих припущень (тобто цей критерій не є стійким). Отже, якщо генеральна сукупність не має нормального розподілу, особливо, коли обсяг вибірки невеликий, точність критерію може значно знизитися [44, 45, 46, 47, 48, 49].

2.2.3. Класифікація на основі Байєсівського підходу

Байєсівський підхід до класифікації заснований на теоремі, яка стверджує, що якщо щільності розподілу кожного з класів відомі, то шуканий алгоритм можна виписати в явному аналітичному вигляді. Більш того, цей алгоритм оптимальний, тобто володіє мінімальною ймовірністю помилок [44, 45, 46, 47, 48, 49].

На практиці щільності розподілу класів, як правило, не відомі. Їх доводиться оцінювати (відновлювати) за навчальною вибіркою. В результаті

байесовский алгоритм перестає бути оптимальним, так як відновити щільність по вибірці можна тільки з деякою погрішністю. Чим коротше вибірка, тим вище шанси підігнати розподіл під конкретні дані і зіткнутися з ефектом перенавчання [44, 45, 46, 47, 48, 49].

Байєсівський підхід до класифікації є одним з найстаріших, але до сих пір зберігає міцні позиції в теорії розпізнавання. Він лежить в основі багатьох досить вдалих алгоритмів класифікації [44, 45, 46, 47, 48, 49].

До числа байесовских методів класифікації відносяться:

– Наївний байесовский класифікатор;
– Лінійний дискриминант Фішера;
– Квадратичний дискримінант;
– Метод парзеновского вікна;
– Метод радіальних базисних функцій (RBF);
– Логістична регресія;

Наївний байесівський класифікатор (naïve Bayes) - спеціальний окремий випадок байєсівського класифікатора , заснований на додатковому припущенні, що об'єкти $x \in X$ описуються n статистично незалежними ознаками (2.2) [50, 51, 52, 53, 54, 55]:

$$x \equiv (\xi_1, \dots, \xi_n) \equiv \left(\mathrm{f}_1(x), \dots, \mathrm{f}_n(x)\right) \tag{2.2}$$

Припущення про незалежність означає, що функції правдоподібності класів представимо у вигляді (2.3) [50, 51, 52, 53, 54, 55]:

$$\mathrm{p_y}(x) = \mathrm{p_{y1}}(\xi_1) \cdot \dots \cdot \mathrm{p_{yn}}(\xi_n) \tag{2.3}$$

де $\mathrm{p_{yj}}(\xi_j)$- щільність розподілу значень j-го ознаки для класу

Припущення про незалежність істотно спрощує завдання, тому що оцінити одновимірних щільності набагато легше, ніж одномірну щільність. На жаль, воно вкрай рідко виконується на практиці, звідси і назва методу [50, 51, 52, 53, 54, 55].

Наївний байесівський класифікатор може бути як параметричних, так і непараметричним, в залежності від того, яким методом відновлюються одномірні щільності [50, 51, 52, 53, 54, 55].

Основні переваги наївного байєсівського класифікатора - простота реалізації і низькі обчислювальні витрати при навчанні та класифікації. У тих рідкісних випадках, коли ознаки дійсно незалежні (або майже незалежні), наївний байесівський класифікатор (майже) оптимальний [50, 51, 52, 53, 54, 55].

Основний його недолік - відносно низька якість класифікації в більшості реальних задач [50, 51, 52, 53, 54, 55].

Найчастіше він використовується або як примітивний еталон для порівняння різних моделей алгоритмів, або як елементарний будівельний блок в алгоритмічних композиціях [50, 51, 52, 53, 54, 55].

2.3. Поняття та класифікація алгоритмів кластеризації машинного навчання

Кластеризація (або кластерний аналіз) - це задача розбиття множини об'єктів на групи, які називаються кластерами. Усередині кожної групи повинні виявитися «схожі» об'єкти, а об'єкти різних групи повинні бути якомога більш відмінні. Головна відмінність кластеризації від класифікації полягає в тому, що перелік груп чітко не заданий і визначається в процесі роботи алгоритму [56, 57, 58, 59, 60, 61].

Застосування кластерного аналізу в загальному вигляді зводиться до наступних етапів [56, 57, 58, 59, 60, 61]:

1. Відбір вибірки об'єктів для кластеризації.
2. Визначення безлічі змінних, за якими будуть оцінюватися об'єкти у вибірці. При необхідності - нормалізація значень змінних.
3. Обчислення значень міри схожості між об'єктами.
4. Застосування методу кластерного аналізу для створення груп схожих об'єктів (кластерів).

5. Представлення результатів аналізу.

Після отримання та аналізу результатів можливе корегування обраної метрики і методу кластеризації до отримання оптимального результату [56, 57, 58, 59, 60, 61].

Міри відстаней.

Отже, як же визначати «схожість» об'єктів? Для початку потрібно скласти вектор характеристик для кожного об'єкта - як правило, це набір числових значень, наприклад, зростання-вага людини. Однак існують також алгоритми, що працюють з якісними характеристиками [56, 57, 58, 59, 60, 61].

Після того, як ми визначили вектор характеристик, можна провести нормалізацію, щоб всі компоненти давали однаковий вклад при розрахунку «відстані». У процесі нормалізації все значення приводяться до деякого діапазону, наприклад, [-1, 1] або [0, 1] [56, 57, 58, 59, 60, 61].

Нарешті , для кожного пари об'єктів вимірюється «відстань» між ними - ступінь схожості. Існує безліч метрик, ось лише основні з них [56, 57, 58, 59, 60, 61]:

1. Евклідова відстань

Найбільш поширена функція відстані. Являє собою геометричних відстанню в багатовимірному просторі (2.4):

$$\rho(x, x') = \sqrt{\sum_{i}^{n} (x_i - x'_i)^3} \tag{2.4}$$

2. Квадрат евклідової відстані

Застосовується для додання більшої ваги більш віддаленим один від одного об'єктів. Це відстань обчислюється таким чином (2.5):

$$\rho(x, x') = \sum_{i}^{n} (x_i - x'_i)^3 \tag{2.5}$$

3. Відстань міських кварталів (Манхеттенська відстань)

Це відстань є середнім різниць по координатах. У більшості випадків ця міра відстані приводить до таких же результатів, як і для звичайного відстані

Евкліда. Однак для цього заходу вплив окремих великих різниць (викидів) зменшується (тому що вони не зводяться в квадрат). Формула для розрахунку манхеттенської відстані (2.6) [56, 57, 58, 59, 60, 61]:

$$\rho(x, x') = \sum_{i}^{n} |x_i - x'_i| \tag{2.6}$$

4. Відстань Чебишева

Це відстань може виявитися корисним, коли потрібно визначити два об'єкта як «різні», якщо вони розрізняються за якоюсь однією координаті. Відстань Чебишева обчислюється за формулою (2.7) [56, 57, 58, 59, 60, 61]:

$$\rho(x, x') = \max(|x_i - x'_i|) \tag{2.7}$$

5. Степенева відстань

Застосовується в разі, коли необхідно збільшити або зменшити вагу (2.8), що відноситься до розмірності, для якої відповідні об'єкти сильно відрізняються. Степенева відстань обчислюється за наступною формулою [56, 57, 58, 59, 60, 61]:

$$\rho(x, x') = \sqrt[r]{\sum_{i}^{n} (x_i - x'_i)^p} \tag{2.8}$$

де r і p - параметри, що визначаються користувачем. Параметр p відповідальний за поступове зважування різниць за окремими координатами, параметр r відповідальний за прогресивне зважування великих відстаней між об'єктами. Якщо обидва параметри - r і p - дорівнюють двом, то це відстань збігається з відстанню Евкліда.

Вибір метрики повністю лежить на дослідника, оскільки результати кластеризації можуть істотно відрізнятися при використанні різних заходів [56, 57, 58, 59, 60, 61].

Існують дві основні класифікації алгоритмів кластеризації.

1. Ієрархічні і плоскі.

Ієрархічні алгоритми (також звані алгоритмами таксономії) будують не одне розбиття вибірки на непересічні кластери, а систему вкладених розбиття. Тобто на виході ми отримуємо дерево кластерів, коренем якого є вся вибірка, а листям - найбільш дрібні кластера. Плоскі алгоритми будують одне розбиття об'єктів на кластери [56, 57, 58, 59, 60, 61].

2. Чіткі і нечіткі.

Чіткі (або непересічні) алгоритми кожному об'єкту вибірки ставлять у відповідність номер кластера, тобто кожен об'єкт належить тільки одного кластеру. Нечіткі (або пересічні) алгоритми кожному об'єкту ставлять у відповідність набір речових значень, що показують ступінь відносини об'єкта до кластерів. Тобто кожен об'єкт відноситься до кожного кластеру з певною ймовірністю [56, 57, 58, 59, 60, 61].

3. Об'єднання кластерів

У разі використання ієрархічних алгоритмів постає питання, як об'єднувати між собою кластера, як обчислювати «відстані» між ними [56, 57, 58, 59, 60, 61].

Існує кілька метрик:

1. Одиночна зв'язок (відстані найближчого сусіда).

У цьому методі відстань між двома кластерами визначається відстань між двома найбільш близькими об'єктами (найближчими сусідами) в різних кластерах. Результуючі кластери мають тенденцію об'єднуватися в ланцюжки [56, 57, 58, 59, 60, 61].

2. Повна зв'язок (відстань найбільш віддалених сусідів).

У цьому методі відстані між кластерами визначаються найбільшою відстанню між будь-якими двома об'єктами в різних кластерах (тобто найбільш віддаленими сусідами). Цей метод зазвичай працює дуже добре, коли об'єкти походять з окремих груп. Якщо ж кластери мають подовжену форму або їх природний тип є «ланцюжковий», то цей метод непридатний [56,

57, 58, 59, 60, 61].

3. Незважене попарне середнє.

У цьому методі відстань між двома різними кластерами обчислюється що середня відстань між усіма парами об'єктів в них. Метод ефективний, коли об'єкти формують різні групи, проте він працює однаково добре і в випадках протяжних («ланцюжкового» типу) кластерів [56, 57, 58, 59, 60, 61].

4. Виважена попарне середнє.

Метод ідентичний методу невиваженого попарного середнього, за винятком того, що при обчисленнях розмір відповідних кластерів (тобто число об'єктів, що містяться в них) використовується в якості вагового коефіцієнта. Тому даний метод має бути використаний, коли передбачаються нерівні розміри кластерів[56, 57, 58, 59, 60, 61].

5. Метод незважений центроїда

У цьому методі відстань між двома кластерами визначається як відстань між їх центрами тяжкості.

6. Метод зваженого центроїда (медіана)

Цей метод ідентичний попередньому, крім того, що при обчисленнях використовуються ваги для обліку різниці між розмірами кластерів. Тому, якщо є або підозрюються значні відмінності в розмірах кластерів, цей метод виявляється переважно попереднього [56, 57, 58, 59, 60, 61].

Ієрархічні алгоритми, що використовують поняття порога

Альтернативою кластерним методам є ієрархічні алгоритми, що використовують поняття порога. Порогові алгоритми ефективні для вихідних сукупностей, у яких слабо виражений ланцюговий ефект і вони природно розпадаються на якусь кількість досить віддалених скупчень точок (кластерів).

Найбільш популярними серед таких алгоритмів є алгоритми типу FOREL ("формальний елемент"). FOREL є прикладом евристичного алгоритму класифікації, заснованого на ідеї об'єднання в один кластер об'єктів в областях їх найбільшого згущення. Таксони, одержувані цим алгоритмом,

мають сферичну форму. Кількість таксонів залежить від радіуса сфер: чим менше радіус, тим більше виходить таксонів [56, 57, 58, 59, 60, 61].

2.3.1. Нейронні мережі Кохонена

Нейронні мережі Кохонена - типовий приклад нейромережевої архітектури, яка навчається без вчителя. Звідси і перелік вирішуваних ними завдань: кластеризація даних або прогнозування властивостей. Крім того, мережі Кохонена можуть використовуватися з метою зменшення розмірності даних з мінімальною втратою інформації [56, 57, 58, 59, 60, 61].

Раніше розглянуті архітектури нейронних мереж навчалися з учителем на вибірках даних, що включають безліч прикладів, що складаються з відповідних один одному пар вхідних і вихідних векторів. При цьому вихідні значення брали безпосередню участь в налаштуванні вагових коефіцієнтів. У нейронних мережах Кохонена вихідні вектора в навчальній вибірці можуть бути, але можуть бути і відсутніми, і, в будь-якому випадку, вони не беруть участі в процесі навчання. Тобто виходи не використовуються в якості орієнтирів при корекції синапсів. Саме тому даний принцип настройки нейронної мережі називається самонавчанням [56, 57, 58, 59, 60, 61].

У розглянутій архітектурі сигнал поширюється від входів до виходів в прямому напрямку. Структура нейронної мережі містить єдиний шар нейронів (шар Кохонена) без коефіцієнтів зміщення (мал. 1). Загальна кількість вагових коефіцієнтів розраховується як добуток (2.9) [56, 57, 58, 59, 60, 61]:

$$N_w = MK \tag{2.9}$$

Кількість нейронів дорівнює кількості кластерів, серед яких відбувається початкове розподіл і подальше перерозподіл навчальних прикладів. Кількість вхідних змінних нейронної мережі дорівнює числу ознак, що характеризують об'єкт дослідження і на основі яких відбувається віднесення його до одного з кластерів [56, 57, 58, 59, 60, 61].

Слід розрізняти власне самонавчання і самоорганізацію нейронної мережі Кохонена. При звичайному самонавчанні мережа має строго фіксовану

структуру, тобто кількість нейронів, що не змінюються протягом усього життєвого циклу. При самоорганізованій мережі, навпаки, не має постійної структури. Залежно від знайденого відстані до нейрона-переможця, або цей нейрон використовується для кластеризації прикладу, або для поданого на входи прикладу створюється новий кластер з відповідними йому ваговими коефіцієнтами. Крім того, в процесі самоорганізації структури мережі Кохонена окремі нейрони можуть виключатися з неї (рис. 2.5) [56, 57, 58, 59, 60, 61].

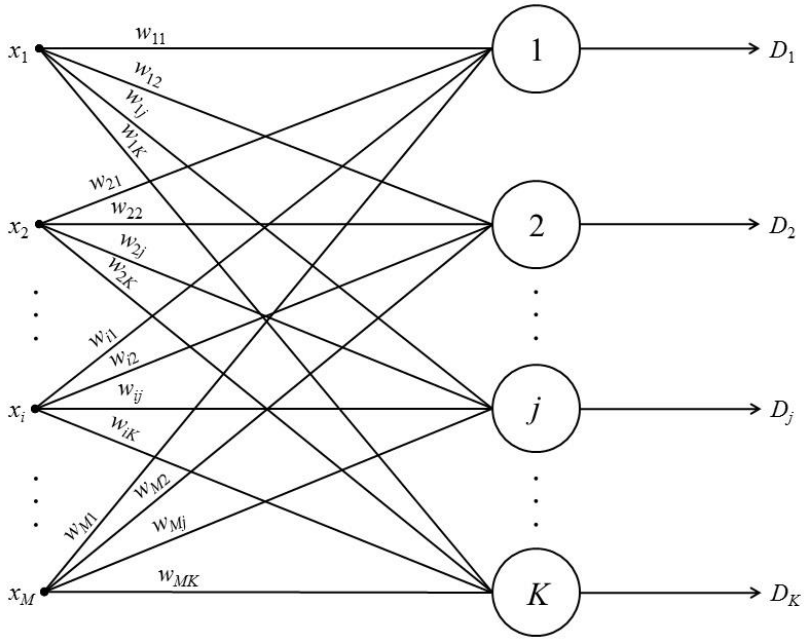


Рис. 2.5. Загальна структура нейронної мережі Кохонена

Нормалізація вхідних змінних виконується в межах [-1, 1] або [0, 1].

Для життєвого циклу нейронних мереж даної архітектури характерні три основні стадії життєвого циклу: навчання, кластерний аналіз та практичне використання [56, 57, 58, 59, 60, 61].

Алгоритм навчання мережі Кохонена включає етапи, склад яких залежить від типу структури: постійної (самонавчальна мережу) або змінною (самоорганізовану мережу). Для самонавчання послідовно виконуються:

1. Задання структури мережі (кількості нейронів шару Кохонена).

2. Випадкова ініціалізація вагових коефіцієнтів значеннями, що задовольняють одному з наступних обмежень:

– при нормалізації вихідної вибірки в межах (2.10) [-1, 1]:

$$\left|w_{ij}\right| = \frac{1}{\sqrt{M}} \tag{2.10}$$

– при нормалізації вихідної вибірки в межах (2.11) [0, 1]:

$$0.5 - \frac{1}{\sqrt{M}} \le w_{ij} \le 0.5 + \frac{1}{\sqrt{M}} \tag{2.11}$$

де M - кількість вхідних змінних мережі - характеристичних ознак об'єкта дослідження.

3. Подача на входи мережі випадкового навчального прикладу поточного навчання і розрахунок евклідових відстаней від вхідного вектора до центрів всіх кластерів (2.12):

$$R_j = \sqrt{\sum_{i=1}^{M} \left(\overline{x_i} - w_{ij}\right)^3} \tag{2.12}$$

4. За найменшому з значень R_j вибирається нейрон-переможець j, в найбільшою мірою близький за значеннями з вхідним вектором. Для обраного нейрона (і тільки для нього) виконується корекція вагових коефіцієнтів (2.13):

$$w_{ij}^{(q+1)} = w_{ij}^{(q)} + v\left(\overline{x}_i - w_{ij}^{(q)}\right) \tag{2.13}$$

де v - коефіцієнт швидкості навчання.

5. Цикл повторюється з кроку 3 до виконання одного або декількох умов закінчення:

– вичерпано заданий гранична кількість епох навчання;

– не відбулося значного зміни вагових коефіцієнтів в межах заданої точності протягом останньої доби навчання;

– вичерпано заданий граничний фізичний час навчання.

Коефіцієнт швидкості навчання може здаватися незмінним за межі [0, 1] або змінним значенням, поступово зменшується від циклу до циклу.

У разі самоорганізації мережі Кохонена алгоритм зазнає певних змін:

1. Здається критичну відстань $R_{кр}$, відповідне максимально допустимому евклидову відстані між входами прикладу і вагами нейрона-переможця. Початкова структура не містить нейронів. При подачі на входи

мережі самого першого прикладу навчальної вибірки створюється перший нейрон з ваговими коефіцієнтами, рівними поданням вхідним значенням [56, 57, 58, 59, 60, 61].

2. На входи мережі подається новий випадково обраний приклад поточної епохи навчання, розраховуються евклідові відстані від прикладу до центру кожного кластера по співвідношенню (2.14) і визначається нейрон-переможець з найменшим з них R_{min}.

3. Якщо виконується умова $R_{min} \leq R_{кр}$, проводиться корекція вагових коефіцієнтів відповідного нейрона-переможця по співвідношенню (4), в іншому випадку в структуру мережі додається новий нейрон, вагові коефіцієнти якого приймаються чисельно рівними вхідним значенням поданого прикладу.

4. Процедура повторюється з п.3. Якщо протягом останньої доби навчання будь-які кластери залишилися не задіяними, відповідні нейрони виключаються зі структури мережі Кохонена [56, 57, 58, 59, 60, 61].

5. Обчислення закінчуються, якщо виконується одна з умов, прописані в алгоритмі самонавчання мережі фіксованого структури [56, 57, 58, 59, 60, 61].

Ще одна модифікація алгоритмів самонавчання і самоорганізації передбачає корекцію вагових коефіцієнтів не тільки нейрона-переможці, а й усіх інших нейронів. Для цього слід використовувати коефіцієнт швидкості навчання, регресний зі збільшенням відстані до центру кластера.

Як значення $R_{кр}$ можна розраховувати середнє відстань для кожного кластера при поточному пред'явленні навчального прикладу. Параметр β рекомендується вибирати рівним $3{,}0 \pm 0{,}5$.

Як правило, практично під час використання самоорганізації нейронної мережі Кохонена доводиться стикатися ще з однією проблемою. З одного боку, якісь кластери можуть містити занадто маленька кількість прикладів, що призводить до складнощів у наступному узагальненні інформації. З іншого боку, деякі кластери можуть виявитися занадто великими, тобто містити дуже

багато прикладів. В цьому випадку для регулювання розміру кластера і вирішення проблеми його переповненості можна задати в якості додаткового параметра граничне число прикладів, які формують кластер $N_{пр}$. Якщо в якийсь момент виявляється, що новий приклад повинен бути віднесений до кластеру, розмір якого вже максимальний, приймається рішення про створення іншого кластера, центр якого буде представляти собою вектор змінних одного з $N_{пр+1}$ прикладів кластера (включаючи новий) найбільш віддаленого від центру даного кластера [56, 57, 58, 59, 60, 61].

До навченої нейронної мережі застосовується процедура кластерного аналізу - процедури опису властивостей кластера на основі аналізу кількісного і якісного складів прикладів, які сформували його. Слід враховувати, що опис кластерів може базуватися не тільки на значеннях вхідних змінних навчальної вибірки, а й на значеннях змінних, які не брали участі у формуванні кластерів. Зокрема, в опис можуть входити дані про середні значення таких змінних серед всіх прикладів, які сформували кластер. Крім того, доцільно для кожного кластера мати дані про середньоквадратичному відхиленні або дисперсії по кожній змінній [56, 57, 58, 59, 60, 61].

При практичному використанні нейронної мережі Кохонена новий приклад подається на її вхід і відноситься до одного з існуючих кластерів, або робиться висновок про неможливість такого віднесення (при великій відстані до центру найближчого кластера). Якщо вибір кластера відбувся, його опис, отримане в результаті кластерного аналізу, і відповідні кластеру рішення повинні поширюватися в тому числі на поданий приклад [56, 57, 58, 59, 60, 61].

Практичне використання мережі Кохонена полегшується за рахунок візуалізації результатів кластеризації. В результаті самонавчання (самоорганізації) мережі виходить набір кластерів, кожен з яких характеризується своїм центром (значеннями вагових коефіцієнтів відповідного нейрона) і кількістю навчальних прикладів, які сформували його. Чи не складає ніяких труднощів визначити евклідова відстань між центрами

всіх можливих пар кластерів і графічно зобразити їх на так званій карті Кохонена - двовимірної графічної структурі, що дозволяє судити не тільки про розміри і положення кожного окремо взятого кластера, а й про близькість один до одного і взаємне розташування окремих кластерів [56, 57, 58, 59, 60, 61].

2.3.2. Кластеризація методом k-means

Метод k-means - це спеціальний алгоритм кластеризації, що має на увазі, що у нас є масив даних, які ми хочемо згрупувати в кластери, а точніше – в k кластерів [56, 57, 58, 59, 60, 61].

Вхідними даними в методі k-means є тільки матриця наших X. Як правило, ми формуємо її так, щоб кожен рядок представляла окремий приклад (зразок), а кожен стовпець - окремий ознака або, користуючись термінами з статистики, фактор. Зазвичай ми говоримо, що є N прикладів і D ознак, так що X є матрицею розмірності NxD [56, 57, 58, 59, 60, 61].

В алгоритмі методу k-means є два основних етапи. Спочатку ми вибираємо k різних центрів кластерів - як правило, це просто випадкові точки в наборі даних. Потім ми переходимо до нашого основного циклу, який також складається з двох етапів. Перший - це вибір, до якого з кластерів належить кожна точка з X. Для цього ми беремо кожен приклад і вибираємо кластер, чий центр ближче всього. Не забувайте, що спочатку ми вибираємо центри випадковим чином. Другий етап - заново обчислити кожен центр кластера, ґрунтуючись на безлічі точок, які до нього приписані. Для цього беруться всі відповідні приклади і обчислюється їх середнє значення, звідси і назва методу - «метод k-means». Все це робиться до тих пір, поки алгоритм не зійде, тобто поки не припиниться зміна в розподілі точок по кластерам або в координатах центрів кластерів. Як правило, це відбувається дуже швидко - в районі від 5 до 14 проходів циклу. Це сильно відрізняється від градієнтного спуску в глибокому навчанні, де можуть пройти тисячі ітерацій, поки не відбудеться сходження [56, 57, 58, 59, 60, 61].

Розглянемо наочний приклад роботи методу k-середній (рис. 2.6). На першому етапі ми приписуємо центри кластерів m_1 і m_3 до випадкових точках X. На наступному етапі - що є першим етапом основного циклу - ми вибираємо, до якого з кластерів належить кожна точка. Так, на малюнку дві точки зліва належать до кластеру 1, а дві точки праворуч - до кластеру 3. На наступному етапі перераховуємо середні значення m_1 і m_3. Тоді m_1 виходить середнім значенням двох точок зліва, оскільки вони належать цьому кластеру. Все, алгоритм зійшовся, оскільки більше не може бути змін до присвоєння даних до кластерів і, отже, в значеннях m_1 і m_3 [56, 57, 58, 59, 60, 61].

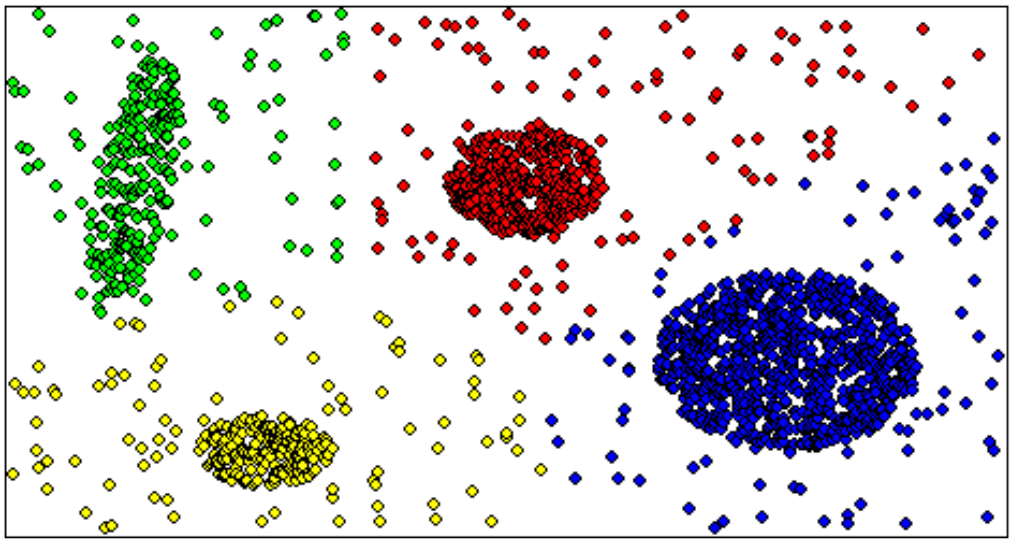


Рис. 2.6. Результат класифікації методами k-means

2.3.4. EM - масштабований алгоритм кластеризації

Кластеризація є однієї з найбільш важливих завдань Data Mining. В даний час розроблено велику кількість методів і алгоритмів кластеризації але, на жаль, не всі вони можуть ефективно працювати з великими масивами даних, тому подальші дослідження в цьому напрямку пов'язані з подоланням цієї проблеми. Одним з широко відомих в аналітичному співтоваристві алгоритмів кластеризації, що дозволяють ефективно працювати з великими обсягами даних, є EM-алгоритм. Його назва походить від слів "expectation-maximization", що перекладається як "очікування-максимізація". Це пов'язано з тим, що кожна ітерація містить два кроки - обчислення математичних очікувань (expectation) і максимізацію (maximisation) [62].

В основі ідеї ЕМ-алгоритму лежить припущення, що досліджуване безліч даних може бути змодельоване за допомогою лінійної комбінації багатовимірних нормальних розподілів, а метою є оцінка параметрів розподілу, які максимізують логарифмічну функцію правдоподібності, використовувану в якості запобіжного якості моделі. Іншими словами, передбачається, що дані в кожному кластері підкоряються певним законом розподілу, а саме, нормальному розподілу (рис. 2.7). З урахуванням цього припущення можна визначити параметри - математичне очікування і дисперсію, які відповідають закону розподілу елементів в кластері, найкращим чином "невластивому" до спостережуваних даними [62].

Таким чином, ми припускаємо, що будь-яке спостереження належить до всіх кластерів, але з різною ймовірністю. Тоді завдання полягатиме в "підгонці" розподілів суміші до даних, а потім у визначенні ймовірностей приналежності спостереження до кожного кластеру. Очевидно, що спостереження повинно бути віднесено до того кластеру, для якого ця можливість вище [62].

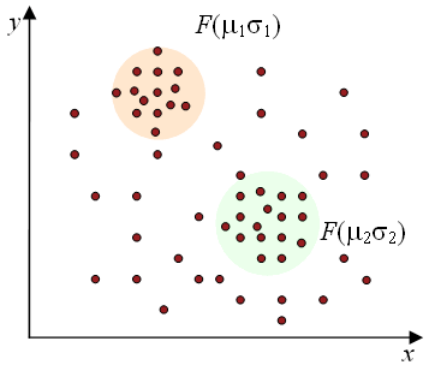


Рис. 2.7. Розподіл елементів в кластерах

Серед переваг ЕМ-алгоритму можна виділити наступні [62]:

– Потужна статистична основа.
– Лінійне збільшення складності при зростанні обсягу даних.
– Стійкість до шумів та перепустками в даних.
– Можливість побудови бажаного числа кластерів.
– Швидка збіжність при вдалій ініціалізації [62].

Однак алгоритм має і ряд недоліків. По-перше, припущення про нормальність всіх вимірювань даних не завжди виконується. По-друге, при невдалій ініціалізації збіжність алгоритму може виявитися досить повільним. Крім цього, алгоритм може зупинитися в локальному мінімумі і дати квазіоптимальне рішення [62].

Статистичні основи алгоритму

Як зазначалося вище, ЕМ-алгоритм передбачає, що кластеризуємі дані підкоряються лінійній комбінації (суміші) нормальних розподілів. Щільність ймовірності нормального розподілу має вигляд (2.14) [62]:

$$p(x) = \frac{1}{\sqrt{3\pi\sigma^3}} e^{-\frac{(x-\mu)^3}{3\sigma^3}} \quad (2.14)$$

де μ - математичне очікування, σ^3 − дисперсія.

Алгоритм передбачає, що дані підкоряються суміші багатовимірних нормальних розподілів для q змінних (2.45). Модель, що представляє собою суміш гаусових розподілів задається у вигляді (2.15) [62]:

$$p(x) = \sum_{i=1}^{k} w_i p(x|i) \quad (2.15)$$

де $p(x|i)$- нормальний розподіл для і-го кластера, w_i- частка (вага) іі-го кластера в вихідній базі даних.

Алгоритм ЕМ заснований на обчисленні відстаней. Він може розглядатися як узагальнення кластеризації на основі аналізу суміші імовірнісних розподілів. У процесі роботи алгоритму відбувається ітеративне поліпшення рішення, а зупинка здійснюється в момент, коли досягається необхідний рівень точності моделі. Мірою в даному випадку є монотонно збільшується статистична величина, звана логарифмічною правдоподібністю. Метою алгоритму є оцінка середніх значень C, коваріацій R і ваг суміші W для функції розподілу ймовірності, описаної вище. Параметри, оцінені алгоритмом, зберігаються в таблиці 2.3 [62]:

Слід зазначити, що одна з популярних алгоритмів кластеризації k-means є окремим випадком алгоритму ЕМ, коли W і R постійні (табл. 2.3).

Таблиця 2.3.

Параметри, оцінені алгоритмом EM

Матриця	Розмір	Містить
C	q×k	Математичні очікування, μ
R	q×q	Коваріації, Σ
W	k×1	Ваги, w_i

Слід звернути увагу, що алгоритм може "застрягти" в локальному оптимумі і дати квазіоптимальне рішення при виборі невдалого початкового наближення. Тому одним з його недоліків слід вважати чутливість до вибору початкового стану моделі [62].

Для оптимізації використовуваного обсягу пам'яті, алгоритм може працювати в двох режимах. У першому завантажується тільки частина доступних даних і на їх основі робиться спроба побудови моделі. Якщо вона увінчалася успіхом, то алгоритм завершує роботу, в іншому випадку завантажується наступна порція даних і т.д., поки не будуть отримані прийнятні результати. У другому режимі завантажуються відразу всі наявні дані. Як правило, останній варіант забезпечує більш точну підгонку моделі, але пред'являє більш жорсткі вимоги до обсягу оперативної пам'яті [62].

Чисельний експеримент

Для ілюстрації роботи алгоритму EM і його порівняння з k-means розглянемо результати чисельного експерименту, для проведення якої була взята вибірка, представлена на рис. 2.8 [62].

Зверніть увагу, що вихідний набір даних не є простим з точки зору завдання кластеризації, оскільки є явне перекриття кластерів (області 1 і 3). В області 1 перекриваються кластери 1 і 3, а в області 3 кластери 4 і 5. Кластери 3 і 6 розташовані відокремлено і, як очікується, будуть легко розділено [62].

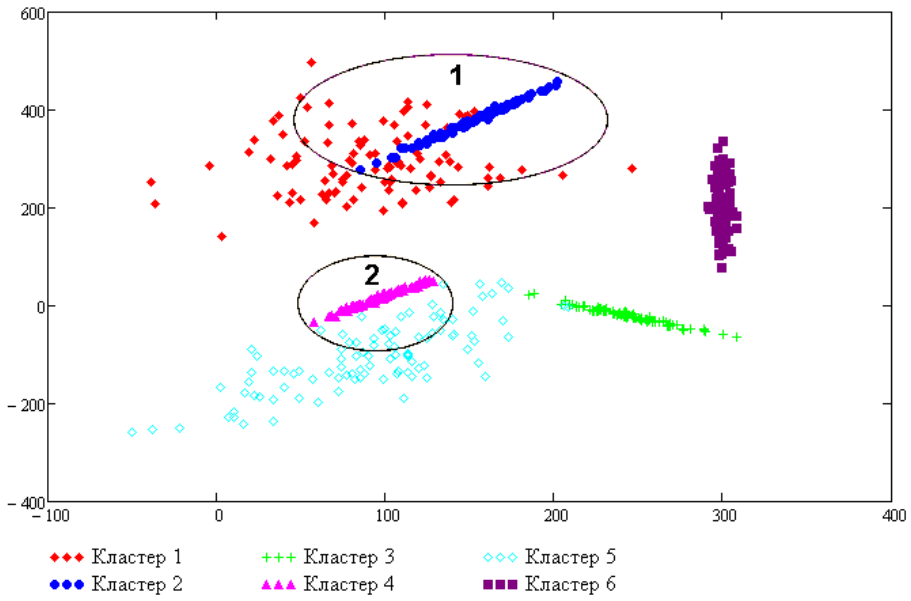


Рис. 2.8. Вихідні кластери

Для алгоритму k - means особливі труднощі повинні виникнути в місцях перекриття кластерів (рис. 2.9). Дане припущення підтверджується результатами, представленими на рис. [62].

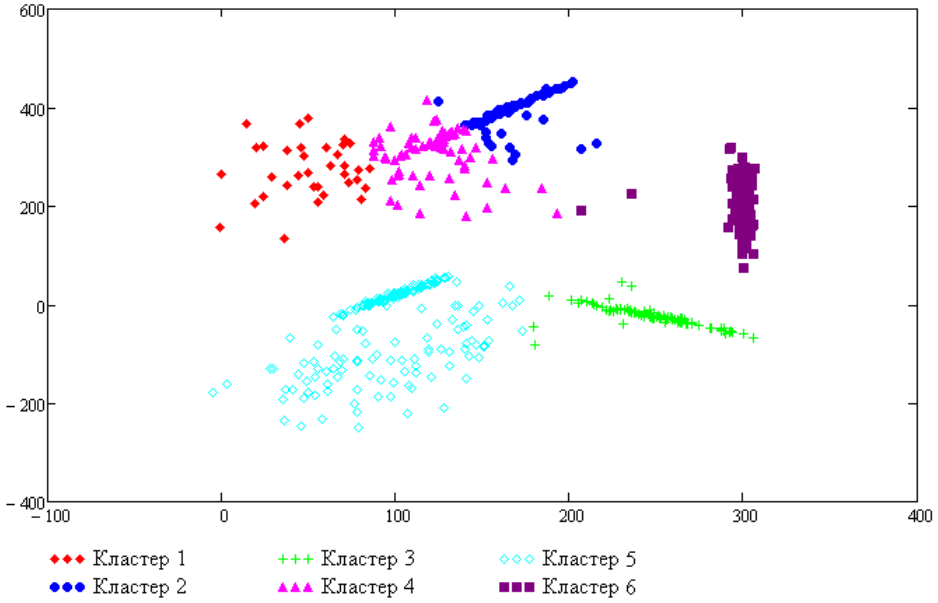


Рис. 2.9. Результати кластеризації k- means

У місцях перекриття кластерів спостерігається найбільше число помилок. У той же час відокремлені кластери 3 і 6 були розпізнані алгоритмом k - means без помилок. Як можна побачити на малюнку рис. 2.10, алгоритм EM вельми успішно виявив перекриваються кластери, хоча й майже не розпізнав кластер 6 [62].

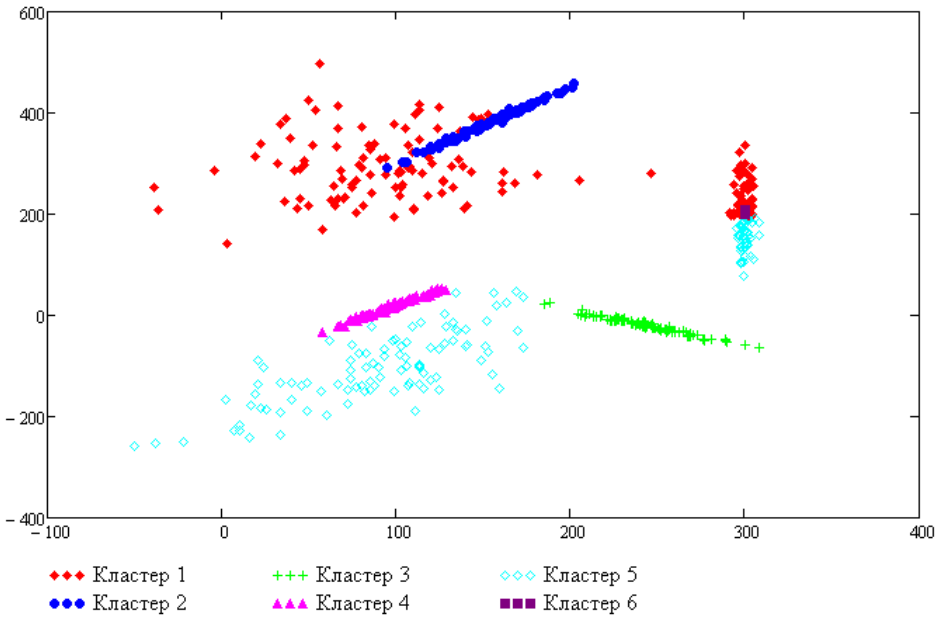


Рис. 2.10. Результати кластеризації EM

Таким чином, можна зробити висновок, що алгоритм k - means може мати перевагу при роботі з відокремленими (неперекривающіхся) кластерами, але повністю програє алгоритму EM при наявності їх перекриття [62].

2.4. Висновок до розділу

В боротьбі за безпеку інформаційної системи ефективність мають різноманітні методи аналізу кіберзагроз. Порівняльний аналіз існуючих методів виявлення кіберзагроз в ІС показав, що найбільш універсальним підходом до виявлення відомих і невідомих кіберзагроз є метод виявлення аномалій. Для підвищення стійкості функціонування ІС необхідний комбінований метод протидії комп'ютерним кіберзагрозам, який гнучко використовує елементи сигнатурного аналізу, виявлення аномалій, функціонального аналізу та статистичного методу для динамічно виконуваних функцій ІС.

Класифікація рівнів та станів загроз, які були розглянуті в межах нейронних мереж справедливі і для інших моделей аналізу кіберзагроз.

Отже для ефективного захисту інформаційного простору необхідно удосконалити методологію аналізу кіберзагроз методами машинного навчання

у поєднанні з статистичними методами відкритих каналів зв’язку на предмет прихованої інформації, яка може завдати шкоду інформаційному простору.

Розглянуто методи машинного навчання. Для передбачення значень залежної змінної використана регресійна модель. Також розглянуто критерій розподілу «Хі-квадрат» Пірсона, а також розглянуто методи кластерного аналізу. Показано переваги та недоліки даних алгоритмів.

Розділ 3. Алгоритм оцінки наявності прихованих кіберзагроз в каналі зв'язку

3.1. Причини приховування та канали передачі кіберзагроз

Сьогодні ми спостерігаємо новий і небезпечний тренд: все більше і більше розробників шкідливого ПЗ і засобів кібершпіонажу вдається до використання стеганографії для приховування кіберзагроз. Більшість антивірусних рішень на сьогоднішній день не захищають від стеганографії або захищають слабо, між тим, потрібно розуміти, що кожен заповнений контейнер небезпечний. У ньому можуть бути приховані дані, які ексфільтруются шпигунським ПЗ, або комунікація шкідливого ПЗ з командним центром, або нові модулі шкідливого ПЗ. Політична та економічна нестабільність окремих суб'єктів міжнародного права, є найулюбленіша мішень для хакерів та кібертерористів. Так одна з найсвіжіших атак «Cobalt» вивела з ладу банківські установки як мінімум в 14 країнах, включаючи Україну, Росію, Великобританію, Нідерланди та інші високорозвинені країни. Для проникнення у внутрішню мережу банку використовується точкова розсилка фішингових листів з стеганографічними вкладеннями. Проникнення і зараження здійснюється з використанням загальнодоступних інструментів. Найкоротший час отримання повного контролю над мережею банку - 10 хвилин.

Головні причини використання стеганографії [63,64]:

– Дозволяє приховати сам факт завантаження / вивантаження даних, а не тільки самі дані [63,64].;

– Допомагає обійти DPI-системи, що актуально в корпоративних мережах [63,64];

– Використання стеганографії може дозволити обійти перевірку в AntiAPT-продуктах, оскільки останні не можуть обробляти всі графічні файли (їх занадто багато в корпоративних мережах, а алгоритми аналізу досить дорогі);

– Антивірусні засоби взагалі і засоби захисту периметра зокрема мало що можуть зробити з заповненими контейнерами: їх дуже важко виявити оскільки вони виглядають як звичайні файли.

Розглянемо одну з найпоширеніших атак: «Zero.T». Потрапляючи в систему загальновідомими шляхами, наприклад через спам в пошті, даний вірус скачує основні та додаткові модулі у вигляді Bitmap-файлів (рис. 3.1, 3.2):

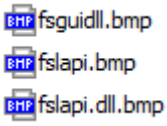


Рис. 3.1. Модулі вірусу приховані стеганографічними методами

Рис. 3.2. Загальній вигляд контейнерів в яких приховані кіберзагрози

Після чого обробляє їх особливим чином методами стеганографії, після чого отримуються шкідливі модулі (рис. 3.3):

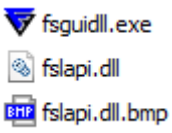


Рис. 3.3. Вірус після ексфільтрації з контейнерів.

При приховуванні шкідливий завантажувач «Zero.T» не стискає свої модулі перед впровадженням. Замість цього він збільшує кількість використовуваних найменш значущих біт: 1,2 або 4. Використання великої кількості найменш значущих біт приводить до появи візуальних артефактів у

зображенні, помітних простому користувачеві. Але ж мова йде про автоматичний аналіз.

Одним з найбільш перспективних підходів для виявлення факту існування та передачі прихованих кіберзагроз є підхід, який представляє приховування кіберзагроз як порушення статистичних закономірностей природних контейнерів. При цьому підході аналізуються статистичні характеристики досліджуваної послідовності і встановлюється, чи схожі вони на характеристики природних контейнерів (якщо так, то прихованої передачі інформації немає), або вони схожі на характеристики наповненого контейнера (якщо так, то виявлено факт існування прихованого каналу передачі інформації). Стегоаналіз це є один з підвидів статистичних моделей аналізу кіберзагроз, через те що вони не дають однозначної відповіді, а формують оцінки типу «дана досліджувана послідовність з ймовірністю 90% містить кіберзагрозу». Імовірнісний характер статистичних методів стегоаналізу не є істотним недоліком, так як на практиці ці методи часто видають оцінки ймовірності існування кіберзагрози, що відрізняються від одиниці або нуля на нескінченно малі величини [63,64].

Для непомітного вбудовування даних стеганокодер повинен вирішити три задачі: виділити підмножину біт, модифікація яких мало впливає на якість (незначущі біти), вибрати з цієї підмножини потрібну кількість біт відповідно до розміру прихованого повідомлення і виконати їх зміну. Якщо статистичні характеристики контейнеру не змінилися, то вбудовування інформації можна рахувати успішним. Так як розподіл незначущих біт часто близько до білого шуму, то вбудовані дані повинні мати той же характер. Це досягається за рахунок попереднього шифрування повідомлення або його стиснення [13].

Аналітік на основі вивчення сигналу завжди може виділити підмножину незначущих біт, роблячи ті ж припущення, що і в стеганографії. Далі він повинен перевірити відповідність їх статистичні характеристики. При цьому, якщо аналітик має у своєму розпорядженні кращу модель, даних, ніж стеганограф, то вкладення буде виявлено. Тому, по-справжньому хороші

моделі сигналів різного характеру, ймовірно, тримаються в секреті, і ви не зустрінете їх у відкритих публікаціях. Можна лише дати рекомендації загального характеру.

Звернемо увагу, що всі метод аналізу кіберзагроз не виносить бінарного вердикту «містить цей контейнер приховану кіберзагрозу», замість цього він визначає приблизний відсоток прихованої кіберзагрози (у відсотках).

Канали передачі кіберзагроз:

– Дискети. Найпоширеніший канал зараження в 1980-1990-і роки. Зараз практично відсутня через появу більш поширених і ефективних каналів і відсутності флоппі-дисководів на багатьох сучасних комп'ютерах.

– Носії даних («флешки»). В даний час USB-накопичувачі замінюють дискети і повторюють їх долю - велика кількість вірусів поширюється через знімні накопичувачі, включаючи цифрові фотоапарати, цифрові відеокамери, портативні цифрові плеєри, а з 2000-х років все більшу роль відіграють мобільні телефони, особливо смартфони (з'явилися мобільні віруси). Використання цього каналу раніше було переважно зумовлене можливістю створення на накопичувачі спеціального файлу autorun.inf, в якому можна вказати програму, що запускається Провідником Windows при відкритті такого накопичувача.

– Електронна пошта. Зазвичай віруси в листах електронної пошти маскуються під нешкідливі вкладення: картинки, документи, музику, посилання на сайти. У деяких листах можуть міститися дійсно тільки посилання, тобто в самих листах може і не бути шкідливого коду, але якщо відкрити таку посилання, то можна потрапити на спеціально створений веб-сайт, що містить вірусний код. Багато поштових вірусів, потрапивши на комп'ютер користувача, потім використовують адресну книгу з встановлених поштових клієнтів типу Outlook для розсилки самого себе далі.

– Системи обміну миттєвими повідомленнями. Тут також поширена розсилка посилань на нібито фото, музику або програми, в дійсності є вірусами, по Viber і через інші програми миттєвого обміну повідомленнями.

– Веб-сторінки. Можливо також зараження через сторінки Інтернету через наявність на сторінках всесвітньої павутини різного «активного» вмісту: скриптів, ActiveX-компонент. В цьому випадку використовуються уразливості програмного забезпечення, встановленого на комп'ютері користувача, або уразливості в ПЗ власника сайту (що небезпечніше, тому що зараження піддаються добропорядні сайти з великим потоком відвідувачів), а нічого не підозрюють користувачі, зайшовши на такий сайт, ризикують заразити свій комп'ютер .

– Інтернет і локальні мережі (черви). Черви - вид вірусів, які проникають на комп'ютер-жертву без участі користувача. Черви використовують так звані «дірки» (уразливості) в програмному забезпеченні операційних систем, щоб потрапити до електронної пошти. Уразливості - це помилки і недоробки в програмному забезпеченні, які дозволяють віддалено завантажити і виконати машинний код, в результаті чого вірус-черв'як потрапляє в операційну систему і, як правило, починає дії по зараженню інших комп'ютерів через локальну мережу або Інтернет. Зловмисники використовують заражені комп'ютери користувачів для розсилки спаму або для DDoS-атак.

Тому ціллю даної роботи є, на основі поєднання статистичних моделей та моделі кінцевих автоматів, розробити алгоритм бінарної класифікації кіберзагроз в каналі зв’язку, який дозволить зменшити кількість станів кіберзагрози, завдяки чому зменшиться кількість ресурсів для виконання первинного аналізу вхідної інформації.

3.2. Статистична оцінка двох класів контейнерів

Для дослідження скористаємося двома типами контейнерів, їх гістограмами і бітовими зрізами найменш значимого біта (рис. 3.4 - 3.9)[65].

Рис. 3.4. Порожній контейнер

Рис. 3.5. Заповнений контейнер

Рис. 3.6. Півтонове уявлення порожнього контейнера

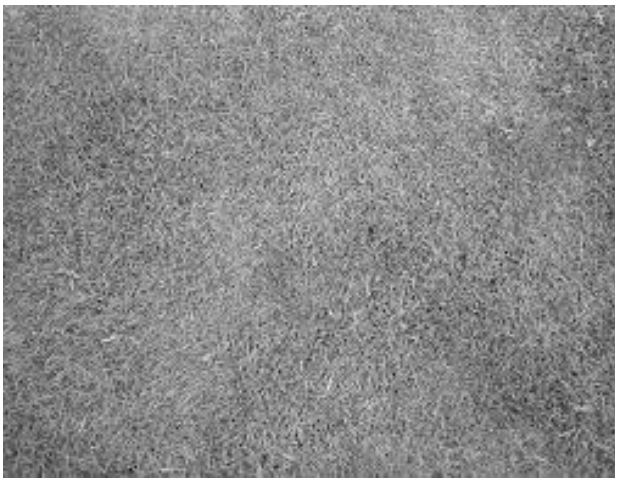


Рис. 3.7. Півтонове уявлення заповненого контейнера

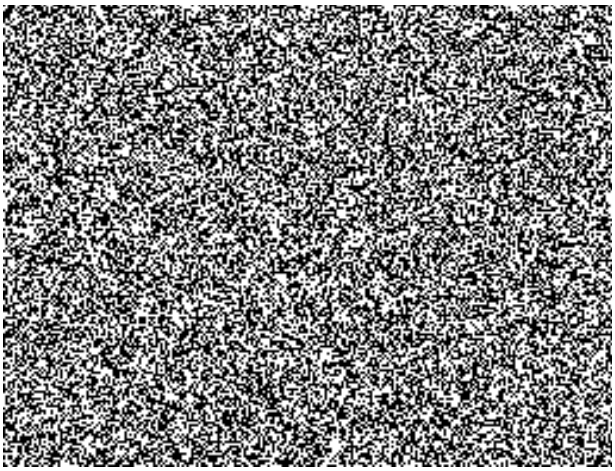


Рис. 3.8. Зріз найменш значимого біта червоного спектра порожнього контейнера

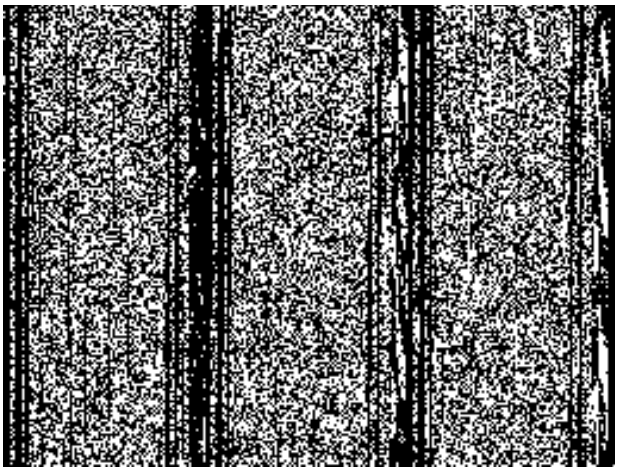


Рис. 3.9. Зріз найменш значимого біта червоного спектра заповненого контейнера

Контейнер в загальному випадку можна визначити як двомірну функцію I(i, j) де i і j - це просторові (площинні) координати, а амплітуда I для кожної пари координат (i, j) називається інтенсивністю або яскравістю контейнера в точці з цими координатами. Самі координати (i, j) називаються пікселями [65].

Для імовірнісних методів аналізу даних необхідно від гістограми перейти до розподілу випадкової величини (Рис. 3.7). Гістограма H(x) (3.1) групує відліки, що мають однакові величини, разом. Це дозволяє обчислювати статистику, працюючи з групами, а не з великим числом окремих відліків [65].

$$H(x) = G(I(i,j)) \tag{3.1}$$

G- функція угруповання вибірки випадкових величин;

Таким чином, верхня частина контуру гістограми утворює статистичний аналог для щільності ймовірності f(x), так само, як і емпірична функція є статистичним аналогом для функції розподілу [65].

Інтеграл від щільності ймовірності Ф(x) (3.2) використовується для знаходження ймовірності знаходження сигналу всередині певної області величин. Це робить інтеграл від щільності розподілу ймовірності досить важливим для класифікації, тому необхідно його розглядати в цьому дослідженні [65].

$$\Phi(x) = \int_{-\infty}^{\infty} f(x)\,dx \tag{3.2}$$

Як видно з дослідження гістограма приймає форму нормального закону розподілу, де інтегральна функція розподілу яркостей пікселів контейнера має вигляд (3.3) і зображена на рис. 3.8.

$$f(x) = \frac{1}{\sqrt{3\pi}\sigma} e^{-\frac{(x-m)^3}{3\sigma^3}} \tag{3.3}$$

При детальному розгляді графіків видно, що вони трохи зміщені відносно один одного, це свідчить про те, що змінюються статистичні характеристики контейнера при встановленні шкідливої інформації. Це легко

проконтролювати оцінками математичного очікування, дисперсії і середньоквадратичного відхилення (табл. 3.1) [65].

Таблиця 3.1.

Статистичні характеристики контейнерів

	Порожній контейнер	Заповнений контейнер
Математичне очікування	0.5150	0.5350
дисперсія	0.0317	0.0337
середньоквадратичне відхилення	0.1194	0.1160

З гістограм яскравостей пікселів, законів розподілу та статистичних характеристик, які отримані в ході експериментів, можна зробити висновок в їх відмінностях, на основі яких і буде проводитися подальша оцінка і класифікація контейнерів.

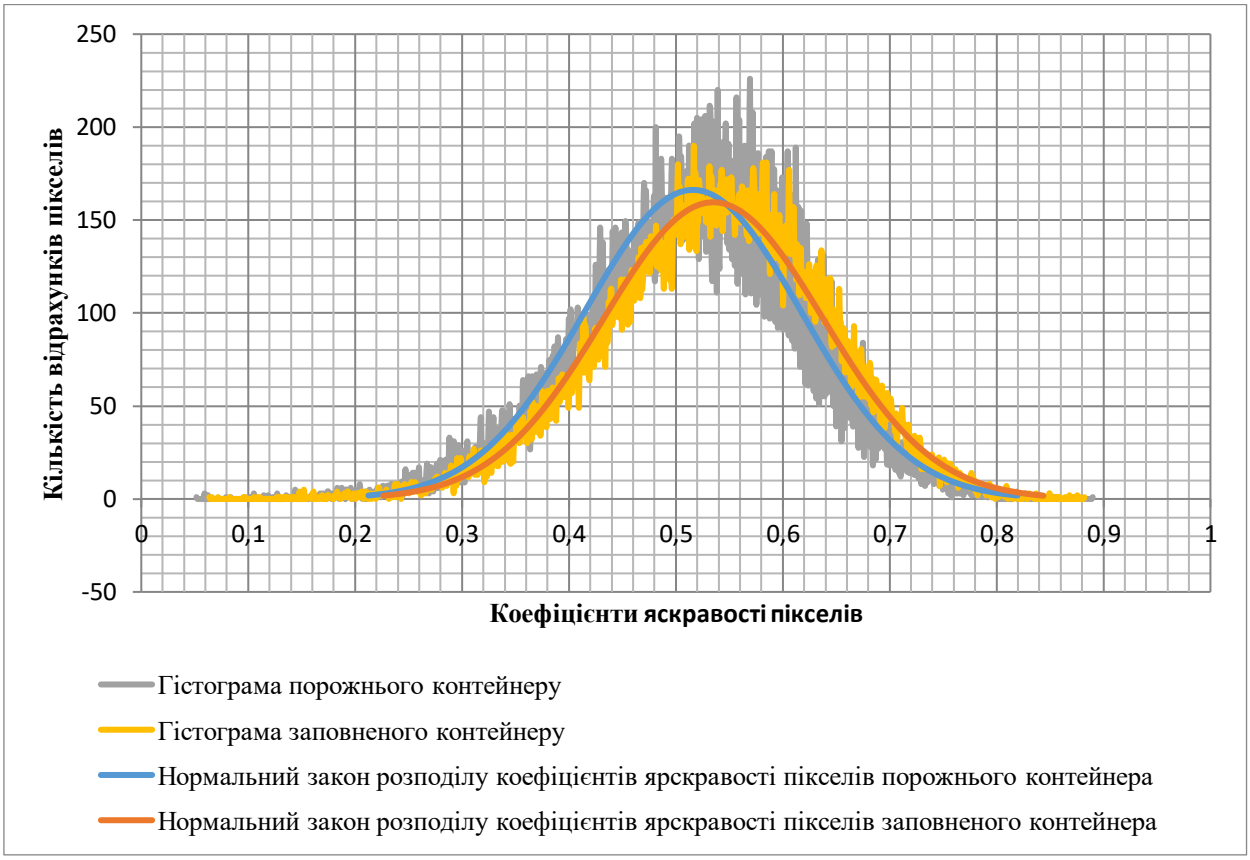


Рис. 3.10. Гістограма порожнього і заповненого контейнера з розподілом коефіцієнтів яскравості пікселів.

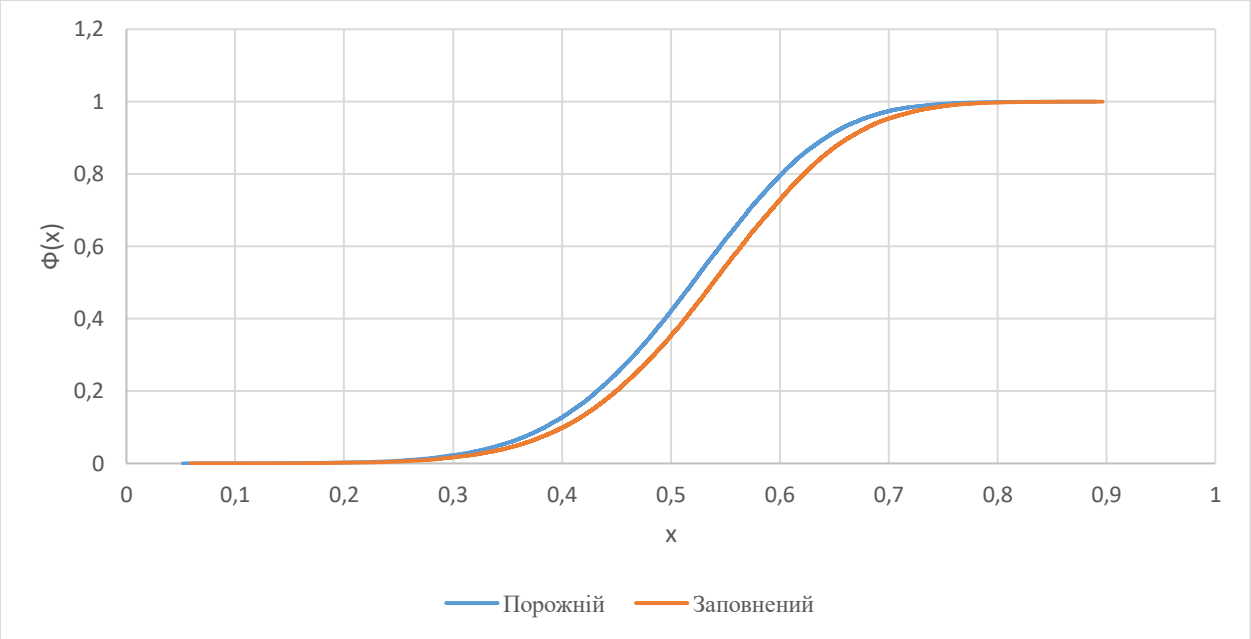


Рис. 3.11. Інтегральна оцінка розподілу ймовірності коефіцієнтів яскравості пікселів Ф (x) заповненого (помаранчевий) і порожнього (синій) контейнерів, де x - координати коефіцієнтів яскравості пікселя.

Проведемо заповнення порожнього контейнера корисною інформацією, з різним відсотком заповнення. В одному випадку глибина зміни бітів буде тільки 1 біт, а в іншому випадку – 3 біти. Обчислимо статистичні характеристики: математичне очікування, дисперсія, середньоквадратичне відхилення та побудуємо графіки зміни цих характеристик відповідно до відсотка заповнення контейнера (табл. 3.2, рис. 3.10, 3.11).

Таблиця 3.2.

Результати оцінки контейнерів

Відсоток заповнення	Глибина заповнення - 1 біт		Глибина заповнення - 3 біт	
	Математичне очікування		Середньоквадратичне відхилення	
1	2	3	4	5
1	0,385456	0,38545	0,343058	0,343063
2	0,385455	0,385444	0,343059	0,343013
3	0,385453	0,385437	0,343059	0,343017
4	0,385451	0,385433	0,343061	0,343014

Продовження табл. 3.2.

1	2	3	4	5
5	0,385449	0,385435	0,343063	0,343014
6	0,385448	0,385415	0,343063	0,343089
7	0,385446	0,385413	0,343065	0,343093
8	0,385445	0,385404	0,343013	0,343105
9	0,385443	0,385398	0,343017	0,343113
10	0,385441	0,385393	0,343068	0,343133
11	0,38544	0,385387	0,343073	0,34313
12	0,385437	0,38538	0,343073	0,343139
13	0,385436	0,38537	0,343014	0,343144
14	0,385434	0,385363	0,343078	0,343147
15	0,385433	0,385356	0,343078	0,343149
16	0,385431	0,38535	0,34308	0,343154
17	0,385439	0,385345	0,343013	0,34317
18	0,385438	0,385339	0,343085	0,343131
19	0,385436	0,385338	0,343088	0,34317
20	0,385436	0,385331	0,343086	0,343131
21	0,385433	0,385311	0,343088	0,343114
22	0,385417	0,385398	0,34309	0,34317
23	0,385415	0,385388	0,343086	0,343157
24	0,385414	0,385331	0,343089	0,343147
25	0,385413	0,385317	0,343088	0,343149
26	0,38541	0,385359	0,343094	0,343141
27	0,385407	0,38535	0,343093	0,343147
28	0,385407	0,385345	0,343093	0,343141
29	0,385404	0,385336	0,343094	0,343147
30	0,385403	0,385333	0,343097	0,343144
31	0,385401	0,385333	0,343098	0,343149

Продовження табл. 3.2.

1	2	3	4	5
32	0,385399	0,38533	0,343098	0,343143
33	0,385396	0,385308	0,343101	0,343145
34	0,385394	0,385196	0,343105	0,343159
35	0,385393	0,385131	0,343106	0,343114
36	0,385393	0,385131	0,343104	0,343131
37	0,385391	0,385178	0,343108	0,343178
38	0,38539	0,385159	0,343109	0,343193
39	0,385388	0,385149	0,343111	0,343116
40	0,385385	0,385148	0,343117	0,343194
41	0,385384	0,385141	0,343119	0,343179
42	0,385384	0,385133	0,343119	0,343196
43	0,385316	0,38513	0,343131	0,343199
44	0,38538	0,385137	0,343131	0,34331
45	0,385333	0,385114	0,343133	0,343198
46	0,385377	0,385109	0,343135	0,343305
47	0,385330	0,385107	0,343139	0,343309
48	0,385330	0,385101	0,343136	0,343314
49	0,38537	0,385094	0,343136	0,343333
50	0,385364	0,38508	0,343136	0,343333
51	0,385368	0,385014	0,343133	0,343333
52	0,385364	0,385014	0,343131	0,343338
53	0,385365	0,385061	0,343135	0,343336
54	0,385359	0,385053	0,343133	0,343343
55	0,385358	0,385034	0,343131	0,343364
56	0,38536	0,385033	0,343131	0,343336
57	0,385357	0,385039	0,343136	0,34334
58	0,385353	0,385017	0,343137	0,343354

Продовження табл. 3.2.

1	2	3	4	5
59	0,385353	0,385013	0,343138	0,343349
60	0,385353	0,384999	0,343134	0,343338
61	0,385346	0,384987	0,343133	0,343334
62	0,385346	0,384998	0,343143	0,343344
63	0,385343	0,384968	0,343138	0,343341
64	0,385336	0,384973	0,343141	0,343347
65	0,38534	0,384959	0,343139	0,343363
66	0,385336	0,384951	0,343138	0,343357
67	0,385333	0,384945	0,34314	0,34335
68	0,385334	0,384937	0,343146	0,343357
69	0,38533	0,384914	0,343149	0,343361
70	0,385331	0,384933	0,343144	0,343356
71	0,385338	0,384919	0,343147	0,343336
72	0,385333	0,384907	0,343146	0,343336
73	0,385333	0,384899	0,343148	0,343333
74	0,385334	0,384888	0,343143	0,343344
75	0,38533	0,384877	0,343145	0,343334
76	0,385314	0,384864	0,343148	0,343333
77	0,385317	0,384861	0,34314	0,343336
78	0,38531	0,384854	0,343144	0,343197
79	0,385313	0,384848	0,343151	0,343178
80	0,385313	0,384831	0,343144	0,343199
81	0,385305	0,384133	0,343148	0,343315
82	0,385304	0,384131	0,343144	0,343193
83	0,385307	0,384161	0,343148	0,343193
84	0,385303	0,384148	0,343148	0,343177
85	0,385303	0,384145	0,343144	0,343177

Продовження табл. 3.2.

1	2	3	4	5
86	0,385303	0,384196	0,343143	0,343113
87	0,385399	0,384731	0,343157	0,343114
88	0,385396	0,38433	0,343146	0,343146
89	0,385393	0,384313	0,343143	0,343143
90	0,385389	0,384309	0,343144	0,343136
91	0,38539	0,384306	0,343149	0,343117
93	0,385386	0,384736	0,343153	0,343099
93	0,385386	0,384735	0,343155	0,34309
94	0,385378	0,384731	0,34317	0,343098
95	0,385333	0,384184	0,343144	0,343103
96	0,385314	0,384131	0,343145	0,343091
97	0,385330	0,384688	0,343146	0,343063
98	0,385330	0,384683	0,343145	0,343044
99	0,385331	0,384673	0,34315	0,343056
100	0,385368	0,384135	0,343145	0,343063

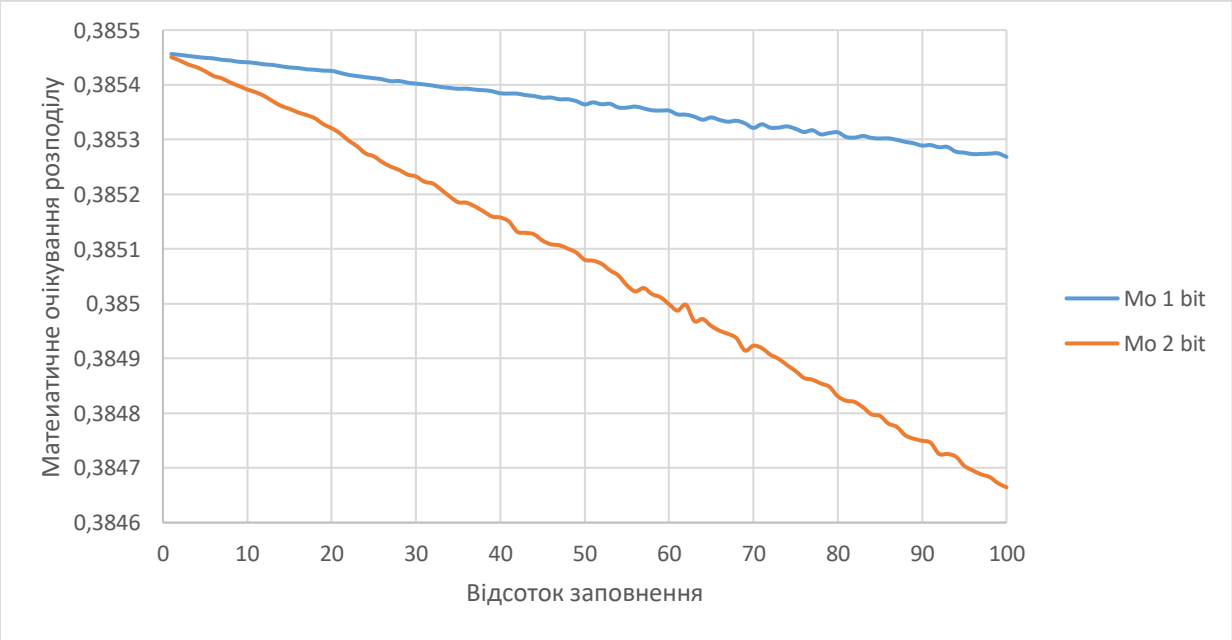


Рис. 3.12. Математичне очікування для контейнерів з глибиною заміни – 1 біт та з глибиною – 2 біти.

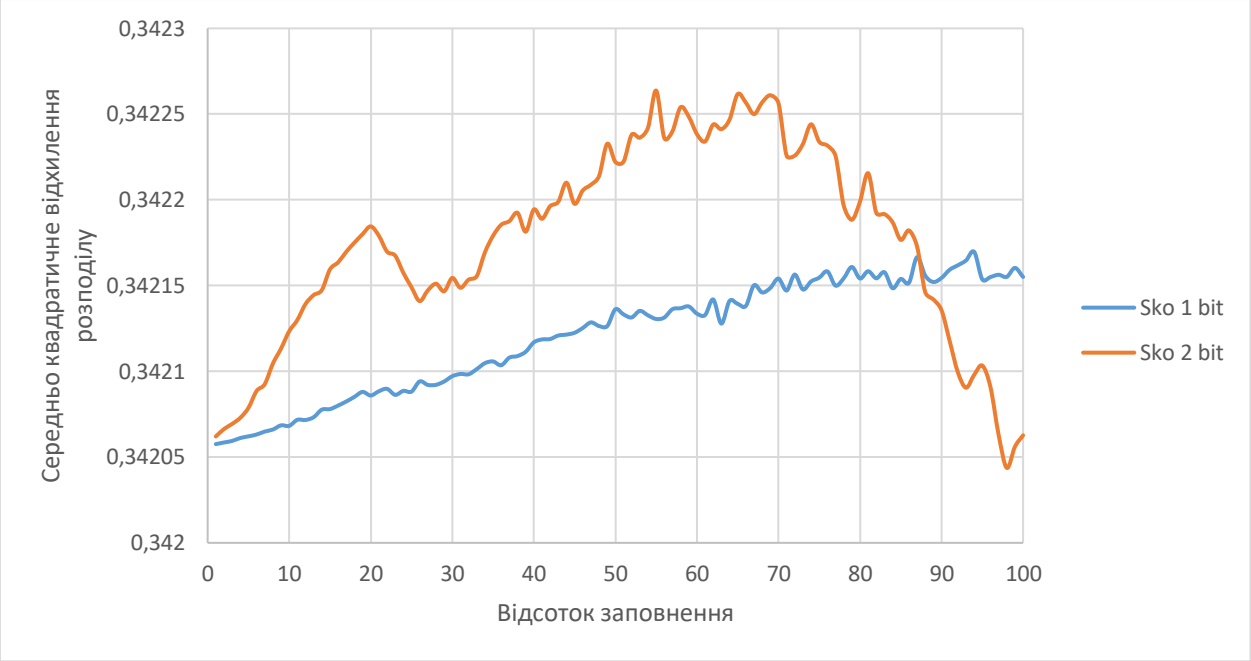


Рис. 3.13. Середньоквадратичне відхилення для контейнерів з глибиною заміни – 1 біт та з глибиною – 2 біти.

Отримані результати під час моделювання показали, що статистичні характеристики заповненого контейнеру є меншим ніж незаповненого контейнеру.

3.3. Принци роботи системи класифікації кіберзагроз на основі розпізнавання образів та машинного навчання

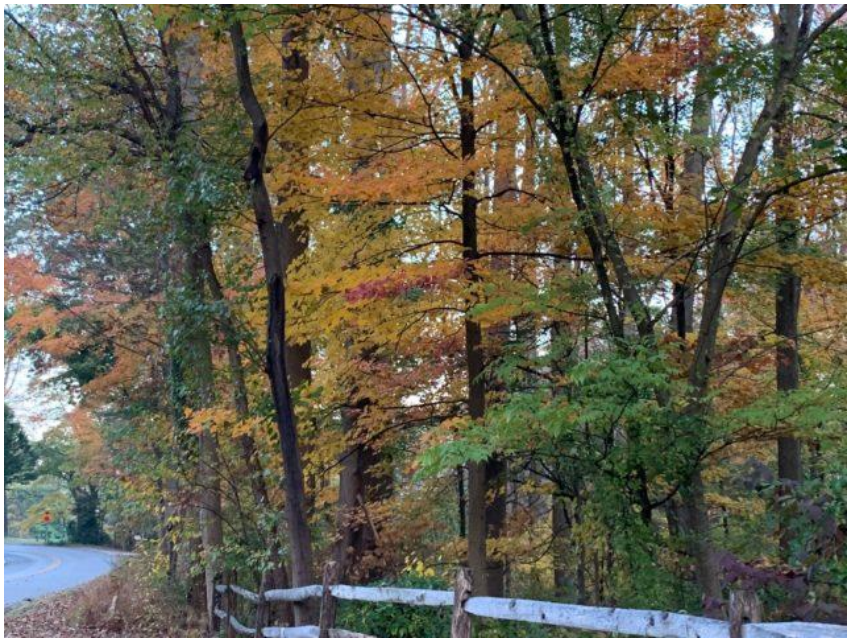


Рис. 3.14. Досліджуваний об’єкт

На вхід системи подається досліджуваний об’єкт (рис. 3.14), з якого робиться копія для подальших математичних перетворень.

Дослідження [13] показали, що зріз найменш значимих біт в фотореалістичноу цифровому зображенні є шумом, тому для моделювання математичної моделі порожнього контейнеру будемо використовувати дане твердження. Скористаємося копією досліджуваного контейнеру, та замінимо існуючий зріз шару найменш значимих бітів, бінарною послідовністю гаусовськоого щуму з параметрами: математичне сподівання дорівнює нулю, середньоквадратичне відхиленя дорівнює одиниці.

Далі виконаємо зміну шару бітів LSB та MSB місцями, для підсилення значень шару LSB обох контейнерів: досліджуваного та його математичної моделі порожнього контейнеру (рис.3.15, 3.16).

Рис. 3.15. Математична модель порожнього контейнеру, отримана з досліджуваного зразка, методом перестановки шару бітів LSB та MSB місцями.

На основі отриманих результатів після заміни біт, виконаємо наступне перетворення: з 3-х кольорової моделі RGB переведемо в напівтонові зображення та побудуємо гістограми на основі яких, буде побудований графік нормального закону розподілу.

Рис. 3.16. Досліджуваний об’єкт, отриманий методом перестановки шару бітів LSB та MSB місцями.

З отриманих графіків закону розподілу обчислимо такі статистичні характеристики: математичне очікування, дисперсія та середньо квадратичне відхилення. Отримані статистичні характеритики класів відрізняються між собою (табл. 3.3), що дає змогу використати математичний апарат розпізнавання образів та математичного навчання для класифікації отриманих об’єктів. Результати даного твердження представлені в розділі 3.2. Варто зазначити одну важливу деталь в розділі 3.2 проводилися дослідження на прямому порядку біт, тобто без перестановки, але результати які були отримані в ході дослідження з об’єктами де була виконана заміна біт,

припущення про зменшення кількісної оцінки статистичних характеристик від відсотка заповнення повністю підтверджується.

Вирішувальний пристрій в умовах апріорної невизначеності не має можливості безпосередньо визначити, які статистичні характеристики відносяться до яких класів досліджуваних об’єктів, бо досліджуваний об’єкт не містить ніяких відомостей, які б вказували до якого класу об’єкт може належати.

Таблиця 3.3.

Статистичні характеристики досліджуваного об’єкту

	Математична модель порожнього контейнера	Заповнений контейнер
Математичне очікування	0.4978	0.5520
Дисперсія	0.1393	0.1270
середньоквадратичне відхилення	0.3733	0.3564

Процес формування підмножин статистичних характеристик, які наділені такими характеристика, при яких виконується умова близькості оцінок {Mo, D, Sko} до істинних значень статистичних характеристик класів, що очевидно можна також отримати хороші оцінки в режимі навчання з вчителем, будемо називати розділення суміші сигналів або класифікація.

В розроблюваному алгоритмі необхідно класифіковувати контейнери не до абстрактних класів, а до реальних класів: {заповнений, порожній}. Задача класифікації в даному режимі самонавчання є специфічною. Тому даний режим класифікації є одним з елементів загальної системи класифікації та грає велику роль, оскільки використання даного режиму, значно знижує вимоги до апріорної інформації про класи, що дозволяє скоротити обчислювальні

ресурси. Інформація в даному режимі може бути вельми схематичною, достатньо лише знати приблизне співвідношення статистичних характеристик досліджуваних класів. Такою інформацією може виступити площа фігури яка перекривається нормальними розподілами, або евклідова відстань між математичними сподіваннями, що побудовані на основі гістограми досліджуваних об’єктів.

Наступним кроком в алгоритмі є оцінка отриманих результатів на основі нечіткої первинної інформації. Для цього використаємо пряму структуру самонавчання (рис 3.17):

Рис. 3.17. Пряма структура самонавчання

Завдяки нечіткій інформації про прив’язку досліджуваних контейнерів до класів, можлива в найкоротші терміни класифікація отриманих контейнерів згідно описаних характеристик класів не чекаючи на інші об’єкти.

Після накопичення результатів можливе використання моделі системи самонавчання зі зворотнім зв’язком із вже накопиченими результатами які також отримані на основі результатів класифікації попередньою моделлю.

Результатом роботи алгоритму є бінарна класифікація досліджуваних об’єктів між двома класами: порожній та заповнений.

Отриманий результат застосовується для зменшення кількості станів кіберзагроз в моделі кінцевих автоматів. До використання алгоритму були такі стани як: {нульовий, дуже низький, низький, нижче середнього, помірний, вище середнього, високий, дуже високий, критичний}, то після використання алгоритму класифікації наведені стани скорочуються до двох: {атака не відбудеться, атака відбудеться}. Якщо алгоритм класифікації класифікував канал зв'язку, як такий, що має приховану кіберзагрозу, то вхідна інформація для системи захисту буде такою {атака відбудеться}, що дозволить своєчасно та ефективніше виконати захист ресурсів в інформаційному просторі. Якщо алгоритм класифікації класифікував канал зв'язку, як такий, що не містить приховану кіберзагрозу, то вхідна інформація для системи захисту буде такою {атака не відбудеться}, що дозволить скоротити та зекономити вичерпні ресурси інформаційного простору.

3.4. Висновок до розділу

Отримані результати під час моделювання показали, що статистичні характеристики відкритих каналів зв'язку без прихованих кіберзагроз та з прихованими кіберзагрозами будуть сильно різниться. Це дало змогу провести математичну класифікацію відкритих каналів зв'язку на предмет прихованих кіберзагроз.

Дослідження показали, що твердження про те, що зміна статистичних характеристик обернено пропорційна відсотку прихованих даних в об'єкті. Дане твердження вірне як для прямого порядку біт, так і з перестановкою шарів біт LSB та MSB місцями.

На основі поєднання статистичних моделей, моделі кінцевих автоматів для аналізу кіберзагроз та методів машинного навчання, було розроблено алгоритм класифікації кіберзагроз, що дозволило зменшити кількість станів кіберзагроз у каналі зв'язку, що в спою чергу дозволяє зменшити кількість ресурсів на виконання первинного аналізу вхідної інформації.

ВИСНОВКИ

Результатом виконання роботи є вирішення задачі оцінки наповненості каналу зв’язку прихованою інформацією, що може бути використано в умовах великого потоку даних

У процесі виконання роботи були отримані наступні результати:

1. Проаналізовано існуючі методи аналізу кіберзагроз на основі нормативно-правового регулювання законодавства України. При досліджені різних видів кіберзагроз основною і часто надважливою складовою є канал зв’язку жертви в інформаційній системі і системи управління зловмисника, або інсайдера з його кураторами. Часто даний канал зв’язку є прихований. Тому дослідження даних каналів зв’язку є найважливішим з етапів дослідження кіберзагроз в цілому.

2. Проаналізовано математичні моделі аналізу кіберзагроз та канали передачі прихованої інформації. Для підвищення стійкості функціонування ІС необхідно комбінувати методи протидії комп'ютерним кіберзагрозам, який гнучко використовує елементи сигнатурного аналізу, евристичного, функціонального та статистичного аналізу для динамічно виконуваних процесів в інформаційній системі.

3. На основі поєднання статистичних моделей, моделі кінцевих автоматів для аналізу кіберзагроз та методів машинного навчання, було розроблено алгоритм класифікації кіберзагроз, що дозволило зменшити кількість станів кіберзагроз у каналі зв’язку, що в спою чергу дозволяє зменшити кількість ресурсів на виконання первинного аналізу вхідної інформації

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Електронний ресурс Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури: http://www.dsszzi.gov.ua/dsszzi/control/ uk/publish/ Режим доступу: вільний.

2. Конахович Г.Ф. Защита информации в телекоммуникационных системах. / Г.Ф. Конахович – К.: МК-Пресс, 2014. – 334 с.

3. Шматок А.С. Методы анализа критических данных на основе машинного обучения. / А.С. Шматок, Ю.И. Финенко // ОРАЛДЫҢ ҒЫЛЫМ ЖАРШЫСЫ - №3 (174) 2019. - Оралқаласы, ЖШС «Уралнаучкнига», 2019. – С. 58-62.

4. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В.. «Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]». - 2015.

5. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

6. Електронний ресурс: Серчинформ https://searchinform.ru/resheniya /biznes-zadachi/zaschita-personalnykh-dannykh/model-ugroz-bezopasnosti-personalnyh-dannyh/ Режим доступу: вільний.

7. Електронний ресурс: BAE Systems: Анализа киберугроз http://www.tadviser.ru/index.php /BAE_Systems Режим доступу: вільний.

8. Електронний ресурс: Анализ угроз информационной безопасности 2016-2017 https://www.antimalware.ru/analytics/Threats_Analysis/ Analysis_information_security_threats_2016_2017 Режим доступу: вільний.

9. Миленький А.В. Классификация сигналов в условиях неопределенности. М.: Советское радио, 1975. 328 с.

10. Bilmes J. A Gentle Tutorial of the EM Algorithm and its Application to Parameter Estimation for Gaussian Mixture and Hidden Markov Models / J.Bilmes; International Computer Science Institute .— Berkeley: Computer Science Division Department of Electrical Engineering and Computer Science, 1998 .— 15 с.

11. Data Analysis, Machine Learning and Applications / C.Preisach, H.Burkhardt, L.Schmidt-Thieme, R.Decker and etc.; Proceedings of the 31st Annual Conference of the Gesellschaft für Klassifikation, Albert-Ludwigs-Universität Freiburg, March 7–9, 2007 .— Berlin Heidelberg: Springer-Verlag, 2008 .— 703 p.

12. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб.: Питер, 2003, 368 с.

13. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. - М.: Солон-Пресс, 2002

14. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. — Springer, 2001

15. Електронний ресурс: eLibrary https://elibrary.ru/item.asp ?id=41137645/. Режим доступу: вільний.

16. Айвазян С. А., Бухштабер В. М., Енюков И. С., Мешалкин Л. Д. Прикладная статистика: классификация и снижение размерности. — М.: Финансы и статистика, 1989.

17. Вапник В. Н., Червоненкис А. Я. Теория распознавания образов. — М.: Наука, 1974.

18. Вапник В. Н. Восстановление зависимостей по эмпирическим данным. — М.: Наука, 1979.

19. Дуда Р., Харт П. Распознавание образов и анализ сцен. — М.: Мир, 1976.

20. Charu C. Aggarwal Data Mining. The Textbook. / C.A.Charu; — Springer, 2015 .— 746 p.

21. Christopher M. Bishop Pattern Recognition and Machine Learning / M.B.Christopher .— Springer, 2006 .— 758 p.

22. Clarke B. Principles and Theory for Data Mining and Machine Learning / B.Clarke, E.Fokoue, H.Zhang .— Dordrecht Heidelberg London New York: Springer, 2009 .— 793 c.

23. Engelmann B. The Basel II Risk Parameters / B.Engelmann, R.Rauhmeier; Estimation, Validation, Stress Testing – with Applications to Loan

Risk Management .— Heidelberg Dordrecht London New York: Springer, 2011 .— 419 c.

24. Giudici P. Applied data mining: statistical methods for business and industry / P.Giudici .— West Sussex, England: John Wiley & Sons Ltd, 2003 .— 378 c.

25. Goodfellow I. Deep Learning / I.Goodfellow, Y.Bengio, A.Courville .— MIT: MIT Press, 2016 .— 800 c.

26. Hand D. Principles of Data Mining / D.Hand, H.Mannila, P.Smyth .— MIT: The MIT Press, 2001 .— 546 c.

27. Hastie T. The Elements of Statistical Learning Data Mining, Inference, and Prediction / T.Hastie, R.Tibshirani, J.Friedman; Second Edition .— Springer, 2017 .— 764 p.

28. Lausen B. Data Science, Learning by Latent Structures, and Knowledge Discovery / B.Lausen, S.Krolak-Schwerdt, M.Böhmer .— Berlin Heidelberg: Springer, 2015 .— 552 c.

29. McLachlan G.J. The EM algorithm and extensions / G.J.McLachlan, T.Krishnan .— New York: John Wiley & Sons, Inc., 1997 .— 288 c.

30. Nisbet R. Handbook of statistical analysys and data mining applications / R.Nisbet, J.Elder, G.Miner .— San Diego: Elsevier Inc., 2009 .— 860 c.

31. Pattern, Recognition and Machine Intelligence / Sergei O. Kuznetsov Deba P. Mandal Malay K. Kundu Sankar K. Pal (Eds.); 4th International Conference, PReMI 2011 Moscow, Russia, June 27 – July 1, 2011 Proceedings .— Springer, 2011 .— 495 p.

32. Sammut C. Encyclopedia of Machine Learning / C.Sammut, G.Webb .— NY: Springer Science+Business Media, 2010 .— 1059 p.

33. Shalev-Shwartz S. Understanding Machine Learning: From Theory to Algorithms / S.Shalev-Shwartz, S.Ben-David .— Cambridge: Cambridge University Press., 2014 .— 449 c.

34. Wang J. Encyclopedia of Data Warehousing and Mining / J.Wang; Second Edition .— Hershey: Information Science Reference, 2009 .— 2227 p.

35. Watanabe M. The EM Algorithm and Related Statistical Models / M.Watanabe, K.Yamaguchi .— NY, Basel: Marcel Dekker, Inc., 2004 .— 214 с.

36. Королев В.Ю. ЕМ-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. / В.Ю.Королев; Теоретический обзор .— М.: ИПИ РАН, 2007 .— 94 с.

37. Прикладная статистика. Классификация и снижение размерности. / С.А.Айвазян, В.М.Бухштабер, И.С.Енюков, Л.Д.Мешалкин .— М.: Финансы и статистика, 1989 .— 607 с.

38. Шумейко А.А., Сотник С.Л. Интеллектуальный анализ данных (Введение в Data Mining).-Днепропетровск:Белая Е.А., 2012.- 212 с.

39. Эсбенсен К. Анализ многомерных данных / К.Эсбенсен .— Черноголовка: ИПХФ РАН, 2005 .— 160 с.

40. Годин, А. М. Статистика: учебник / А. М. Годин. – Москва: Дашков и К°, 2016. – 451 с.

41. Гореева, Н. М. Статистика в схемах и таблицах /. – Москва: Эксмо, 2017. – 414 с.

42. Едроновва Общая теория статистики / Едроновва, В.Н; Едронова, М.В.. - М.: ЮРИСТЪ, 2017. - 511

43. Елисеева, И. И. Статистика: [углубленный курс]: учебник для бакалавров / И. И. Елисеева и др.]. – Москва: Юрайт: ИД Юрайт, 2016. – 565 с.

44. Зинченко, А. П. Статистика: учебник / А. П. Зинченко. – Москва: КолосС, 2016. – 566 с.

45. Ивченко, Г.И. Математическая статистика / Г.И. Ивченко, Ю.И. Медведев. - М.: [не указано], 2016. - 329 с.

46. Лексин, В. Н. Муниципальная Россия. Социально-экономическая ситуация, право, статистика. Том 3 / В.Н. Лексин, А.Н. Швецов. - Москва: СИНТЕГ, 2017. - 992 с.

47. Ниворожкина, Л. И. Статистика: учебник для бакалавров: учебник /. – Москва: Дашков и К°: Наука–Спектр, 2015. – 415 с.

48. Рейтлингер, Л.Р. Материалы для статистики глазных болезней, господствующих в войсках русской армии / Л.Р. Рейтлингер. - М.: С-Пб.: Богельман, 2017.- 128 с.

49. Романовский, В.И. Избранные труды, том 2. Теория вероятностей, статистика и анализ / В.И., Романовский. - М.: [не указано], 2017. - 145 с.

50. Статистика: учебник / [И. И. Елисеева и др.]. – Москва: Проспект, 2015. – 443 с.

51. Статистика и бухгалтерский учет / [А. П. Зинченко и др.]. – Москва: КолосС, 2018. – 436 с.

52. Статистика: учебно–практическое пособие / [М. Г. Назаров и др.]. – Москва: КноРус, 2018. – 479 с.

53. Статистика: учебное пособие для высших учебных заведений по экономическим специальностям / В. М. Гусаров, Е. И. Кузнецова. – Москва: ЮНИТИ–ДАНА, 2016. – 479 с.

54. Статистика: теория и практика в Excel: учебное / В. С. Лялин, И. Г. Зверева, Н. Г. Никифорова. – Москва: Финансы и статистика: Инфра–М, 2016. – 446,

55. Статистика финансов: учебник / [М. Г. Назаров и др.]. – Москва: Омега–Л, 2018. – 460 с.

56. Тумасян, А. А. Статистика промышленности: учебное пособие / А. А. Тумасян, Л. И. Василевская. – Минск: Новое знание. – Москва: Инфра–М, 2017. – 429 с.

57. Тюрин, Ю.Н. Лекции по математической статистике / Ю.Н. Тюрин. - М.: [не указано], 2017. - 992 с.

58. Харченко, Н. М. Экономическая статистика: учебник / Н. М. Харченко. – Москва: Дашков и К°, 2016. – 365 с.

59. Экономическая статистика: учебник / [А. Р. Алексеев и др.]. – Москва: Инфра–М, 2016. – 666 с.

60. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс – М.; Феникс, 2008. – 174 с.

61. Харкевич А.А. Опознавание образов // Радиотехника. 1959. Т. 14, №5. С. 3-9.

62. Пугачев В.С. Введение в теорию вероятностей. М.: Наука, 1968. 368 с.

63. Електронний ресурс: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/ Режим доступу: вільний.

64. Шматок А.С. Методы анализа критических данных на основе машинного обучения. / А.С. Шматок, Ю.И. Финенко // ОРАЛДЫҢ ҒЫЛЫМ ЖАРШЫСЫ - №3 (130) 3019. - Оралқаласы, ЖШС «Уралнаучкнига», 3019. – С. 58-63.

65. Шматок О.С. Штучний інтелект та машинне навчання в задачах стеганоаналізу даних. / О.С. Шматок, Ю.І. Фіненко, А.Б. Єлізаров, В.А. Телющенко // Вісник Університету «Україна», Серія: «Інформатика, обчислювальна техніка та кібернетика» - №3 (33) 3019. – Київ, Університет «Україна», 3019. С.319-337.

66. Агеев А. С. Автоматизированные системы контроля защищенности объектов электронно-вычислительной техники и перспективы их развития // А. С. Агеев, Вопросы защиты информации. 2015 — №2. – 93 с.

67. Арьков П. А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации: дис…. канд. техн. наук: 05.13.19. — Волгоград, 2009. — 410 с.

68. Барзилович Е.Ю. Модели технического обслуживания сложных систем // Е. Ю. Барзилович, М.: Высшая школа, 2012 — 231 с.

69. Герасименко В. А. Защита информации в автоматизированных системах обработки данных : В 2 кн. — М.: Энергоатомиздат, 2014 – 156 с.

70. Горбатов В.С., Кондратьева Т.А. Информационная безопасность. Основы правовой защиты // В.С. Горбатов, М.: МИФИ, 2015 – 320 с.

71. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов // Ф. М. Курилов, Технические науки: теория и

практика: материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). — Чита: Издательство Молодой ученый, 2016. — 112 с.

72. Нестеров С. А. Анализ и управление рисками в сфере информационной безопасности: Учебный курс. — СПб.: СПбГПУ, 2007. — 47 с. Отчет «Исследование текущих тенденций в области информационной безопасности бизнеса» [Электронный ресурс] // Лаборатория Касперского. — 2017. URL: http://media.kaspersky.com/ (дата обращения: 23.03.2017).

73. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа // А. Ю. Щеглов, СПб: Наука и техника, 2014. — 384 с.

74. Ярочкин В.И. Безопасность информационных систем // В. И. Ярочкин, М.: Ось, 2015 — 320 с.

75. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М: Горячаялиния-Телеком, 2008. 452 с.

76. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. 1985. Vol. SMC-15, no 1. P. 116-132. DOI: 10.1109/TSMC.1985.6313399

77. Хайкин С. Нейронные сети: полный курс: пер. с англ. М.: Издательский дом «Вильямс», 2006. 1104 с.

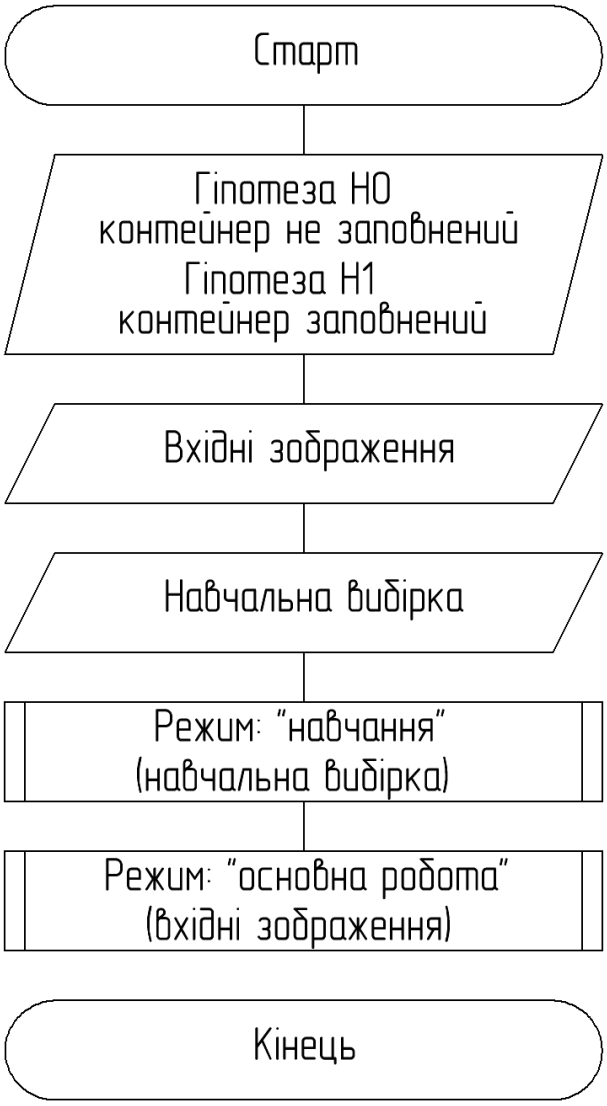
78. Булдакова Т.И. Нейросетевая защита ресурсов автоматизированных систем от несанкционированного доступа // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 5. DOI: 10.7463/0513.0566210

79. Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф., Воскресенский С.И. К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2004. № 4. С. 25-31.

ДОДАТКИ

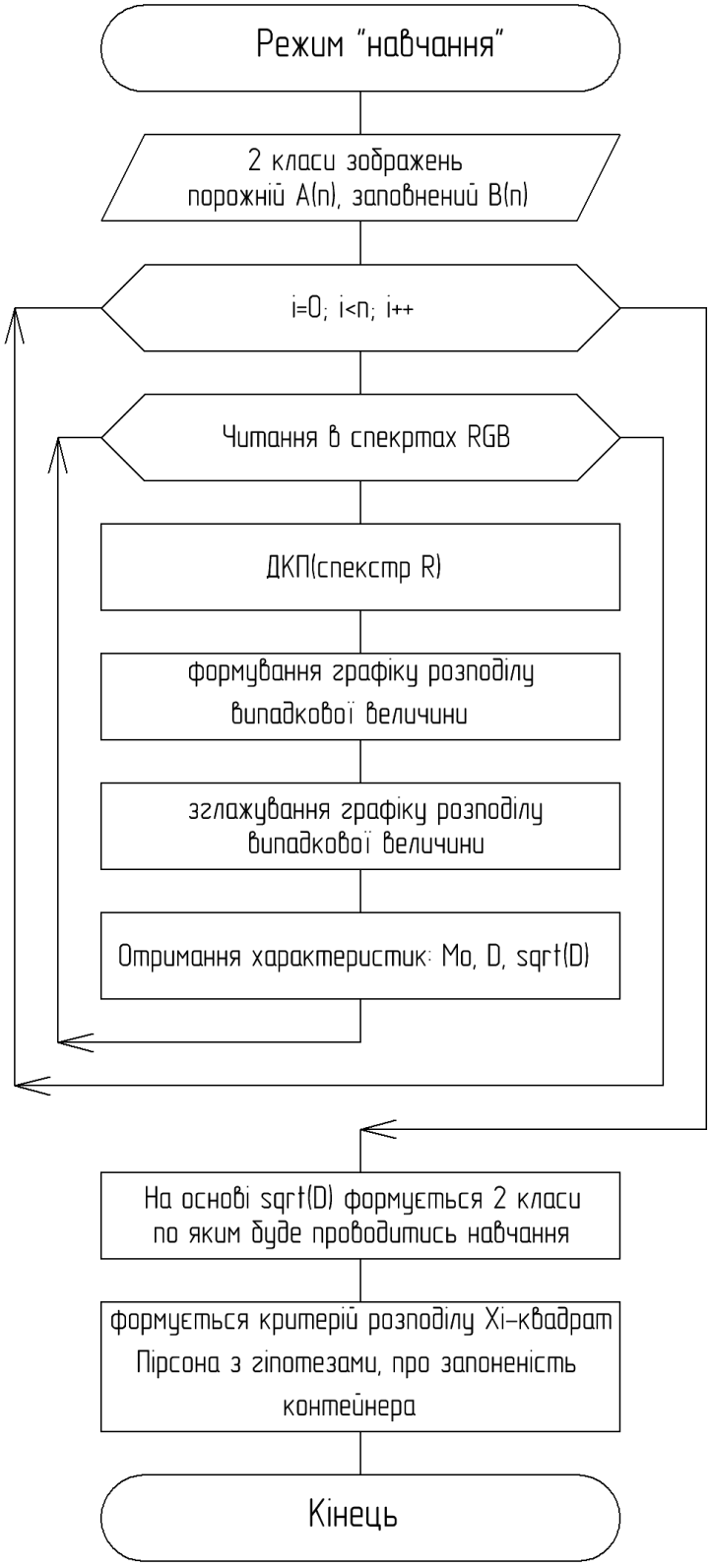
Додаток А

Принцип роботи основного алгоритму



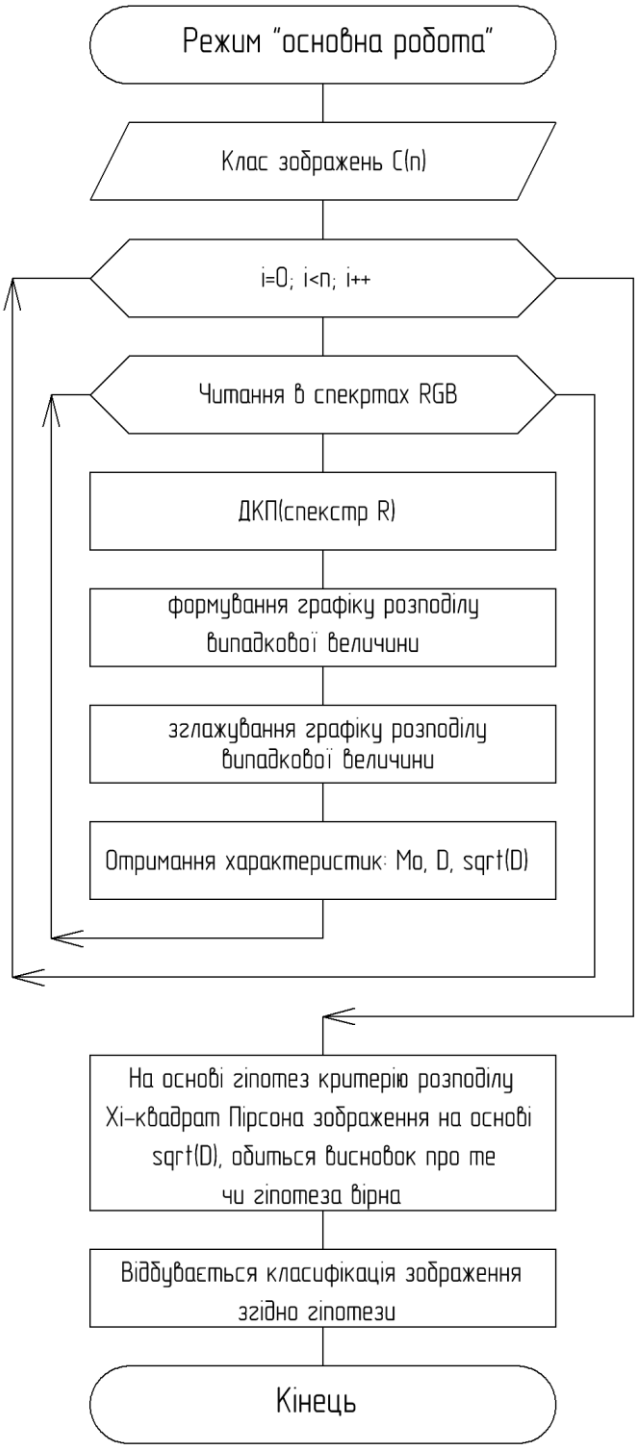
Додаток Б

Принцип роботи підпрограм режиму навчання



Додаток В

Принцип роботи підпрограми «Основна робота»



Додаток Г

Програма оцінки статистичних характеристик контейнерів в середовищі «MATLAB»

```
I = imread('.\Test480\8.bmp');
% figure(1);
% imshow(I);
J = imread('.\TestStego480\8.bmp');
% figure(3);
% imshow(J);
%LAB
iLAB = rgb3lab(I);
jLAB = rgb3lab(J);
L1 = iLAB(:,:,1)/100;
L3 = jLAB(:,:,1)/100;
% %HSV
% iHSV = rgb3hsv(I);
% jHSV = rgb3hsv(J);
% L1 = iHSV(:,:,3);
% L3 = jHSV(:,:,3);
% % figure, imhist(L1);
% % hold on;
% % imhist(L3);
x=0:0.001:1;
hist1 = hist(L1(:),x);
hist3 = hist(L3(:),x);
FltH1 = medfilt1(hist1,14); %Предобработка медианным фильтром
FltH3 = medfilt1(hist3,14); %Предобработка медианным фильтром
SumBrightness1 = sum(FltH1);
for i=1:1:length(FltH1)
   F1(i)=FltH1(i)/SumBrightness1;
end
SumBrightness3 = sum(FltH3);
for i=1:1:length(FltH3)
   F3(i)=FltH3(i)/SumBrightness3;
end
figure(3)
plot(x,F1);
hold on;
plot(x,F3);
xlabel('Pixel Brightness');
ylabel('Probability') ;
[f1,x1]=ecdf(L1(:));
```

```
[f3,x3]=ecdf(L3(:));
figure(4);
plot(f1,x1);
hold on;
plot(f3,x3);
xlabel('x');
ylabel('Ф(x)') ;
figure(5)
h1=histfit(L1(:),1000);
hold on;
h3=histfit(L3(:),1000);
xlabel('Pixel Brightness');
ylabel('Number of pixels') ;
figure(6)
scatter(mean(h1_curve_x),mean(h1_curve_x));
hold on;
scatter(mean(h3_curve_x),mean(h3_curve_x));
title('Mo');
h1_curve_x=get(h1(3),'XData');
h1_curve_y=get(h1(3),'YData');
h3_curve_x=get(h3(3),'XData');
h3_curve_y=get(h3(3),'YData');
disp('Математическое оживание');
disp('Пустого контейнера');
disp(mean(h1_curve_x));
disp('Заполненного контейнера');
disp(mean(h3_curve_x));
disp('Дисперсия');
disp('Пустого контейнера');
disp(var(h1_curve_x));
disp('Заполненного контейнера');
disp(var(h3_curve_x));
disp('Среднеквадратическое отклонение');
disp('Пустого контейнера');
disp(std(h1_curve_x));
disp('Заполненного контейнера');
disp(std(h3_curve_x));
```