МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет

Факультет комп’ютерних інформаційних технологій

Кафедра кібербезпеки

КЛЬОЦ Юрій Павлович

Метод визначення підозрілої поведінки комп’ютерів корпоративної мережі / A method for determining suspicious behavior of corporate network computers

спеціальність 125 Кібербезпека

освітньо-професійна програма - Кібербезпека

кваліфікаційна робота

Виконав студент групи КБм-21

Ю.П. Кльоц

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Науковий керівник:

к.т.н., доцент І.З.Якименко

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Яцків

підпис

Тернопіль – 2021

ВСТУП

Сучасне життя складно уявити без інформаційної взаємодії, що стосується як окремих членів суспільства, і великі організації, зокрема реалізують інтереси цілого держави. Крім очевидних переваг, що отримуються, така взаємодія несе також низку істотних недоліків [1]. Так, передача інформації через мережу піддає її тріаді загроз інформаційній безпеці: конфіденційності, цілісності та доступності. При цьому безпека інформації має бути забезпечена як за її передачі через відкриті мережі, і усередині комп'ютерної мережі (КС), під якою насамперед розуміється корпоративна комп'ютерна мережа. Однак до інформації в КС, що особливо носить критично важливе значення можуть мати доступ внутрішні співробітники, частина з яких спочатку має такі повноваження, що входять до кола їх посадових. обов'язків. Таким чином, виникає проблема протидії атакам на КС, як випадковим, так і зловмисним, виробленим у тому числі внутрішніми працівниками організації.

Існують різні способи протидії інсайдерській діяльності на різних етапах – до самої атаки, під час її проведення та після атаки. Кожен із способів має свої переваги та недоліки, проте важливим є той факт, що інформація може застаріти та її цінність, відповідно, зменшуватись. Отже, надання пізньої протидії інсайдерським атакам може виявитися безглуздим, оскільки інформація до цього часу вже буде скомпрометована та використана третіми особами. Так, у разі порушення цілісності даних або надання неправомірного доступу до даних факт виявлення одного з подібних порушень матиме для організації істотно менший ефект, ніж недопущення інсайдерської атаки загалом. Отже, затребуваним є саме недопущення інсайдерської атаки, що може бути досягнуто шляхом виявлення інсайдерів до моменту проведення самої атаки. Після виявлення інсайдерів, звичайно, передбачається їхня нейтралізація. Нейтралізація інсайдерів може проводитися або автоматично – програмними засобами, або вручну – експертами з інформаційної безпеки [2].

Згідно з останніми дослідженнями [3], весь IP-трафік та число пристроїв, підключених до Інтернету, потрояться за наступні 5 років. Вважається, що це відбудеться внаслідок розвитку сервісів та послуг, що надаються телекомунікаційними компаніями. При цьому особливу популярність набирають: хмарні послуги у вигляді Platform-as-a-Service (PaaS) та Software-as-a-Service (SaaS); рішення для зберігання даних; аналітичні системи; рішення для ведення бізнесу та прогнозування ризиків; рекомендаційні системи. Розширення сфер застосування мережевих технологій означає децентралізацію мережевий інфраструктури загалом як у плані зберігання даних, і у плані одержуваного доступу до цієї інфраструктури [6]. Це ускладнює вирішення інженерних завдань, стоять перед фахівцями інформаційної безпеки, оскільки стає важче контролювати всі аспекти мережевої безпеки під час захисту критично важливих даних від загроз, що виходять як із зовнішньої мережі, так і зсередини, від учасників мережі [7, 8].

Таким чином, основна складність виявлення інсайдерів у КС безпосередньо випливає із сучасних тенденцій розвитку інформаційних технологій, нерозривно пов'язаних із постійним збільшенням параметрів мережного трафіку: його обсяг; швидкості генерації; кількості джерел та отримувачів трафіку; кількості логічних потоків, не пов'язаних зі своїмицілями та завданнями; збільшення рівня гетерогенності даних та ін [9].

Все це призводить до суттєвого ускладнення аналізаторів трафіку, оскільки далеко не всі існуючі системи здатні справлятися з такими великими обсягами та складністю, у той час як інсайдери приховують свої дії у загальному потоці дій законних користувачів. Крім того, сучасні інсайдерські атаки є комплексними та використовують безліч способів реалізації та безліч векторів для отримання несанкціонованого доступу та компрометації інформаційних об'єктів у внутрішньої КС [10].

Таким чином, основне протиріччя предметної області полягає в наступному: з одного боку, необхідно підвищення точності виявлення інсайдерів, оскільки їх атаки постійно ускладнюються та комплексуються, мережевий трафік атак стає менш помітним через зростання обсягу всього трафіку у КС, а самі інсайдери маскують свої дії під законні; з іншого боку, існуючі моделі, методики та алгоритми виявлення інсайдерів не володіють необхідною ефективністю роботи, оскільки або мають високий ризик пропуску інсайдера (помилка ІІ роду), або, навпаки, – ризик віднесення до інсайдеру законного користувача (помилка І роду). Можливою причиною породження даної суперечності є деякою суб'єктивністю, властивою всім критеріям інсайдерської діяльності, що вводяться. Так, наприклад, частина користувачів, визначених як інсайдери, могли просто виконувати низку помилкових дій: невірно ввести свій пароль, помилково завантажити документ або надіслати документ на неправильну адресу, підключити чужий пристрій тощо.

Вирішення зазначеного протиріччя може лежати у площині застосування високоефективних спеціалізованих технологій обробки мережевого трафіку для сфери інформаційної безпеки, а також у поєднанні існуючих та нових способів аналізу та виявлення інсайдерської діяльності. Все це може бути досягнуто в такий спосіб.

По-перше, тенденція зростання популярності появи рішень для роботи з великими даними дозволяє припустити гіпотетичну потрібність даної технології для вирішення виявленої вище основної суперечності предметної галузі. Так, з появою інструментів для розробки систем, використовують концепцію великих даних [11-13], постає питання про використання обробки великих даних для інформаційної безпеки та, зокрема, систем моніторингу безпеки. Стає все складніше виявляти потенційні загрози безпеці. Пропускна здатність сучасних систем моніторингу та попередження мережевих атак перестає задовольняти вимогам мереж, що постійно розростаються: у зв'язку з великою кількістю трафіку, що надходить, і низькою швидкістю його обробки результати такого аналізу виходять неактуальними та не відображають реального стану мережі [14]. Використовуючи нові та ефективні технології для агрегації та зберігання великих обсягів даних, а також для організації роботи системи виявлення зловмисника, можна досягти потрібних результатів, а саме отримати достатній рівень контролю за ситуацією в КС.

Також важливо враховувати, що не всі моделі представлення даних у достатньо адаптовані до своєчасної обробки великих обсягів інформації та подій. Специфіка завдань кібербезпеки полягає в необхідності застосування нових моделей баз даних та використання методів Обробка великих даних для аналізу трафіку комп'ютерних мереж.

По-друге, існуючим підходом, що добре зарекомендував себе виявлення інсайдерів (враховуючи складність строгої формалізації критеріїв виявлення останніх та їх можливості до приховування своїх дій) використання алгоритмів на основі правил, складених експертами з урахуванням власного накопиченого досвіду та існуючих «best practices» (експертних правил).

І, по-третє, облік комплексності атак, що проводяться інсайдерами, а також їх розподіленості: по мережі (наприклад, атака на цілий ряд не пов'язаних хостів), по об'єктам (наприклад, спроба доступу до частин документа з метою збору спільної критичної маси конфіденційної інформації), за часом (наприклад, послідовність подій, пов'язаних тривалим проміжком часу), – дає можливість припустити затребуваність застосування методів машинного навчання, що дозволяють враховувати безліч, на перший погляд, важко пов'язаних один з одним параметрів [15].

Все вищесказане передбачає застосування виявлення інсайдерів у КС підходу, заснованого на використанні експертних правил, методів машинного навчання та обробки великих даних. Цим обумовлюється актуальність теми дослідження.

1. СИСТЕМНИЙ АНАЛІЗ ЗАВДАННЯ ВИЯВЛЕННЯ ІНСАЙДЕРІВ У КОМП’ЮТЕРНИХ СИСТЕМАХ

1.1. Місце та роль завдання виявлення інсайдерів у комп’ютерних системах

В даний час вирішення проблеми виявлення інсайдерських атак приділяється багато уваги. Доказом цього можуть бути інсайдерські атаки, здійснені протягом 2019 року.

Компанія DeviceLock, що є виробником DLP-систем, провела дослідження каналів інсайдерських витоків інформації в компаніях. В рамках дослідження, що охопило період із січня по травень 2019 року, було проаналізовано понад 800 документів, викладені на різні ресурси проекту DarkNet, а також надані продавцями послуги як зразки запропонованих ними даних.

Іншим підтвердженням зростання інсайдерських атак може бути щорічний звіт Data Breach Investigations Report (DBIR) від компанії Verizon, що надає глибокий аналіз останніх тенденцій та змін, пов'язаних з інцидентами кібербезпеки. Провівши глибокий аналіз звіту, можна зробити висновок про те, що останні 4 роки кількість інцидентів, пов'язаних з інсайдерськими загрозами, зростає на 5%, починаючи з низького показника у 2015. Звіт за 2019 рік показав, що 34% усіх порушень сталося внаслідок інсайдерських атак.

Компанія Cisco Systems Inc. недавно вивчила тенденції витоку даних [16], застосувавши алгоритм з урахуванням методів машинного навчання, щоб скласти профілі 150 000 користувачів у 34 країнах, що користуються послугами постачальників хмарних сервісів, з січня до червня 2019 року. Цей алгоритм враховував не тільки обсяг документів, що завантажуються, а й різні змінні дані, наприклад, час завантаження протягом дня, IP-адреси та розташування. Профілі користувачів складалися протягом півроку, потім дослідники півтора місяці вивчали аномалії, – 0,5% користувачів було відзначено як що здійснюють підозрілі дії зі скачування програм. З-поміж цих підозрілих завантажень 62% припадало на стандартний робочий годинник, 40% відбувалося у вихідні [16].

Проаналізувавши звіт аналітичного центру компанії InfoWatch можна зазначити, що за 2019 рік було зареєстровано 1039 випадків витоку конфіденційної інформації, що на 12% більше, ніж роком раніше. Слід зазначити, що обсяг інформації, скомпрометованої з вини хакерських та інших атак під впливом зовнішнього порушника, зменшився вдесятеро, склавши лише близько 0,5 млрд. записів. При цьому внаслідок порушень усередині організацій постраждали понад 1,5 млрд. записів даних, включаючи персональні та платіжні.

Таблиця 1.1 Загальна таблиця порушників

|  |  |  |  |
| --- | --- | --- | --- |
| **Потенціал порушника** | | **Кількість**  **загроз** | **Частка загроз** |
| Внутрішній порушник | з низьким  потенціалом | 91 | 42% |
| із середнім потенціалом | 52 | 24% |
| з високим  потенціалом | 3 | 1% |
| **Усього** | **146** | **68%** |
| Зовнішній порушник | | 216 | 32% |

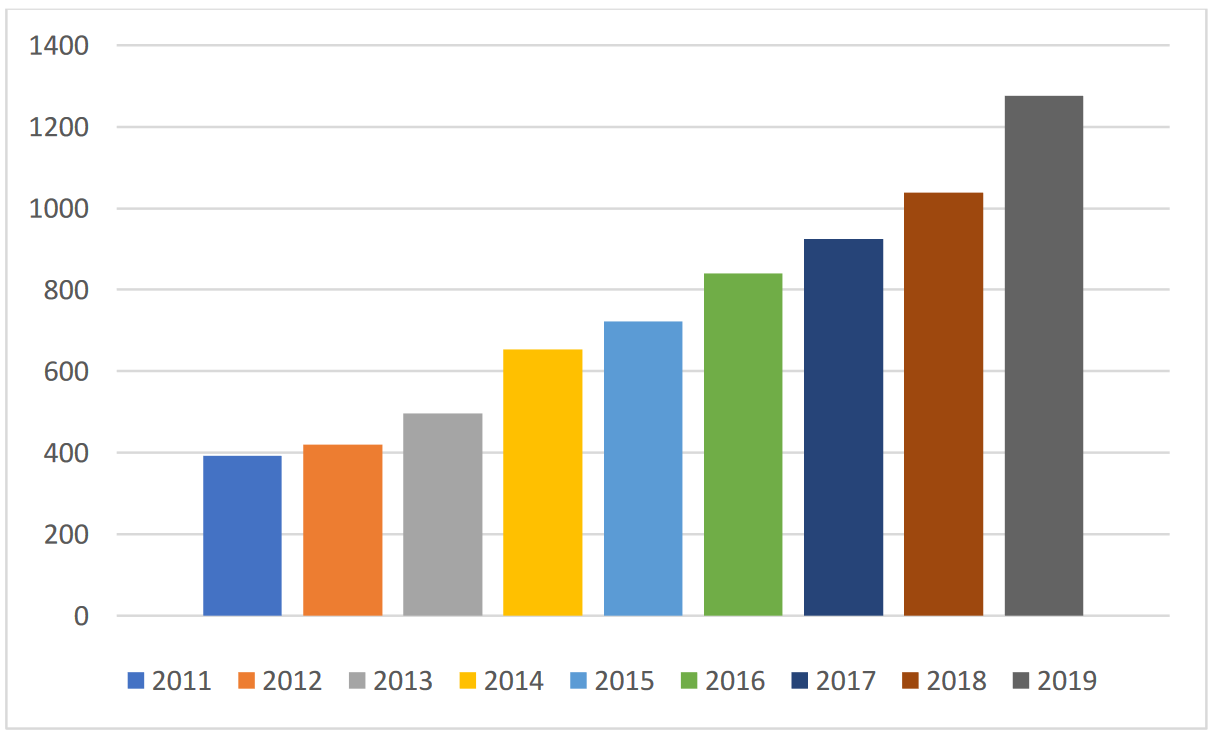


Рисунок 1.1 – Загальна кількість атак інсайдерів

**Таксономії інсайдерів та інсайдерських загроз.** В даний час одним з найбільш широко застосовуваних підходів для складання таксономії інсайдерів є опитувальний метод. В основі цього методу лежить аналіз матеріалів розслідувань інцидентів комп'ютерної безпеки, які проводили фахівці з комп'ютерної безпеки. На основі розслідуваних інцидентів можливо здійснити категоризацію досліджень та використовувати як технічні, так і психосоціальні дані.

Розглянемо список опитувань, пов'язаних із внутрішніми загрозами. Salem [17, 18] ввів таксономію зловмисників, розділивши їх на дві категорії відповідно до наявних у них знань про цільову систему: зрадники та маскарадники. Провівши аналіз літератури з виявлення інсайдерів, можна розділити роботи на три типи на вигляд підходів: «підходи профілювання користувачів на основі хоста», «підходи мережного рівня» та «інтегровані підходи». Мережевий рівень та хост на основі профілювання може мати високу ймовірність виявлення зрадників, у той час як профіль користувачів на основі хоста може бути успішним при виявленні прихованих загроз. Автори стверджують, що зловмисні дії інсайдерів відбуваються на рівні додатків та бізнес-процесів. Hunker і Probst [19] запропонували категоризацію дослідження, засновану на комбінації психосоціальних вихідних даних із технічними даними. Результати категорії складаються з трьох типів підходів до виявлення загроз з боку інсайдерів: 1) «соціологічний, психологічний, організаційний», 2) «соціально- технічний» та 3) «технічний». Автори наголосили, що для успішних методів виявлення внутрішніх загроз потрібне поєднання різних підходів. Технічні можливості атакуючого значно зростають у тому випадку, якщо користувач пристрою, що знаходиться всередині периметра, усвідомлено сприяє аутсайдеру, діючи відповідно до нього. Однак, можлива ситуація, коли на пристрої співробітника без його відома та згоди встановлено програмні засоби віддаленого управління та спеціалізоване ПЗ для збору інформації та виконання атаки на КС. Співробітник, перебуваючи всередині периметра, фактично надає технічну платформу для атаки, часто неусвідомлено. Відповідно, технічні можливості аутсайдера в цьому випадку будуть визначатися можливостями прихованого ПЗ. При цьому атакуючий також обмежений у знаннях та можливостях підключення до КС, а значить, накопичення потрібної інформації буде відбуватися менш ефективно. Використання BYOD може викликати і ненавмисне поширення всередині периметра шкідливого програмного забезпечення з принесеного пристрою внаслідок його недостатньої захищеності та недосвідченості користувача.

На думку Неймана [20], аутсайдерами вважаються зловмисники, які успішно проникли в ІС або мережу та не отримали достатньо знань, щоб зробити їх невідмінними від інсайдерів, якими вони маскуються. Для проведення диференціації аутсайдерів та інсайдерів автор розглядає тест Тюрінга. Більш того, інсайдерська загроза також була визначена як частина ширших тем, які виникали протягом всієї історії комп'ютерних систем, таких як спроби вторгнення, загрози безпеці та контрпродуктивна поведінка на робочому місці. В даний час найбільш актуальні масштаби внутрішньої загрози підтримуються підрозділом CERT Інституту програмної інженерії Університету Карнегі-Меллона та засновані на базі даних більш ніж 1000 реальних прикладів із практики.

Pfleeger [21] визначає інсайдера як "обличчя, що має законний доступ до комп'ютерів та мереж організації". Звіт RAND Corp. [22] визначає інсайдера як "заздалегідь довірена особа, яка має доступ до конфіденційної інформації та інформаційних систем" (ІС).

Термін "ненавмисна внутрішня загроза" згідно з [22] визначається як "поточний або колишній співробітник, підрядник або інший діловий партнер», який: 1) "має або мав санкціонований доступ до мережі, системи або даним організації" і 2) "не мав злого наміру, пов'язаного з його діями (або бездіяльністю), що завдали шкоди або істотно збільшили ймовірність серйозної шкоди конфіденційності, цілісності або доступності інформації або ІБ організації в майбутньому". У [25] вважають, що ненавмисна внутрішня загроза визначається як "неуважні, самозадоволені або ненавчені люди, яким для виконання своєї роботи потрібен дозвіл та доступ до ІС".

Таксономія інсайдерів може бути побудована на основі аналізу мотивації. Розглядаючи мотивацію, Wall в [23] стверджує, що ненавмисні внутрішні загрози діляться згідно з попередніми дослідженнями на благонамірні та недбалі. Далі автор пропонує в якості основи для структурної оцінки типологію чотирьох типів співробітників, які можуть призвести до витоку даних: порушники (ті, які роблять своє життя простіше, не дотримуючись політики безпеки), надмірно амбітні (ті, які спеціально оминають заходи безпеки, щоб бути більш ефективними), соціальні інженери та особи, які займаються крадіжкою даних. Автор описує різні способи витоку даних, такі як випадковий витік (втрата USB-накопичувачів); для зручності користувачів (копіювання даних на домашні комп'ютери); інші (наявність даних на жорстких дисках, пошкоджених ПК,

**Таксономія людських помилок.** Як зазначалося раніше, проблема інсайдерських інцидентів перестав бути суто технічною, а виходить із взаємодії людини з технічною системою. При цьому, крім явних намірів здійснити певні дії, користувачі всередині периметра можуть робити помилки. Reason [24] визначає людську помилку як "недосягнення бажаного результату в запланованій послідовності психічних або фізичних дій, коли невдача не викликана випадковістю". Автор пропонує загальну систему моделювання помилок (GEMS). GEMS ділить помилки на наступні групи: "прослизання", які являють собою неправильне виконання правильної послідовності дій (збій виконання), та "помилки", які є правильним виконанням неправильної послідовності дій (збій планування).

**Типи внутрішніх атак.** Bellovin [26] виділяє три види внутрішніх атак:

* + 1. Зловмисне використання доступу, яке, на думку автора, найбільше важко виявити, оскільки інсайдери використовують законний доступ, але не за призначенням.
    2. Обхід захисту, коли інсайдери вже пройшли деякі лінії захисту (наприклад, брандмауери), можуть також обійти інші.
    3. Створення технічних проблем, коли елемент контролю доступу має неправильні налаштування, або такий елемент присутній у доступі. Передумови для таких атак можуть створювати адміністратори КС, що недбало ставляться до питань призначення доступу та зберігання облікової інформації.

**Рівні внутрішніх загроз.** На основі різних потенційних наслідків та шкоди для організації, Cole і Ring [27] розрізняють три рівні внутрішніх загроз:

Рівень 1: Інсайдери з власною мотивацією не мотивовані жодними третіми особами, але діють самостійно з особистих причин.

Рівень 2: Завербовані інсайдери – це особи, які діють на шкоду та мотивовані третьою стороною. Оскільки такий тип завербованого інсайдера є ризиком як для інсайдера, так і для вербувальника, очевидно, що кращим способом для зловмисників є використання власного підготовленого інсайдера.

Рівень 3: Шкідливі організації, які цілеспрямовано розміщують інсайдерів у компанії-жертві. Знаходячи відповідного роль інсайдера співробітника, організації навчають його, влаштовують працювати у компанію, та був починають використовувати інсайдерів скоєння зловмисних дій.

**Типи мотивів інсайдерів.** На думку Cole і Ring [27] існує безліч факторів, які можуть сприяти мотивації інсайдерів. Найбільш популярні три основні мотивації: 1) фінансові труднощі чи бажання додаткового заробітку; 2) політичні – деякі співробітники з політичними переконаннями можуть бути налаштовані дуже радикально та мотивовані заподіяти шкоди у разі будь-якої можливості; 3) індивідуальні.

**Профільування інсайдерів CERT.** Cappelli [28] пропонують розділити шкідливі внутрішні загрози на три типи:

1. Саботаж у сфері ІТ, при якому "інсайдер використовує ІТ для завдання конкретної шкоди організації або окремій особі". Такими інсайдерами зазвичай є незадоволені технічно підготовлені співробітники, які мають адміністративні привілеї.
2. Крадіжка інтелектуальної власності. Зазвичай йдеться про шпигунство, яке здійснюється як технічним персоналом, а також не технічним персоналом. Винні можуть красти інформацію, до якої вони щодня мають доступ, і забирати її із собою, коли залишають організацію.
3. Шахрайство, при якому "інсайдер використовує ІТ для несанкціонованої модифікації даних організації з метою особистої вигоди або розкрадання". Зазвичай відбувається співробітниками нижчої ланки з не технічною освітою, мотивом яких є жадібність або фінансові труднощі, шахрайство відбувається протягом тривалого періоду.

**Таксономія інсайдерської загрози з урахуванням політик.** Таксономія внутрішньої загрози на основі політик може бути виведена з визначень та відповідної моделі внутрішньої загрози, запропонованих Bishop at al. [29]. Автори стверджують, що "політика безпеки є правилами контролю доступу, що застосовуються в організації". Виходячи з цього визначення, інсайдерську загрозу можна класифікувати з урахуванням двох примітивних дій: 1) "порушення політики безпеки з використанням законного доступу", що включає дії, що не відповідають чинній безпеці; та 2) "порушення політики контролю доступу шляхом отримання несанкціонованого доступу" – інсайдери зловживають своїм законним доступом з метою розширення своїх фактичних привілеїв, порушуючи чинну безпекову політику.

**Категоризація внутрішніх зловмисників із фізичної присутності.** Розглядаючи фізичну присутність, Neumann [36] поділяє інсайдерів на дві категорії: логічну та фізичну. Логічний інсайдер здійснює свої дії фізично поза робочого простору організації, а фізичний інсайдер діє у межах фізичних кордонів робочого простору організації, зокрема зовнішніх довірених мереж [34]. Ця класифікація не визначає наміри інсайдерів, і може застосовуватися як до ненавмисних, так і до зловмисних внутрішніх загроз.

**Людино-орієнтована таксономія внутрішніх зловмисників.** Magklaras і Furnell [29] пропонують орієнтовану на людину таксономію внутрішніх зловмисників, що враховує три виміри: роль інсайдерів у системі, причини неправильного використання та наслідки для системи.

1. Системна роль – перший вимір класифікує людей за "типом і рівнем системних знань, якими вони володіють". Цей аспект складається з: системних адміністраторів, які повністю контролюють більшу частину ресурсів ІС; просунутих користувачів, які не мають привілейованого доступу, але мають великий обсяг знань про системи та мережі організації, та здатні виявити вразливості системи [8]; та користувачів програм, які використовують певні стандартні програми, але мають більше прав доступу, ніж зазвичай.
2. Причина неправомірного використання – цей аспект визначає ознаки інцидентів, пов'язаних з інсайдерською загрозою. Враховуючи цей аспект, автори поділяють інсайдерів на дві групи: навмисні неправомірні дії з різних причин та випадкові зловживання, які також можуть бути класифіковані з фактичної причини, яка негативно вплинула на поведінку законного користувача.
3. Системні наслідки – цей аспект розрізняє різні методи скоєння неправомірних процесів, що виявляється у наявності певних слідів в ІТ-інфраструктурі на системному рівні.

Автори описують три рівня, які приписуються цим наслідків:

1. ОС – зміни у структурі файлової системи, встановлення несанкціонованого програмного забезпечення тощо; 2) мережні – мережні пакети можуть містити несанкціонований вміст, ексфільтрацію конфіденційних даних через служби обміну електронною поштою або файлами тощо; 3) апаратне – вандалізм чи видалення апаратних компонентів, встановлення реєстраторів, зміна конфігурації критичних апаратних компонентів (наприклад, з метою саботажу чи крадіжки IP).

**Виявлення внутрішніх атак.** Phyo and Furnell [30] пропонують класифікацію внутрішніх атак, яка розрізняє чотири рівні моніторингу системи-мішені, на яких можна виявити атаку:

* 1. мережа;
  2. операційна система;
  3. додаток;
  4. дані.

Ця таксономія заснована на припущенні, що одна внутрішня атака може виявлятися на певних рівнях системи, а сліди іншої внутрішньої атаки можуть бути присутніми на різних рівнях (наприклад, порушення цілісності даних може бути очевидним на рівні додатків та даних, а витік даних може виявлятися на рівні мережі та ОС).

1.2 Аналіз методик та алгоритмів виявлення інсайдерів у комп'ютерних системах

Розглянемо перелік аналогічних робіт у галузі інформаційної безпеки для виявлення або класифікації інсайдерів [31-33].

**SIEM системи та системи виявлення атак та протидії атакам.**​​ У [38] описується рішення, яке збирає зовнішню інформацію про шкідливі IP-адреси, занесені в публічні чорні списки, і внутрішню інформацію організації про інциденти безпеки для розрахунку показників репутації для зовнішніх IP-адрес та публічних чорних списків IP-адрес. Оцінка репутації використовується правилами SIEM для вибору типу оповіщення кожної IP-адреси, що підлягає моніторингу. Подане рішення спрямоване на розширення охоплення SIEM діяльності щодо боротьби з кіберзлочинністю в мережі організації.

Як видається, немає рішення, здатного повністю усунути внутрішню загрозу всередині організації. Крім того, технічний підхід сам по собі може виявитися не найефективнішим способом запобігання та/або виявлення шкідливих внутрішніх загроз. Одним із перспективних підходів до підвищення ефективності та результативності SIEM-систем є використання методів машинного навчання.

**Machine Learning алгоритми.** Алгоритмам машинного навчання (Machine Learning Algorithms) присвячено досить велику кількість досліджень. У роботі [39] пропонується використовувати спеціальний фреймворк визначення аномалій в комп'ютерної мережі. Як вхідні дані багатовимірні вхідні дані, такі як логи взаємодії користувачів з апаратними засобами, записи веб-доступу та електронні листи. Для виявлення взаємозв'язків між багатовимірними об'єктами використовуються графи. Взаємодія користувача з пристроями ілюструється зваженим неорієнтованим двомірним двостороннім графом G = (V; E; W), де V – безліч вершин (користувачі), E

* безліч ребер, а W - вага ребер. Набір вершин складається з двох типів об'єктів
* користувачів та пристроїв, у той час як ребра представляють взаємодію користувача з пристроєм.

Схема роботи фреймворку представлена ​​рис. 1.2. Фреймворк і двох основних компонентів: «Блок графічної обробки (GPU – Graphical Processing Unit) і «Блок виявлення аномалій» (ADU – Anomaly Detection Unit). Дані, отримані від різноманітних джерел комп'ютерної мережі, форматуються та подаються до графічного процесора, який генерує граф, що представляє взаємозв'язки між вузлами мережі. Ці вхідні потоки можуть бути з різних інформаційних джерел із різними форматами даних. Наприклад, дані можуть бути з журналів подій (вхід / вихід із системи), журналів електронної пошти, записів HTTP, даних доступу до соціальної мережі та різних записів персоналу, таких як психометричні дані. За підсумками цієї інформації кожного користувача розраховуються параметри графа. Оскільки кінцевою метою є ізоляція найбільш аномальних користувачів від інших користувачів, всі атрибути розраховуються індивідуально кожного користувача. Ще одним завданням GPU є генерація породжених підграф кожного користувача для різних рівнів підграфів. Деякі властивості, такі як число вершин, число ребер, щільність, діаметр і кількість бенкетів (Peers), розраховуються кожного рівня подграфов. Розраховані параметри графа та подграфа подаються до ADU. Паралельно з вищевказаним процесом дані також подаються в ADU. Алгоритм ізолюючого лісу (Isolation Forest) виконується для виявлення аномальних користувачів у блоці ADU, а як вихідні дані ADU виступає оцінка аномальності кожного користувача. Ці значення застосовуються виявлення і відділення потенційних зловмисних користувачів з інших працівників.

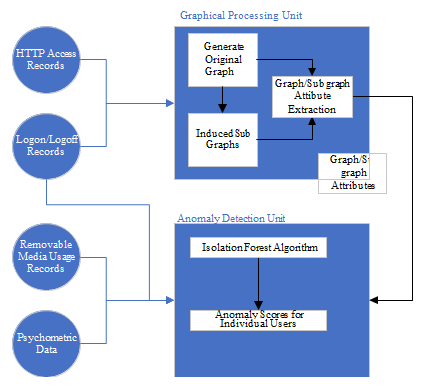


Рисунок 1. 2 – Схема роботи фреймворку виявлення аномалій

В якості набору даних (data set) був використаний набір, опублікований комп'ютерною групою реагування на надзвичайні ситуації університету Карнегі-Меллона, - файл "R4.2.tar.bz". Цей набір даних містить інформацію про ім'я користувача, ім'я комп'ютера, URL запити з тимчасовими мітками сесій HTTP, дані про вход в систему, використовувані пристрої, список змінених файлів від 1000 співробітників за більш ніж 17-місячний період часу.

Як основний алгоритм виявлення аномалій обраний алгоритм Isolation Forest. Принцип роботи алгоритму Isolation Forest полягає в наступному: проводиться випадкове розбиття простору ознак - таке, що в середньому ізольовані точки відсікаються від нормальних, кластеризованих даних. Остаточний результат усереднюється за кількома запусками алгоритму.

**UBA/UEBA системи.** Системи класу UBA та UEBA з'явилися відносно недавно і допомагають у забезпеченні безпеки як внутрішньої, пов'язаної з поведінкою співробітників, так і зовнішньої, наприклад, сприяють запобіганню атаки за допомогою компрометації облікового запису законного користувача. Сама абревіатура UEBA прозвучала вперше у звіті компанії Gartner у середині 2016 року [32]. Саме в цих звітах компанія радить використовувати аналіз поведінки для виявлення аномалій та запобігання загрозам.

UEBA/UBA-системи є наступним поколінням систем, які дозволяють виявляти невідомі типи загроз, внутрішніх порушників та цільові атаки. Спираючись лише на поведінковий аналіз, ці системи здатні визначати аномалії та неочевидні взаємодії користувачів із КС, а це, у свою чергу, надає адміністраторам можливість своєчасно реагувати на потенційні загрози.

В даний момент на ринку існує велика кількість різних UBA-і UEBA-систем, установка яких можлива як окремих модулів з двосторонньою інтеграцією з базою даних управління конфігурацією. Варто враховувати, що для зберігання та застосування змін у режимі близькому до реального часу знадобляться великі потужності, оскільки система активно використовує розподілені високонавантажені платформи зберігання даних [30, 34]. Перед інтеграцією системи має виконуватися профіль поведінки мережевої інфраструктури. Залежно від її розміру час інтеграції може досягати декількох тижнів.

Системи класу UBA/UEBA – важливий елемент виявлення загроз, цільових атак, а також співробітників, що порушують внутрішні правила інформаційної безпеки всередині компанії [35]. UBA/UEBA системи націлені на вирішення наступних основних завдань:

* + проста та розширена аналітика в режимі реального часу;
  + оперативне виявлення аномалій у мережі;
  + визначення значущості події;
  + реакція у відповідь на події, за рахунок того, що адміністратори мають комплексну інформацію про інцидент.

UBA/UEBA-системи стають особливо популярними в наш час і їх інтеграція в SIEM, DLP та інші системи різних виробників доводить цей факт.

Слід також виділити ряд завдань із інтегрованого використання UBA та UEBA-систем з іншими механізмами захисту, наприклад, їх інтеграцію з серверами аутентифікації, які у разі визначення інсайдерів негайно закривають їм доступ [15].

У статті [36] запропоновано підхід, що ґрунтується на динамічному моделюванні. Цей підхід використовує так звану модель інтеграції інформації, схематично представлену на рис. 1.3.

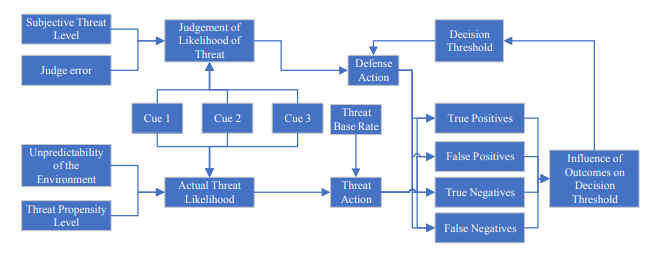


Рисунок 1.3 – Модель інтеграції інформації

У моделі потік транзакцій входить до організації, та інформаційні працівники обробляють ці транзакції. Угоди, які здійснює фірма, є або «хорошими» (відсутня шкідлива дія), або

"поганими" (що вказує на можливу наявність шахрайства чи помилки). Не існує абсолютного тесту на невідповідність, де «позитивний» результат завжди вказує на шахрайство, а «негативний» результат завжди правильно вказує на відсутність шахрайства. Одним із завдань, які вирішують працівники, є завдання винесення суджень про підозрілі транзакції. Працівники повинні використовувати свої знання, щоб вирішити, чи слід розслідувати транзакції. Вони виносять судження про транзакції, інтегруючи інформацію, що надходить з різних повідомлень, присутніх у потоці транзакцій (див. рис. 1.3, Cue 1, Cue 2 і Cue 3), враховуючи складність транзакцій, кількість повернень, пов'язаних з транзакцією, та обсяг. В результаті судження про ймовірність загроз порівнюються з порогами прийняття рішень, унаслідок чого захисні заходи або вживаються, або ні. Отримані рішення, своєю чергою, стають переконаннями, які у поєднанні з організаційними стимулами впливають значення цих порогів прийняття рішень.

**Rule-based архітектури.** [27] розглядаються різні підходи до постійної оцінки (РЄ) для виявлення внутрішніх загроз, які доступні уряду США, і оцінюється актуальність цих підходів для ситуацій, створюваних такими внутрішніми загрозами. У звіті CE визначається процес перевірки та винесення рішення, що дозволяє на постійній основі перевіряти особу, яка була визначена як така, що має право на доступ до секретної інформації або зайняття посади.

У [36] представлений метод виявлення аномальної поведінки шляхом профілювання користувачів. Автори використовують алгоритми оцінки k-середніх та щільності ядра, щоб вивчити нормальну поведінку користувача та встановити нормальні профілі користувачів на основі поведінкових даних. Потім вони порівнюють поведінку користувача із звичайними профілями, щоб виявити ненормальні моделі поведінки.

**Рішення, що базуються на обробці великих даних.** У пошуках кращого загального класифікатора, [39] емпірично оцінюють 88 алгоритмів машинного навчання в 16 основних сімействах. Вони отримують функції ризику з набору даних CERT, який поєднує реальну поведінку мережі з окремими описами загроз, а також виявляють прогностичну важливість вимірювання настрою працівників. Серед основних сімей класифікаторів, протестованих на CERT, найкращий вибір пропонують алгоритми випадкових лісів, які дають точність понад

Схема роботи GAMUT представлена ​​рис. 1.4, у якому зображено узагальнений алгоритм обробки даних у системі. Дані (Requirements) збираються до множини (Data Set) і стають вхідним елементом генератора даних, потім вони надходять в обробник з перетворенням і піддаються валідації в модулі оцінки (Scoring Module), видаючи, нарешті, підсумковий звіт (Test Report).

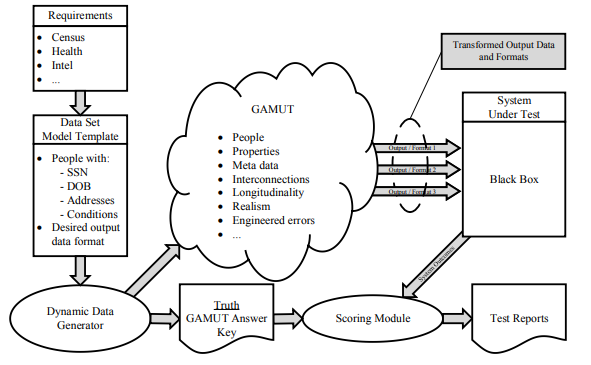


Рисунок 1.14 – Схема роботи системи GAMUT

Для вихідного набору даних автори використовують набір даних, опублікований комп'ютерною групою реагування на надзвичайні ситуації Карнегі-Меллона.

Як основний алгоритм використовується алгоритм, що генерує великі набори випадкових даних, що містять синтетичні дані про користувачів, їх параметри, відомості про з'єднання та запити, серед яких є невелика кількість аномалій. З цих даних будується граф відносин між користувачами, комп'ютерами, файлами, створюється поведінкова модель і модель комунікацій, висуваються сценарії загроз. Для аналізу такого набору даних застосовується візуалізація, що реалізується через графи відносин.

В результаті дослідження релевантних робіт у даній предметній області можна зробити висновок про те, що проблема виявлення інсайдерів у мережі є важким завданням та шляхи її вирішення продовжують удосконалюватися, а підходи досить різноманітні, щоб дійти єдиного способу виявлення, оскільки кожне завдання вирішується індивідуально. В більшості робіт автори брали за основу математичний апарат технологій статистичного аналізу при виявленні аномалій, використовували алгоритми кластеризації, а метрики оцінки ефективності ґрунтувалися на оцінці площ під кривими ROC-AUC (Receiver Operating Characteristic, Area Under the Curve).

Таким чином, в результаті аналізу релевантних робіт можна використовувати досвід новітніх розробок у цій галузі щодо способів агрегації даних з подальшим їх аналізом засобами статистичного аналізу та методів машинного навчання. Спираючись на правила виявлення внутрішніх порушників, потрібно створити комплексний підхід виявлення інсайдерів.

1.3. Вимоги до системи виявлення інсайдерів у комп'ютерних мережах

Порівняльний аналіз досліджень у галузі виявлення інсайдерських атак у КС дозволив визначити вимоги до системи виявлення інсайдерів, в основу реалізації яких повинен бути покладений модельно-методичний апарат, що розробляється в цій роботі. Ці вимоги можна розділити на дві групи: функціональні та нефункціональні. Функціональні вимоги є переліком функцій, які має виконувати система. Нефункціональні вимоги описують цільові характеристики системи, такі як обмеження часу, міри помилок, повноти, точності тощо.

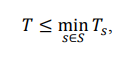
Визначимо безліч функціональних вимог до системи виявлення інсайдерів, що реалізує підходи, що розробляються в даній роботі, наступним чином:

* облік досвіду та напрацьованої бази використовуваних раніше та нині систем виявлення інсайдерів у КС;
* облік специфіки КС та дій інсайдерів у них;
* прогнозування можливої ​​інсайдерської діяльності ще до самої атаки порушником;
* використання існуючих наукових підходів для реалізації методів виявлення інсайдерів (алгоритми, засновані на експертних правилах, методи машинного навчання та обробки великих даних тощо);
* можливість подальшого аналізу всіх внутрішніх даних, що використовуються системою у своїй роботі (наприклад, для коригування алгоритмів);
* можливість налаштування роботи алгоритмів системи експертом з інформаційної безпеки відповідно до КС, що обслуговується;
* генерація звітів про роботу системи та отримані результати у вигляді, адаптованому для експерта з інформаційної безпеки;
* облік специфіки КС, включаючи типові для неї атаки інсайдерів.

Створювана система виявлення інсайдерів повинна враховувати успішне застосування існуючих підходів аналізу КС.

Безліч нефункціональних вимог до системи виявлення інсайдерів можна визначити, як три класичні компоненти ефективності: своєчасність (*T*), обґрунтованість (*O*) та ресурсоспоживання (*R*) [37].

Під своєчасністю розуміється здатність системи забезпечувати розв'язання задачі – виявлення інсайдерів – у встановлений проміжок часу. Вимоги до своєчасності можуть бути задані у формальному вигляді:



де 𝑇 - час виявлення інсайдерів системою, що розробляється, 𝑇𝑆- час виявлення інсайдерів системою 𝑠 з безлічі всіх альтернативних систем 𝑆. Для того щоб розроблювана система могла використовуватися в близькому режимі до реального часу вона повинна виявляти інсайдерів за час, що не перевищує заданої межі. Ця вимога до своєчасності може бути задана у такому вигляді:



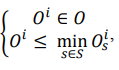
де 𝑃𝑇– ймовірність завершення процесу роботи системи виявлення інсайдерів за заданий час,𝑇𝑑𝑒𝑓 – допустимий час роботи системи (рівний min 𝑇𝑠), 𝑃0𝑇- Допустиме значення ймовірності.

*Обґрунтованість* означає міру виконання задачі системи, а саме – частку виявлених інсайдерів у порівнянні з їхньою реальною наявністю в мережі. Формальна відповідність системи даному критерію може бути визначена за допомогою заходів якості (які будуть описані далі) та задано у формальному вигляді, як:

а) для повноти, точності, акуратності, F-міри:



б) для помилок:



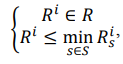
де 𝑂- безліч заходів якості, 𝑂𝑖- і-та міра якості,𝑂𝑖- і-тий захід якості системи 𝑠 з безлічі всіх альтернативних систем 𝑆.

𝑠

Підвищення обґрунтованості роботи системи означатиме загальне підвищення захищеності КС, отже, і досягнення мети дослідження. Однією з найбільш загальних заходів, що характеризують якість роботи, є F-міри і, отже, ця вимога може бути записана наступним чином:

*F-міра → max*.

*Ресурсспоживання* характеризує програмні та апаратні засоби, необхідні системі виявлення інсайдерів для вирішення свого завдання, а також їх характеристики. Визначимо вимогу у формальному вигляді як сукупність наступних показників – кількість хостів (*h*), середній мережевий трафік (*n*), обсяг займаного простору на SSD/HDD (*v*), середнє навантаження на CPU (*c*), середнє завантаження пам'яті (*m*):



де 𝑅 - безліч показників ресурсоекономності, 𝑅𝑖- i-й показник ресурсоекономності (*h, n, v, c, m*), 𝑅s𝑖- і-й показник ресурсоекономності системи 𝑠 з безлічі всіх альтернативних систем 𝑆.

𝑠

Необхідно зазначити, що безпосереднє визначення інсайдерів (як суб'єктів чи особистостей) можливе за мережевим трафіком їхньої активності в КС, а саме – за ID мережевою сесією. Для цього може бути застосований відповідний алгоритм перетворення таких сесій ID в безпосередній ідентифікатор інсайдерів. Тому зсуваємо завдання дослідження до виявлення ідентифікаторів користувачів (user id), а також мережевих пакетів, об'єднаних у сесії та які стосуються інсайдерської діяльності.

Для визначення точних характеристик інсайдерів (імена облікових записів, прізвища, посади тощо) можуть застосовуватись додаткові дії; наприклад, зіставлення IP-адрес зловмисних мережевих пакетів зі звітами сервера журналювання про працюючих за даним комп'ютером користувачах, аналізом камер спостереження, відмітками про проходження на територію співробітників та ін. Все це виходить за рамки предметної області дослідження.

Загальна вимога до задовільності вирішення задачі розроблюваної системою виявлення інсайдерів може бути виражена за допомогою наступних, досить відомих і часто вживаних заходів якості: *TP* (True Positive) – кількість сесій, визначених як інсайдерські, і є такими; *FP* (False Positive) – кількість сесій, визначених як інсайдерські, але не є такими; *TN* (True Negative) кількість користувальницьких сесій, не визначених як інсайдерські та є такими (тобто які не інсайдерські); *FN* (False Positive) – кількість сесій, не визначених як інсайдерські, але не є такими (тобто, які інсайдерські [39]). Класичним синонімом *FP* ​​служать помилки першого роду, а *FN* - помилки другого роду.

Якість виявлення інсайдерів системою можна оцінити з допомогою інших, більш зрозумілих людині заходів: повноти, точності, акуратності, помилки, F-меры [2, 3, 17].

Повнота (*r*) характеризує здатність системи виявляти інсайдерів, не враховуючи при цьому кількість неправильних спрацьовувань. Міра повноти може бути обчислена, як частка вірно визначених інсайдерських сесій серед усіх інсайдерських сесій:



Точність (*p*) характеризує здатність системи виявляти тільки інсайдерів, не захоплюючи при цьому легітимний трафік. Міра точності може бути обчислена, як частка вірно визначених інсайдерських сесій серед усіх певних інсайдерських сесій:



Акуратність (*a*) характеризує здатність системи робити правильні рішення щодо визначення інсайдерів. Міра акуратності може бути обчислена, як частка вірно визначених інсайдерських і не інсайдерських сесій серед усіх сесій користувача:



Помилка (*e*) характеризує здатність системи робити неправильні рішення щодо визначення інсайдерів. Міра помилки може бути обчислена, як частка невірно визначених інсайдерських і не інсайдерських сесій серед усіх сесій користувача:



F-мера (*f*), як правило, застосовується для спільної оцінки системи з позиції повноти та точності. F-мера може бути обчислена як ставлення подвоєного твору повноти і точності системи до їх суми:



За допомогою зазначених заходів розроблювана система виявлення інсайдерів у КС може бути порівняна як з найближчими аналогами, так і з її власними модифікаціями.

1.4 Постановка задачі

Сформульована задача полягає у розробці: моделі представлення великих даних про інсайдерські атаки у форматі NoSQL; моделі та алгоритми комбінованого застосування експертних правил (RB-алгоритм, від англ. Rule-Based – на базі правил) та методів машинного навчання (ML-алгоритм, від англ. Machine Learning – машинне навчання) в інтересах виявлення інсайдерських атак; методики виявлення інсайдерів у КС з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних; архітектури та програмної реалізації системи виявлення інсайдерів у КС з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних.

Метою дослідження є підвищення безпеки КС від внутрішніх атак. У роботі показник захищеності визначається через показник обґрунтованості (F-міри) з урахуванням обмежень інших показників обґрунтованості (повноти, точності, акуратності, помилки), а також з урахуванням вимог до своєчасності та ресурсоспоживання.

Дотримуючись встановлених вимог до системи виявлення інсайдерів у КС, визначимо загальний шлях дослідження.

Методика виявлення інсайдерів у КС, очевидно, має використовувати нові рішення у сфері захисту; вони, по-перше, повинні мати суттєвий рівень високотехнологічності, а, по-друге, бути поки що важко нейтралізованими зловмисниками (тобто інсайдерами). З іншого боку, накопичений досвід класичних рішень щодо протидії інсайдерській діяльності також має враховуватися.

Таким чином, результатом досліджень має стати поєднання різних успішних підходів до виявлення інсайдерів у КС; Вочевидь, таке об'єднання має враховувати позитивні боку підходів, максимально позбавившись їх негативних сторін. Також мають бути враховані можливі додаткові ефекти, що виникають при об'єднанні двох підсистем, - гіпотетично, як підвищують підсумковий результат, і знижують його; останнє, очевидно, має бути мінімізованим.

Для формування пулу можливих підходів, з яких може бути складена результуюча методика, необхідно проаналізувати як існуючі на даний момент і підходи, що активно використовуються, так і є перспективними, але можливо, застосовуваними для близьких завдань. В результаті можна буде виділити набір моделей, методик та алгоритмів, які можуть бути використані у дослідженні. При цьому, узагальнюючою ланкою підходів можна вважати їхню схильність для роботи з атрибутами поведінки користувача в мережі, що визначаються за допомогою аналізу мережевого трафіку (як на рівні мережевих пакетів, так і виходячи з логів роботи мережевих сервісів тощо).

Виходячи з величезної і постійно зростаючої кількості атрибутів, що генеруються в одиницю часу, якими може бути описана робота користувача в КС, доцільним може виявитися використання обробки великих даних.

Тим самим можуть бути вирішені як поточні, так і, можливо, майбутні завдання збору та зберігання даних. В інтересах зберігання даних, очевидно, знадобиться розробка власної бази даних, адаптованої для зберігання інформації про поведінку користувачів.

Використовуючи модель представлення великих даних у форматі NoSQL, можна розробити відповідні алгоритми виявлення аномалій даних, що сигналізують про дії зловмисників – інсайдерів КС. У первинному варіанті досить розробити по одному алгоритму, що умовно протиставляється один одному з позицій використовуваного ними підходу. Так, як перший алгоритм підходящим може бути алгоритм, побудований на основі експертних правил. Під експертними правилами розуміються правила, жорстко задані експертом на підставі логіки, законів галузі застосування та практичного досвіду експерта. Як другий алгоритм потенційно затребуваним є алгоритм, який використовує у своїй роботі результати машинного навчання,

Результатом об'єднання цих алгоритмів буде комплексна методика виявлення інсайдерів у КС, у створенні якої полягає робота; в міру своєї специфіки, обидва алгоритми можуть працювати паралельно.

Для практичного використання створеної методики необхідна розробка архітектури програмного комплексу системи виявлення інсайдерів в КС, що включає її основні модулі, інформаційні та керуючі потоки, а також алгоритми роботи. Реалізація такої архітектури як програмного комплексу дозволить безпосередньо перевірити роботу методики практично.

Необхідною умовою досягнення мети дослідження має стати порівняння розробленої методики з аналогами, результати якого обґрунтовано покажуть ступінь підвищення захищеності КС.

Слід мати на увазі, що оскільки кожен з алгоритмів на виході видаватиме свою множину виявлених інсайдерів (заданих пов'язаним з кожним із них ID мережевої сесії), - просте об'єднання цих множин може бути некоректним. Так, наприклад, може виявитися, що один з алгоритмів у принципі працюватиме краще за інший і об'єднання їх виходів лише погіршить кінцевий результат. Отже, крім порівняння розробленої методики з аналогами, знадобиться порівняння різних варіацій методики, пов'язаних з формулами обчислення кінцевого результату (тобто безлічі інсайдерів) – за результатом роботи алгоритмів на основі експертних правил 𝐼𝑅𝐿 або методів машинного навчання 𝐼𝑀𝐿.

Кінцевий результат 𝐼𝑅𝑒𝑠 може бути підрахований за допомогою однієї з чотирьох таких формул: як об'єднання множини результатів алгоритмів – 𝐼𝑅𝑒𝑠 = 𝐼𝑅𝐵 ∨ 𝐼𝑀𝐿, як їх перетин - 𝐼𝑅𝑒𝑠 = 𝐼𝑅𝐵 ⋀ 𝐼𝑀𝐿 або як результат одного з алгоритмів (очевидно, найкращого) – 𝐼𝑅𝑒𝑠 = 𝐼𝑅𝐵 або 𝐼 = 𝐼𝑀𝐿. Кінцевий вибір найкращої варіації методики може бути зроблений на підставі введених раніше заходів: повноти, точності, акуратності, помилки та F-заходи. Врахуємо також те, що алгоритм з урахуванням методів машинного навчання можливо представлений на нижньому рівні як базові класифікатори: *DT, NB, k-NN, SVM*; на верхньому рівні – у вигляді композицій базових класифікаторів: голосування більшістю (*PV*), виважене голосування (*WV*) та м'яке голосування (*SV*), а також Adaboost [32]. Вибір методу класифікації впливатиме на результати роботи методики.

Виходячи з передбачуваного ходу дослідження, опишемо завдання, вирішення яких буде необхідним:

* 1. розробка моделі представлення великих даних про інсайдерські атаки у форматі NoSQL (включаючи модель інсайдера);
  2. розробка алгоритму виявлення інсайдерів у КС, що базується на експертних правилах;
  3. розробка моделі та алгоритмів комбінованого застосування експертних правил та методів машинного навчання на користь виявлення інсайдерських атак;

4) розробка методики виявлення інсайдерів у КС з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних;

5) побудова архітектури та реалізація програмного комплексу системи виявлення інсайдерів у КС на базі запропонованої методики, налаштування алгоритму на основі методів машинного навчання за допомогою набору даних, що характеризують дії інсайдерів за заданою множиною сценаріїв атак, та експериментальна оцінка розробленої методики системи виявлення інсайдерів у КС.

На змістовному рівні наукове завдання дослідження можна сформулювати таким чином: розробити модельно-методичний апарат (модель уявлення великих даних про інсайдерські атаки у форматі NoSQL, модель і комплекс алгоритмів виявлення інсайдерів, методику виявлення інсайдерів, архітектуру системи виявлення інсайдерів) . Розробка та експериментальна перевірка функціонування програмної реалізації відповідної системи виявлення дозволить визначити результативність модельно-методичного апарату.

Вхідними завдання дослідження є такі дані, що описують поведінки користувачів 𝑈𝑠𝑒𝑟𝑠:

{𝑁𝑒𝑡𝑓𝑙𝑜𝑤, 𝐴𝑝𝑝𝑙𝑖𝑐𝑎𝑡𝑖𝑜𝑛𝑠, 𝐷𝑎𝑡𝑎, 𝑆𝑐𝑎𝑛𝑛𝑒𝑟𝑠, 𝑆𝑒𝑟𝑣𝑒𝑟𝑠, 𝐷𝑒𝑣𝑖𝑐𝑒𝑠 },

де Netflow – статистичні дані про взаємодію хостів мережі, Applications – користувацькі програми, Data – сирі дані (необроблена послідовність байт), Scanners – сканери, що реалізують збір інформації про мережу, Servers – сервери, що надають послуги користувачам у комп'ютерній мережі (DHCP, RADIUS, DNS), Devices - пристрої користувача.

Потрібно знайти внутрішніх порушників (інсайдерів) {𝐼𝑛𝑠𝑖𝑑𝑒𝑟𝑠}. Визначення інсайдерів складає основі атрибутів поведінки користувачів. Поведінка інсайдера може бути формалізована на основі введення порогів, що задають різні характеристики дій, що виконуються інсайдером, наприклад обсяг завантажених файлів. Поведінка інсайдера визначається за допомогою моделі інсайдера, що може бути описано в наступному вигляді:

𝐼 =< 𝑅, 𝐿, 𝑄, 𝐺 >,

де *R* – критерії атрибутів інсайдера, *L* – рівні доступу, *Q* – кваліфікація інсайдера, *G* – ціль інсайдера.

Таким чином, наукове завдання може бути описано наступним чином: для наявного набору вхідних даних про поведінку користувача знайти наступний кортеж:

< 𝑀𝑜𝑑, 𝐴𝑙𝑔, 𝑀𝑒𝑡, 𝐴𝑟𝑐ℎ >*,*

де *Mod* – модель представлення великих даних про атаки інсайдерів у форматі NoSQL, що включає модель інсайдера; *Alg* – модель та алгоритми комбінованого застосування експертних правил та методів машинного навчання на користь виявлення інсайдерських атак; *Met* – методика виявлення інсайдерів у КС, *Arch* – архітектура та програмна реалізація системи виявлення інсайдерів у КС.

При цьому необхідно досягти максимізації показника F-заходи комплексу алгоритмів при обмеженнях наступних заходів: повноти, точності, акуратності; помилки; з урахуванням вимог до своєчасності та ресурсоспоживання.

МОДЕЛІ ТА АЛГОРИТМИ ВИЯВЛЕННЯ ІНСАЙДЕРІВ У КОМП’ЮТЕРНИХ СИСТЕМАХ

2.1 Модель представлення великих даних про інсайдерські атаки форматі NoSQL

Сучасні інсайдерські атаки є комплексними та використовують безліч способів реалізації та векторів атак для отримання несанкціонованого доступу та компрометації інформаційних об'єктів у внутрішній мережі. Інсайдер може бути будь-який користувач мережі. Отже, у системах захисту від атак необхідно виконувати процедури аналізу та контролю дій користувачів, які називаються профільуванням поведінки користувачів.

У існуючих дослідженнях та розробках ці процедури отримали назву аналітики поведінки користувачів – User Behavior Analytics (UBA) та User and Entity Behavior Analytics (UEBA) [23, 35]. Формально системи UBA та UEBA належать до одного і того ж класу систем, але між ними є одна фундаментальна різниця. UBA-системи використовують інформацію, що містить тільки дані про активність користувача, отже, фокусуються на користувачах та їх ролях. UEBA-системи разом з даними, що застосовуються в UBA-системах, враховують інформацію про системне оточення (мережевий трафік, системи зберігання даних, робочі станції та програмне забезпечення). Це дає можливість UEBA-системам профілювати не лише користувачів, а й стан програмного та апаратного забезпечення загалом.

Для реалізації UBA і UEBA необхідна система управління базами даних (СУБД), здатна легко масштабуватися і має високу швидкість обробки запитів. Для цього в даний час використовуються СУБД NoSQL (Not only SQL) [16, 24, 28, 40]. Рішення на основі NoSQL в цілому надають масштабований та гнучкий спосіб вирішення завдань, які раніше керувалися реляційними базами даних. Прикладом СУБД NoSQL є OrientDB [38], яка поєднує в собі можливості документоорієнтованої та графоорієнтованої баз даних (БД). Це означає, що вона має повні графічні можливості у поєднанні з функціями, які зазвичай присутні тільки в базах даних документів.

Для побудови моделі представлення великих даних про інсайдерські атаки з метою виявлення інсайдерів в КС розглянемо джерела даних, що збираються. Як джерела даних для аналітики поведінки користувачів візьмемо всі клієнтські пристрої, підключені як до бездротових, так і до провідних компонентів КС. У запропонованій моделі передбачається здійснювати контроль над усім обладнанням, що знаходиться в локальній мережі, та над тими пристроями, наявність яких не передбачалося власником мережі, наприклад, мобільних телефонів, ноутбуків та інших пристроїв, що мають можливість бездротового з'єднання.

На рис. 2.1 наводиться приклад джерел для збору відомостей, якими можуть виступати дані, що передаються по мережі, різні програми, а також використовувані пристрої.

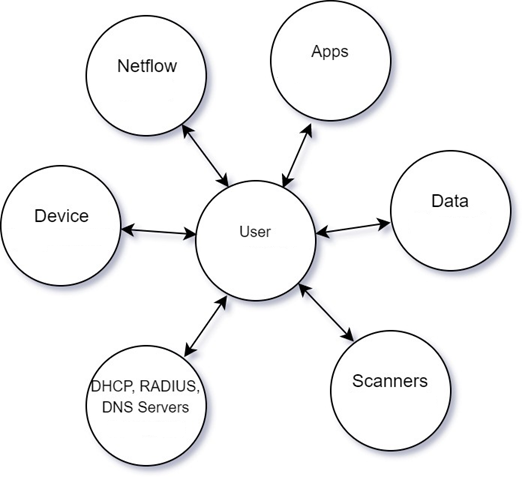


Рисунок 2.1 – Джерела для збору даних, що описують поведінку користувача в КС

Формальний вид моделі уявлення великих даних про інсайдерські атаки має такий вигляд:

𝑀 = 〈𝐴, 𝐼〉,

де *A* – елементи, що є атрибутами поведінки користувача, *I* – модель інсайдера та критерії, які дозволяють визначити поточного користувача до категорії інсайдерів.

Уявимо виділені атрибути поведінки користувачів і їх взаємозв'язку формально:

𝐴 = <𝐷𝑎𝑡𝑎𝑆𝑜𝑢𝑟𝑐𝑒𝑠, 𝑈𝑠𝑒𝑟𝑠, 𝐷𝑎𝑡𝑎, *Parcer*>.

Перерахуємо елементи, що входять до цього кортежу:

 𝐷𝑎𝑡𝑎𝑆𝑜𝑢𝑟𝑐𝑒𝑠 = <𝑁𝑒𝑡𝑓𝑙𝑜𝑤, 𝐴𝑝𝑝𝑙𝑖𝑐𝑎𝑡𝑖𝑜𝑛, 𝑆𝑐𝑎𝑛𝑛𝑒𝑟, 𝑆𝑒𝑟𝑣𝑒𝑟, 𝐷𝑒𝑣𝑖𝑐𝑒>- джерела даних, кожен елемент яких є відповідно мережевий потік, додаток, файл операційної системи, сканер, сервер, пристрій;

𝑈𝑠𝑒𝑟𝑠 =⋃𝑃i=1 - користувачі, 𝑈𝑠𝑒𝑟𝑖 = <𝑈𝑠𝑒𝑟𝐼𝐷𝑖, 𝐴𝑡𝑡𝑟𝑖, 𝑆𝑒𝑠𝑠𝑖𝑜𝑛*i*> - триплет, що являє собою відповідно ідентифікатор користувача, атрибути користувача та відповідні йому сесії;

 𝐷𝑎𝑡𝑎 = {0,1}+ = {0,1,00,01,10,11,000, … } - дані, що являють собою всілякі бітові ланцюжки, що зберігаються на джерелах даних;

 𝑃𝑎𝑟𝑠𝑒𝑟: 𝐷𝑎𝑡𝑎 × 𝐷𝑎𝑡𝑎𝑆𝑜𝑢𝑟𝑐𝑒 × 𝑇𝑑𝑑- відображення, що формує сесію з сирих даних в залежності від типу джерела цих даних і часу.

Модель інсайдера може бути описана у такому вигляді:

𝐼 =< 𝑅, 𝐿, 𝑄, 𝐺 >,

де *R* - критерії атрибутів, що складаються з набору ознак, за якими приймається рішення про віднесення користувача до багатьох інсайдерів (наприклад, регламентований графік роботи, допустиме навантаження на мережу, оцінка роботи з інформаційними ресурсами); *L* – рівні доступу, що визначають права користувачів у КС, порушення яких означатиме потенційну інсайдерську діяльність (наприклад, оператор, інженер чи адміністратор); *Q* – кваліфікація інсайдера, що визначає необхідний рівень підготовки для проведення атаки (наприклад, хакер – який володіє знаннями про вразливості інформаційних систем, засоби їх експлуатації, методами приховування слідів порушень; вандал – який володіє в основному методами та механізмами зламу елементів КС, у тому числі фізичного; неблагонадійний користувач – не вміє завдавати свідомої шкоди КС і інформації, що циркулює в ній, але схильний до отримання, спотворення та поширення інформації умовно-законними способами без злого наміру); *G* – мета інсайдера, що визначає основний вектор інсайдерської діяльності, пов'язаний з відповідними загрозами порушення конфіденційності, цілісності та доступності інформації (наприклад, збір не призначеної для користувача інформації; винесення конфіденційної інформації за периметр організації та/або її передачу третім особам; модифікація інформації, включаючи її повне знищення тощо).

Розглянемо елементи, що є атрибутами поведінки користувачів. Джерела даних містять інформацію про користувачів у сирому вигляді. Для перетворення цих даних на сесії застосовується відображення *Parser*. Наприклад, у разі мережного потоку дане відображення дозволяє виділити TCP-з'єднання або HTTP-сесію, а у випадку програми/файла сформувати характеристики сесії ОС, в рамках якої ця програма була встановлена/файл був створений.

Припустимо, що на одному з джерел даних datasrc були згенеровані дані data в певний час часу. Тоді ідентифікатор користувача uid, в рамках однієї із сесій якого було згенеровано ці дані, визначається наступним чином:

𝑢𝑖𝑑 ∈ {𝑢𝑠𝑒𝑟𝑖𝑑 | <𝑢𝑠𝑒𝑟𝑖𝑑, 𝑎𝑡𝑡𝑟, 𝑠𝑒𝑠𝑠𝑖𝑜𝑛𝑠> ∈ 𝑈𝑠𝑒𝑟𝑠 ∧ 𝑃𝑎𝑟𝑠𝑒𝑟(𝑑𝑎𝑡𝑎, 𝑑𝑎𝑡𝑎𝑠𝑟𝑐, 𝑡𝑖𝑚𝑒) ∈𝑑

У досліджуваних даних виділимо основні атрибути поведінки користувачів, необхідні дослідження їх активності та детектування аномалій з метою можливого виявлення інсайдерів.

Наведемо приклад атрибутів поведінки користувачів:

* **UserFields**– поля, що належать користувачеві (не залежить від конкретної сесії);
* **ID**- Унікальний номер користувача;
* **User-Agent**– атрибути кінцевого користувача, які дозволяють визначити інформацію про його тип, операційну систему, вендори тощо;
* **Login**- логін користувача;
* **Pass**– пароль користувача;
* **T** – граничне значення, що вказує ступінь довіри до користувача (є встановленим числом, яке може бути скориговано оператором системи виявлення інсайдерів);
* **Rights**- Права доступу на читання, зміна, редагування файлів;
* **TotalAuth**– загальна кількість спроб входу (необхідне оцінки кількості спроб входу до системи з різних пристроїв);
  + **Active Directory-проби**- проби, засновані на отриманих даних з AD;
* **AD-host**- Ознака того, чи є хост членом домену;
* **AD-domain**- Домен підключення;
* **AD-operation-system**- поточна операційна система;
* **AD-version OS**- поточна версія операційної системи;
* **AD-service pack**- поточний пакет оновлень операційної системи;
* **Radius-проби**– список проб, що базуються на зверненні кінцевого пристрою до Radius сервера;
  + **Calling-Station-ID**- MAC-адреса кінцевої точки;
  + **NAS-IP-Address**– IP-адреса мережевого пристрою доступу, який є автентифікатором у мережі;
  + **NAS-Port**- Номер фізичного порту автентифікатора;
  + **Framed-IP-Address**- IP-адреса кінцевої точки;
  + **Acct-Session-ID**- Унікальний ідентифікатор сесії обліку;
  + **Acct-Session-Time** - Час, протягом якого кінцева точка отримує сервіс;
  + **Acct-Terminate-Cause** – якщо сесія або з'єднання розірвано, це поле міститиме інформацію про причину;
  + **On-For-Login-Auth** – використовується для пересилання міток QoS у пакетах автентифікації;
  + **DHCP-проба**– список проб, що базуються на DHCP-зверненні кінцевого пристрою;
  + **Dhcp-class-identifier**- Повідомляє платформу пристрою або інформацію про ОС;
  + **Dhcp-client-identifer**– відображає MAC-адресу кінцевого пристрою;
  + **Dhcp-user-class-id** – параметр деяких ОС (MAC/Windows), що є унікальним корпоративним ідентифікатором клієнта;
  + **Dhcp-requsted-address**- IP-адреса пристрою;
  + **Dhcp-server-identifier**- Ідентифікатор сервера;
  + **Dhcp-parameters-request-list**- Унікальний ідентифікатор типу пристрою;
  + **Dhcp-message-type**- Тип DHCP-повідомлення;
  + **DNS-проби**– проба, що базується на отриманні інформації від DNS сервера;
  + **DNS-FQDN**- Повне доменне ім'я;
  + **NMAP-проби** - сканування відкритих портів на кінцевому влаштування;
  + **Session**- список сесій з інформацією про них (є список кортежів типу SessionData);
  + **SessionData**– поля, що належать до конкретної унікальної сесії та містять інформацію про неї;
  + **SessionID**- Унікальний номер сесії;
  + **Changes**– список файлів, яких було здійснено доступ із часу входу в систему;
  + **Auth**- Число спроб входу в систему перед успішною аутентифікацією в даній сесії;
  + **LogPass**– зв'язування логін-пароль, що використовується при спробі входу в систему;
  + **Sites** - Використання нестандартних мережевих ресурсів (вказує, чи відвідував користувач під час сеансу підозрілі веб ресурси: користувачі, які не володіють високими привілеями і використовують незвичайні ресурси, можуть виявитися порушниками інформаційної безпеки);
  + **Periph**- використовувані периферійні пристрої (поле містить список всіх пристроїв, що використовуються в ході сесії);
  + **Time**- час, що минув від початку сесії, або час виходу із системи (підозрілими можуть вважатися сесії, скоєні в незвичайний для користувача час);
  + **Progs** - Наявність на комп'ютері додатків, що здійснюють підозрілу активність (це можуть бути утиліти, що здійснюють у фоновому режимі підвищену мережну активність);
  + **NoAV**- Вказує на відсутність антивірусних програм на пристрої, або на ситуацію, коли антивірусні основи сильно застаріли (є важливим критерієм при детектуванні інсайдерів);
  + **LogType** - спосіб входу в систему (стандартний або нестандартний; може бути здійснений з робочого місця або через приватну віртуальну мережу);
  + **Geo** – географічне положення (підозрілою може вважатися різка зміна географічного положення під час роботи в системі);
  + **DeviceID**- Унікальний номер пристрою;
  + **AppID**- Унікальний номер програми;
  + **DeviceFields**– поля, що належать до конкретного пристрою та не залежать від користувача;
  + **Name**- Ім'я пристрою;
  + **OS**- Назва операційної системи, версія, поточний пакет оновлень;
  + **Vendor**- Найменування фірми-виробника;
  + **AppFields**– поля, що належать конкретному додатку на пристрої;
  + **AppName –**назва ПЗ;
  + **Version**- Версія ПЗ;
  + **Developer**- Розробник ПЗ;
  + **Ports**- Порти, що використовуються додатком;
  + **Netflow**– список потоків, що містить інформацію про мережну активність користувача у конкретній сесії;
  + **Source IP address**- IP-адреса джерела;
  + **Destination IP address**- IP-адреса призначення;
  + **Next-Hop IP address**– IP-адреса наступного маршрутизатора, на яку буде переданий мережевий потік;
  + **Input ifIndex**- SNMP індекс інтерфейсу, через який маршрутизатор отримує мережевий потік;
  + **Output ifIndex** - SNMP індекс інтерфейсу, через котрий маршрутизатор передає мережевий потік;
  + **Packets**– загальна кількість отриманих пакетів у межах потоку;
  + **Bytes**– загальна кількість байт, отриманих у межах потоку;
  + **Start time of flow**- Час початку потоку;
  + **End time of flow**- Час закінчення потоку;
  + **Source port**- Порт джерела;
  + **Destination port**- порт призначення;
  + **TCP Flags**- TCP прапори;
  + **IP protocol**- Номер IP протоколу;
  + **ToS**- Тип сервісу;
  + **Source AS**- Номер автономної системи IP джерела;
  + **Destination AS**- Номер автономної системи IP призначення;
  + **Source Mask**- маска мережі IP джерела;
  + **Destination Mask**- маска мережі IP призначення;
  + **Padding**- Відступи для ефективного використання всієї довжини заголовка;
  + **Source VLAN**- Номер VLAN джерела;
  + **Destination VLAN**- Номер VLAN призначення;
  + **Source MAC**- MAC-адреса джерела;
  + **Destination MAC**– MAC-адреса призначення
  + **Income Traffic [SIZE]** - масив значень обсягу отриманого мережевого трафіку за кожну годину протягом останніх 30 днів (отже, SIZE = 24 \* 30 = 720);
  + **Outcome Traffic [SIZE]** – масив значень обсягу відправленого мережевого трафіку за кожну годину протягом останніх 30 днів (отже, SIZE = 24 \* 30 = 720)
  + **Traffic Time** – час завершення збору інформації про мережний трафік (використовується як відправна точка) для полів Income Traffic/Outcome Traffic.

Ці та інші поля разом із взаємозв'язками з-поміж них зображені рис. 2.2.

Для пояснення ідеї роботи моделей наведемо приклади відображення в них інсайдера (𝑈𝐼) та законного користувача (𝑈𝐿). Припустимо, інсайдерська діяльність першого користувача полягає у завантаженні великого розміру трафіку з внутрішніх ресурсів організації та подальшому відвідуванні підозрілих сайтів (наприклад, з метою надсилання оброблених даних поза периметром організації). Відповідно, другий користувач може робити те саме, але в значно менших обсягах - тобто вести законну діяльність (наприклад, в рамках посадових обов'язків).

Таблиця 2.1. Приклад моделі та критеріїв подання інсайдера у форматі NoSQL

|  |  |
| --- | --- |
| **Ключ** | **Документ** |
| Критерій 1 | {  "Name": "Функціонування мережі", "Умови": {  "Максимальна кількість звернень до хостів (шт./хв)": [1000, "Заборонено"],  "Максимальна кількість нетипових запитів (шт./хв)": [1000, "Заборонено"],  "Нестандартні завершення сесії": "Заборонено"  }  } |

Таблиця 2.1. Приклад моделі та критеріїв подання інсайдера у форматі NoSQL (продовження)

|  |  |
| --- | --- |
| **Ключ** | **Документ** |
| Критерій 2 | {  "Name": "Функціонування Active Directory", "Умови": {  "Наявність вузлів – не члени домену": "Заборонено", "Відсутність доменного імені": "Заборонено"  }  } |
| Критерій 3 | {  "Name": "Зараження ПК",  "Умови": {  "Необхідні версії програмного забезпечення": [["Windows 10", "Windows server 2019"], "Заборонено"]  "Небезпечні сайти": [["vk.com", "casino.ru", "cia.gov"], "Підозріло"], "Межа нетипової активності додатків (%)": ["70", "Підозріло"] , "Нестадартні підключення": ["Підозріло "]  }  } |
| Критерій 4 | {  "Name": "Людський фактор", "Умови": {  "Нові периферійні пристрої": ["Догляд"], "Нестандартні пристрої – зміна параметрів": [["ОС", "MAC", "IP"],  " Підозріло"]  }  } |
| Критерій 5 | {  "Name": "Аутентифікація","Критерії": {  "Максимальна кількість невдалих аутентифікацій": [[3, "Підозріло"], [10, "Заборонено"]]  }  } |

Таблиця 2.1. Приклад моделі та критеріїв подання інсайдера у форматі NoSQL (продовження)

|  |  |
| --- | --- |
| **Ключ** | **Документ** |
| Критерій 6 | {  "Name": "Збір та витік інформації", "Умови": {  "Максимальне перевищення кількості відправленої за межі периметра організації інформації (Гб/година)": [[1, "Підозріло"], [10, "Заборонено"]],  "Максимальне перевищення кількості зібраної в рамках периметра організації інформації (Гб/год)": [[1, "Підозріло"], [10, "Заборонено"]]  } } |
| Критерій 7 | {  "Name": "Робочий розпорядок користувачів",  "Критерії": {  "Початок сесії (час)": [["пн|вт|ср|чт", ["09:00-18:00"], "Підозріло"],  ["пт", ["09:00-13:00", "14:00-18:00"], "Підозріло"]],  "Кінець сесії (час)": [["пн|вт|ср|чт", ["09:00-18:00"], "Підозріло"],  ["пт", ["09:00-13:00", "14:00-18:00"], "Підозріло"]]  } } |
| Критерій 8 | {  "Name": "Обмеження","Умови": {  "Висока важливість": 3,  "Критична важливість": 6,  “Мінімальний рівень доступу”: “Operator”, “Максимальний рівень доступу”: “Administrator”,  “Кваліфікація інсайдера”: [“Хакер”, “Вандал”, “Неблагонадійний користувач”],  "Мета інсайдера": ["Збір інформації", "Винос інформації", "Модифікація інформації"],  }  } |

Для виявлення таких атак у моделі інсайдера (описаних у термінах NoSQL бази даних: Ключ – Документ) буде використано наступні критерії.

Таблиця 2.2. Приклад критеріїв та умов моделі подання інсайдера у форматі NoSQL

|  |  |
| --- | --- |
| **Ключ** | **Документ** |
| Критерій 3 | {  "Name": "Зараження ПК", "Умови": {  "Небезпечні сайти": [["vk.com", "casino.ru", "cia.gov"], "Підозріло"],  }  } |
| Критерій 6 | {  "Name": "Збір та витік інформації", "Умови": {  "Максимальна кількість зібраної в периметрі організації інформації (Гб/год)": [[1, "Підозріло"], [10, "Заборонено"]]  }  } |
| Критерій 8 | {  "Name": "Обмеження","Умови": {  "Висока важливість": 3,  "Кваліфікація інсайдера": "Неблагонадійний користувач"], "Мета інсайдера": ["Збір інформації", "Винос інформації"],  }  } |

Невідповідність поведінки користувачів цим критеріям може сигналізувати про інсайдерську діяльність.

Розглянемо вид моделі уявлення великих даних про інсайдерські атаки для поведінки 𝑈𝐼 (з Id сесії 1001) та 𝑈𝐿 (c Id сесії 2001) у частині її полів, пов'язаних із цими критеріями.

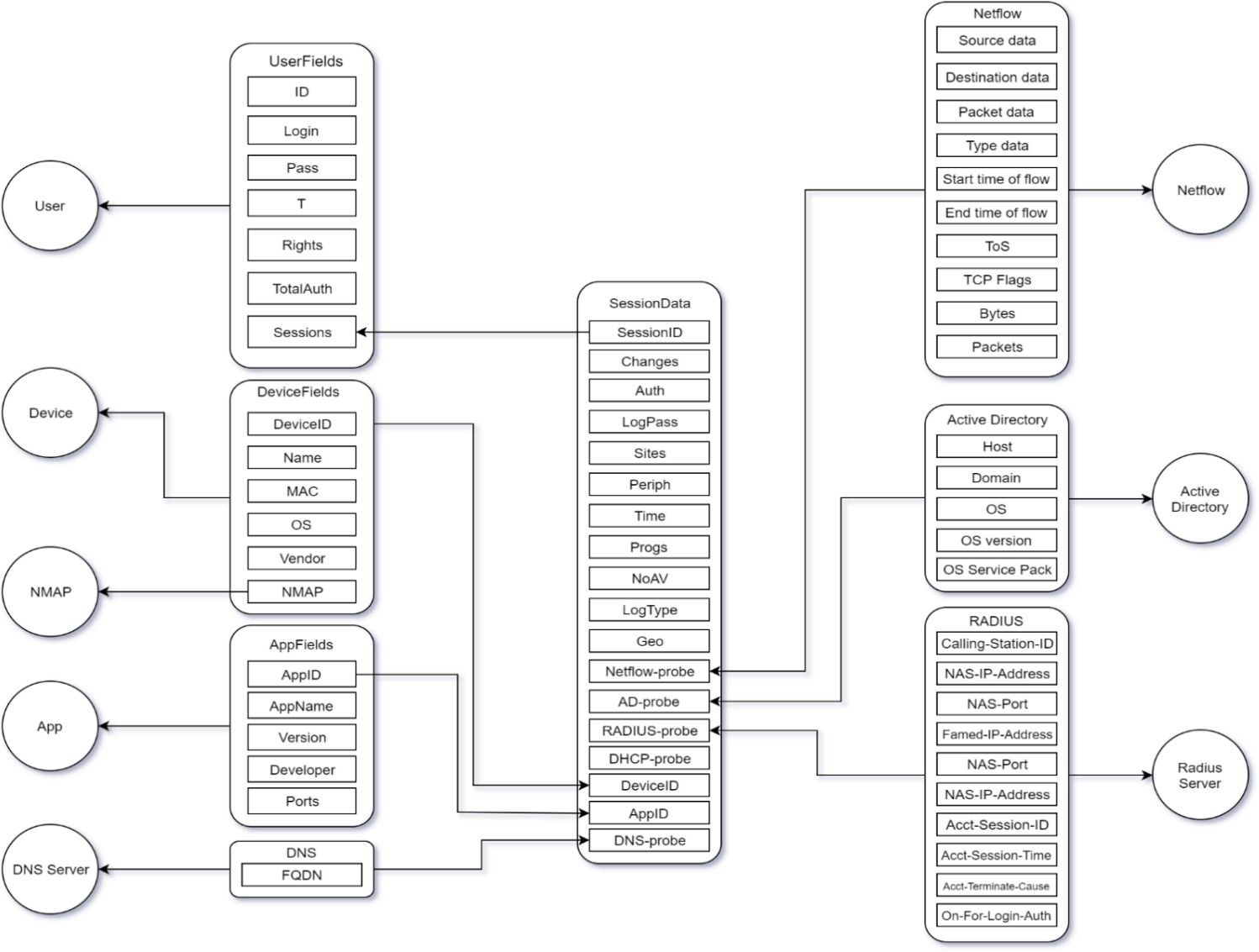


Рисунок 2.2 – Взаємозв'язок між основними атрибутами поведінки користувачів

Для коректного функціонування необхідно також попередньо підготувати профілі нормальної поведінки користувачів, на підставі відхилення яких визначається, чи належить користувач інсайдерам. Чим більше буде кількість полів та кількість профілів нормальної поведінки, тим більш точно будуть визначатися інсайдери у мережі. Інсайдерів у наведеній схемі можна визначити за такими параметрами: нестандартний пристрій, з якого виконується підключення; використання додатків, які раніше не використовувалися користувачем; час завершення сесії у неробочий час; відсутність антивірусного ПЗ; прояв під час сесії підозрілої мережевої активності від пристрою; коригування нестандартних файлів під час сесії; кількість спроб аутентифікації перед створенням конкретної сесії.

Модель побудована з використанням NoSQL підходів, що відрізняються від традиційних СУБД, що використовуються, саме орієнтованістю на управління великими даними. Так, замість ACID вимог щодо атомарності, узгодженості, ізольованості та довговічності/надійності (Atomicity, Consistency, Isolation, Durability), в NoSQL основний аспект зміщений у бік базової доступності, гнучкого стану та узгодженості в кінцевому стані. Також, характерними рисами NoSQL-рішення є лінійна масштабованість, різнорідність типів сховищ, можливість розробки без завдання схеми бази даних та ін.

2.2 Алгоритм виявлення інсайдерів у КС із використанням експертних правил

Для виявлення інсайдерів у КС було розроблено алгоритм, заснований на експертних правилах. Передумовою для створення експертних правил послужив варіант типової політики безпеки в організації (стосовно поведінки користувачів в КС), який був створений на підставі думок експертів у даній галузі. Очевидно, що наведена політика безпеки є лише одним із можливих прикладів. Тим не менш, запропонований підхід формування алгоритму може бути застосований і до більшості політик, що реально діють.

Політика складається з набору базових правил, з кожним з яких асоціювалося безліч критеріїв визначення відповідності правилам, а також ступінь критичності не відповідності їм (таблиця 2.3).

Таблиця 2.3 – Приклад можливої ​​політики інформаційної безпеки поведінки користувача у КС організації

|  |  |  |
| --- | --- | --- |
| **Правило політики** | **Критерій відповідності правилу** | **Ступінь**  **критичності** |
| 1. Запобігання порушенням функціонування комп'ютерної мережі всередині організації. | Створення великої кількості звернень до хостів (за короткий час – протягом 1 хвилини)  – близько 1000 повідомлень). | Заборонено |
| Створення великої кількості нетипових запитів обсягом близько 1000 запитів на хвилину (з прапорами TCP Reset, SYN, SYN +  FIN). | Заборонено |
| Нестандартне завершення сесії. | Заборонено |
|  | | |

Таблиця 2.3 – Приклад можливої ​​політики інформаційної безпеки поведінки користувача у КС організації (продовження)

|  |  |  |
| --- | --- | --- |
| **Правило політики** | **Критерій відповідності правилу** | **Ступінь**  **критичності** |
| 2. Забезпечення коректного функціонування Active Directory. | Наявність вузлів, які не є членами  домену - чи є пристрій корпоративним. | Заборонено |
| Відсутність доменного імені. | Заборонено |
|  | | |
| 3. Запобігання та визначення факту зараження ПК шкідливим ПЗ. | Невідповідність ОС, її служб та оновлень необхідним версіям – оновлення ПЗ має бути здійснено протягом одного  дня після виходу оновлення. | Заборонено |
| Відвідування небезпечних/заборонених сайтів – відповідно до списку заборонених URL  адрес організації. | Підозріло |
| Наявність програм з нетиповою активністю – для кожної типової програми задана стандартна активність. Наприклад, програма Skype активно  працює у фоновому режимі. | Підозріло |
| Поява нестандартних підключень – у КС з'явилися програми або пристрої, які використовують нестандартні порти  підключення. | Підозріло |
| 4. Запобігання людському фактору. | Підключення нових периферійних  пристроїв. | Підозріло |
| Поява нестандартних пристроїв – зміна  ОС, MAC, IP та ін. | Підозріло |
|  | | |
| 5. Запобігання перебору логіну та паролю. | Виконання понад 3 невдалих  автентифікацій. | Підозріло |
| Виконання понад 10 невдалих  автентифікацій. | Заборонено |

Таблиця 2.3 – Приклад можливої ​​політики інформаційної безпеки поведінки користувача у КС організації (продовження)

|  |  |  |
| --- | --- | --- |
| **Правило політики** | **Критерій відповідності правилу** | **Ступінь**  **критичності** |
| 6. Запобігання витоку інформації за периметр організації. | Відправлення великої кількості даних поза периметром організації – перевищення обсягу переданої інформації за 1 годину становить близько 10 Гб порівняно із середньоденною  відправкою за попередні 6 місяців. | Заборонено |
| Надсилання даних в обсязі більше 1 Гб за годину поза периметром організації в порівнянні з середньо-денною відправкою за попередні 6  місяців. | Підозріло |
|  | | |
| 7. Запобігання нелегітимному збору інформації з внутрішніх ресурсів організації. | Отримання великої кількості даних усередині периметра з внутрішніх ресурсів організації – перевищення обсягу отриманої інформації за 1 годину становить близько 10 Гб порівняно із середньоденним трафіком, отриманим за попередні 6  місяців. | Заборонено |
| Отримання даних в об'ємі понад 1 Гб за годину з внутрішніх серверів за 1 годину порівняно із середньоденною відправкою за попередні  6 місяців. | Підозріло |
| 8. Підзвітність дій користувачів. | Початок сесії в неробочий час (з 18.00 вечора до 9.00 ранку; нарада у п'ятницю з  13:00 до 14:00). | Підозріло |
| Завершення сесії у неробочий час (з 18.00 вечора до 9.00 ранку; нарада у п'ятницю з  13:00 до 14:00). | Підозріло |

Примітка. У таблиці 2.3 у стовпці Ступінь критичності зазначено важливість критерію для відповідності політиці безпеки. Так, значення «Заборонено» означає неприпустимість невідповідності сесії користувача даному критерію, а значення «Підозріло» – необхідність звернути увагу на факт невідповідності (наприклад, якщо користувач одночасно відвідує небезпечні сайти, підключає до мережі власний ноутбук, працює на вихідних та встановлює програму з нетиповою) мережевою активністю), що може бути додатковою зовнішньою ознакою для розпізнавання інсайдера.

Відповідно до таблиці 2.3, було сформовано 8 правил політики безпеки (щодо мережної активності користувачів та їх пристроїв), перевірка кожного з яких здійснюється за 2 – 4 критеріями.

Тип дії в позначці до сесії може приймати такі значення, що асоціюються з потенційними атаками:

* 1. DoS атака
  2. SYN-FIN запит
  3. SYN-флуд
  4. Аномальна сесія
  5. Неактуальна версія ОС
  6. Непізнаний користувач
  7. Невідповідність MAC адреси
  8. Невідповідність ОС адреси
  9. Нестандартне завершення сесії
  10. Відсутнє доменне ім'я
  11. Поширення шкідливого коду
  12. Сканування мережі
  13. Збір інформації
  14. Витік інформації
  15. Вразливий пристрій
  16. Фальшиві TCP Reset

Важливість дії у позначці до сесії може набувати наступних значень:

1. Середня – дії є підозрілими, однак вони можуть бути наслідком випадкових збоїв у роботі КС та не бути причиною інсайдерської діяльності.
2. Висока – хоча причиною дій є потенційно інсайдери, проте дії, швидше за все, безпосередньо не призведуть до порушення інформаційної безпеки в КС;
3. Критична – дії можуть призвести до суттєвого порушення інформаційної безпеки в КС та вимагають негайної реакції (від ручного аналізу до автоматичного блокування користувача).

**Основна гілка алгоритму**

Крок 1. Поділ вхідного потоку даних до списку сесій.

Крок 2 Обробка кожної сесії у циклі (лічильник довіреності користувача обнулюється). Після закінчення обробки сесій відбувається вихід із алгоритму. Наступні кроки виконуються послідовно (з викликом підпрограм за умовою).

Крок 3. Перевірити наявність даних Netflow. У разі їхньої присутності запускається Підпрограма A; інакше лічильник збільшується на 3.

Крок 4. Перевірити наявність даних ActiveDirectory. У разі їхньої присутності запускається Підпрограма B; інакше лічильник збільшується на 3.

Крок 5. Перевірити наявність даних RADIUS. У разі їхньої присутності запускається Підпрограма C; інакше лічильник збільшується на 3.

Крок 6. Перевірити наявність даних DHCP. У разі їхньої присутності запускається Підпрограма D; інакше лічильник збільшується на 3.

Крок 7. Перевірити наявність даних DNS. У разі їхньої присутності запускається Підпрограма E; інакше лічильник збільшується на 3.

Крок 8. Перевірка перевищення 3 спроб аутентифікації користувачем. У разі перевищення 10-ти спроб автентифікації до сесії додається позначка “Аномальна з Критичною важливістю” та відбувається перехід на Крок 2. У разі перевищення 3-х спроб, але менше 10 спроб, лічильник збільшується на 1.

Крок 9. Перевірка відвідування користувачем підозрілих сайтів. У разі підтвердження відвідин лічильник збільшується на 1.

Крок 10. Перевірка початку або завершення сесії користувачем у неробочий час. У разі підтвердження цього лічильник збільшується на 1.

Крок 11. Перевірка наявності у користувача програм з підозрілою активністю. У разі підтвердження цього лічильник збільшується на 1.

Крок 12. Перевірка появи нових периферійних пристроїв користувача.

У разі підтвердження цього лічильник збільшується на 1.

Крок 13. Перевірка виявлення нестандартних підключень у користувача.

У разі підтвердження цього лічильник збільшується на 1.

Крок 14. Перевірте підключення користувачем нестандартних пристроїв. У разі підтвердження цього запускається підпрограма F.

Крок 15. Порівняння лічильника з рівнем довіри користувача. Якщо значення лічильника більше або дорівнює рівню довіри користувача, але менше його подвоєного значення, то до сесії додається позначка "Аномальна з Високою важливістю". Якщо значення лічильника більше або дорівнює подвоєного рівня довіри користувача, то до сесії додається позначка “Аномальна з Критичною важливістю”.

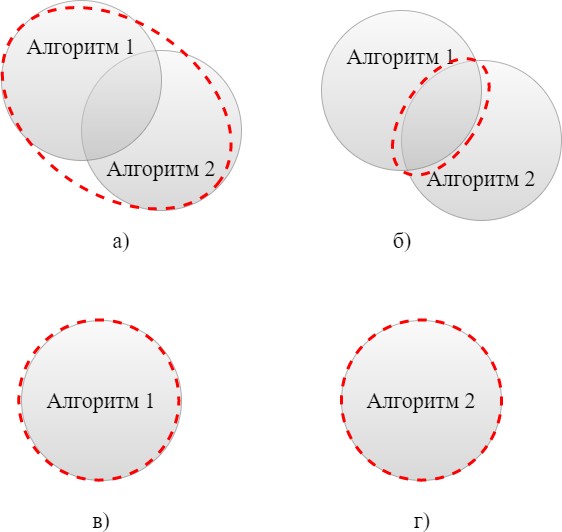
2.3 Модель та алгоритми комбінованого застосування експертних правил та методів машинного навчання на користь виявлення інсайдерських атак

Виходячи з поставлених функціональних вимог, система, що розробляється, повинна поєднувати кілька успішних підходів до виявлення інсайдерів в КС. Цього можна досягти комбінацією різних алгоритмів виявлення інсайдерів в такий спосіб.

Оскільки кожен з алгоритмів на вході має ті самі дані – атрибути поведінки користувачів, а на виході – ідентифікатори виявлених інсайдерів, то можливе їх паралельне виконання з комбінуванням результатів одним із способів. Існує 4 найбільш поширені способи комбінування результатів з позиції роботи з множинами (два останні з яких можна вважати виродженими, але, тим не менш, необхідними для розгляду):

* + 1. об'єднання – результат роботи комплексу включає інсайдерів, виявлених будь-яким з алгоритмів (операція –∨);
    2. перетин – результат роботи комплексу включає інсайдерів, виявлених обома алгоритмами одночасно (операція –∧);
    3. тільки перший – результат роботи комплексу включає інсайдерів, виявлених лише першим з алгоритмів (операція –𝐼);
    4. тільки другий – результат роботи комплексу включає інсайдерів, виявлених тільки другим з алгоритмів (операція –𝐼𝐼).

Графічна інтерпретація способів комбінування наведено на рис. 2.3 (Пунктирною червоною лінією позначений результат комбінування).

Рисунок 2.3 – Графічна інтерпретація способів комбінування: а) об'єднання, б) перетин, в) лише 1-й, г) лише 2-й

Вибір однієї з формул обчислення, пов'язаною з відповідним способом, очевидно, повинен показувати найкращі значення заходів якості роботи системи. Такий обґрунтований вибір буде здійснено за допомогою відповідної експериментальної оцінки.

Схематично, заходи якості *TP, TN, FP, TN* роботи будь-якого алгоритму виявлення інсайдерів можуть бути представлені у графічному вигляді наступним чином (рис. 2.4).

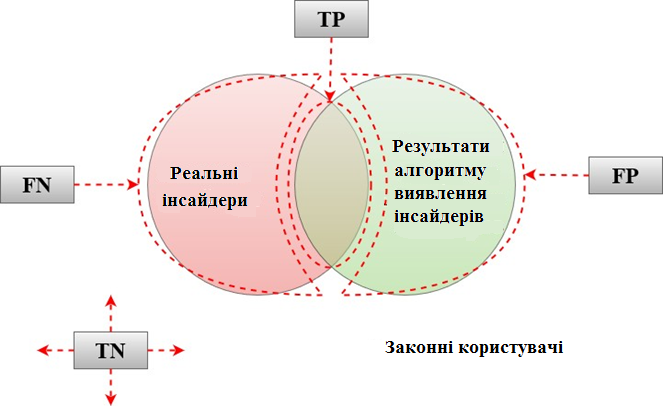


Рисунок 2.4 – Графічна інтерпретація метрик якості алгоритму виявлення інсайдерів

На рис. 2.4 показані дві області інсайдерів: реально діючих у КС (червоне коло) та виявлених алгоритмом (зелене коло); вся біла область навколо кіл відповідає законним користувачам. Таким чином, перетин червоного та зеленого кіл означає правильне спрацьовування алгоритму (заходу *TP*), а відсутність кіл (біла область) – правильне визначення алгоритмом законних користувачів (*TN*); при цьому частина реальних інсайдерів не були виявлені алгоритмом (*FN* або помилка ІІ-го роду – перепустка мети), а частина законних користувачів алгоритм помилково порахував як інсайдерів (*FP* або помилка першого роду - помилкова тривога).

Виходячи з вищесказаного, запропонуємо наступну функціональну структуру комплексу алгоритмів (𝐾𝐴) Виявлення інсайдерів в КС, що складається з двох алгоритмів (𝐴1і 𝐴2), скомбінованих одним з описаних вище способів. Формальний запис комплексу алгоритмів має такий вигляд:



де⊗- операції комбінування, *I* - результат роботи комплексу включає інсайдерів, виявлених тільки першим з алгоритмів, *II* - результат роботи комплексу включає в себе інсайдерів, виявлених тільки другим з алгоритмів,*∨* – результат роботи комплексу включає інсайдерів, виявлених будь-яким з алгоритмів, *∧* – результат роботи комплексу включає інсайдерів, виявлених обома алгоритмами одночасно.

Комбіноване застосування алгоритмів може бути представлене у вигляді моделі, представленої у графічному вигляді на рис. 2.5.

Модель відображає взаємозв'язок наступних сутностей, представлених на рисунку за допомогою 3-х еліптичних областей та асоційовані з інсайдерами: червона – реальні інсайдери в КС (𝐼0), зелена – інсайдери, виявлені алгоритмом на основі експертних правил (𝐼𝑅𝐵), синя – інсайдери, виявлені алгоритмом на основі методів машинного навчання деякого класифікатора (𝐼𝑀𝐿).

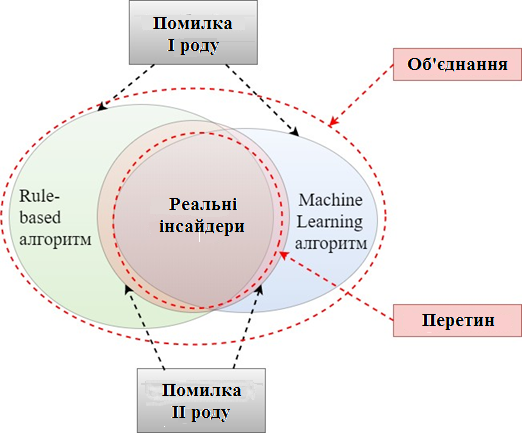


Рисунок 2.5 – Графічна інтерпретація моделі комбінування алгоритмів виявлення інсайдерів у КС

Кожна із зеленої та синьої областей (на рис. 2.5) відповідає окремому результату роботи кожного з алгоритмів, об'єднання цих областей:

* об'єднання результатів роботи алгоритмів, перетин – відповідно до перетину результатів їх роботи. Перетин червоної області з результатом роботи одного із способів комбінування алгоритмів відповідає мірі *TP* – тобто вірно виявленим інсайдерам, а область поза червоною, зеленою та синьою областями відповідає мірі *TN* – тобто користувачам, вірно не віднесеним до інсайдерів. За аналогією, зелена або синя області, що не перетинаються з червоною, відповідають мірі *FP* (або помилці I роду) – тобто інсайдеру, не виявленому алгоритмом; а червона область, що не перетинається з результатом роботи одного із способів комбінування алгоритмів відповідає мірі *FN* (або помилці II роду)
* тобто пропуску інсайдера комплексом.

Очевидно, ідеальною роботою комплексу алгоритмів (тобто результатом 𝐼) буде ситуація, коли або перетин, або об'єднання алгоритмів співпаде з реальними інсайдерами (тобто коли *FP* і *FN* тотожні 0). Однак, така ситуація рідко досяжна через те, що будь-який з алгоритмів може пропускати частину інсайдерів, так і визначати їх неправильно.

**Типові сценарії атак інсайдера.** Як типові сценарії інсайдерських атак були обрані наступні сім, що представляють на думку експертів найбільшу поширеність серед типових атак у КС; також вказані критерії визначення атак:

1. Сканування внутрішніх MAC/IP-адрес та TCP/UDP портів (наприклад, відправлення запитів на з'єднання всіх портів поспіль) – за великою кількістю ехо-запитів до всіх пристроїв мережі та/або їх портів;
2. Відмова в обслуговуванні за допомогою «SYN-флуд» (надсилання великої кількості SYN-запитів сервісу за короткий період) – за підрахунком кількості та часу відправлених SYN-запитів;
3. Невдала спроба входу до сервісу через HTTP/FTP (наприклад, більше 5 відмов аутентифікації протягом 1 хвилини) – за відповідями сервера ААА;
4. Аномальне отримання надмірно великої кількості даних із внутрішніх ресурсів організації (наприклад, отримання протягом одного дня 10Гб трафіку, якщо за попередні 6 місяців виходило 100Мб даних на день) – за різким підвищенням кількості відправлених даних порівняно з середньостатистичними за період;
5. Аномальне надсилання надмірно великої кількості даних поза периметром організації (наприклад, відправка протягом одного дня 10Гб трафіку, якщо за попередні 6 місяців відправлялося 100Мб даних на день) – за різким підвищенням кількості отриманих даних у порівнянні з середньостатистичними за період;
6. Виконання шести етапів: очікування на неробочий час (наприклад, коли відсутні інші співробітники); підключення до мережі нового пристрою (наприклад, власного ноутбука) через гостьовий WiFi; вхід до системи аутентифікації з першої спроби з чужого облікового запису (тобто легального користувача); завантаження помірно великого обсягу інформації на підключений пристрій з внутрішніх ресурсів мережі (наприклад, отримання протягом однієї години 2 Гб трафіку, якщо за попередній період протягом 6 місяців виходило по 1 Гб даних на день); відсутність активності протягом деякого часу (наприклад, протягом однієї години); відключення пристрою від мережі – за цілою низкою ознак про мережеву активність, роботу сервера аутентифікації тощо, а також їх закономірності;
7. Виконання шести етапів: очікування робочого часу (тобто виконання працівником своїх посадових обов'язків); вхід до системи аутентифікації з першої спроби (тобто використання облікового запису легального користувача); запуск на власному комп'ютері програми пошуку та отримання персональних даних у мережі організації; завантаження помірно великого обсягу інформації на комп'ютер мережі з внутрішніх ресурсів; створення зашифрованого каналу передачі даних поза периметра організації; надсилання завантажених даних по створеному каналу на зовнішню IP адресу, що відноситься до розряду підозрілих (наприклад, розташований в іншій країні або належить конкуруючій організації).

2.4 Висновки до розділу 2

Подано підхід до побудови системи аналізу поведінки користувачів у комп'ютерній мережі організації.

Створено модель представлення великих даних про атаки інсайдерів у форматі NoSQL, що включає модель інсайдера.

Обґрунтовано вибір класифікаторів для роботи алгоритму на основі методів машинного навчання, включаючи їхню комбінацію.

Розроблено модель та комплекс алгоритмів виявлення інсайдерів у комп'ютерній мережі на основі експертних правил та методів машинного навчання.

Запропоновано схему обчислень результату роботи комплексу алгоритмів виявлення інсайдерів.

Описано типові сценарії інсайдерських атак, що складаються з трьох простих, двох складних та двох комплексних, які можуть бути використані для тестування алгоритмів виявлення інсайдерів у КС.

МЕТОДИКА, АРХІТЕКТУРА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИЯВЛЕННЯ ІНСАЙДЕРІВ У КОМП’ЮТЕРНИХ СИСТЕМАХ

3. 1 Методика виявлення інсайдерів у комп’ютерних системах

Запропонована методика виявлення інсайдерів у КС з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних визначає основні етапи та кроки використання розроблених моделей та алгоритмів.

Методика виявлення інсайдерів у КС ґрунтується на процесі збору даних про асоційовану з користувачами мережну активність, розпаралелену попередню обробку даних з подальшим застосуванням алгоритмів на основі експертних правил та методів машинного навчання, а також остаточне виведення результатів аналізу в людино-орієнтованому вигляді. Методика заснована на трьох наступних етапах:

Етап 1. Збір інформації та налаштування параметрів.

Етап 2. Застосування алгоритмів виявлення інсайдерів. Етап 3. Аналіз вихідних даних.

Кожен елемент методики асоційований з діями одного з учасників: оператора або системи виявлення; також зазначені відповідності дій системи з компонентами, що їх реалізують.

Опишемо етапи методики докладніше.

Етап 1. Збір інформації та налаштування параметрів

На даному етапі відбувається збір інформації про мережевий трафік КС у відповідному для аналізу вигляді з наступним налаштуванням параметрів системи. Етап може бути поділений на наступні підетапи:

* формулювання завдання дослідження КС та визначення параметрів, за якими вона досліджуватиметься;
* вибір параметрів роботи системи, що дозволяє оператору вказати класифікатор для роботи методу машинного навчання, вибравши відповідний метод із набору реалізованих, а також комбінацію результатів роботи алгоритмів на основі експертних правил та методів машинного навчання;
* запуск процесу збирання інформації системою виявлення з серверів AAA, AD, DHCP та DNS; для збору використовуються відповідні агенти системи виявлення, що збирають повідомлення системних журналів, міжмережевих екранів та сторонніх програм, одержують дані з сенсорів і датчиків, що накопичують інформацію про завантаження мережі та навантаження хостів, а також реєструючі повідомлення про порушення інформаційної безпеки;
* коригування даних оператором, що дозволяє внести деякі коригування в зібрані дані збільшення точності роботи алгоритмів виявлення;
* підсумкове формування поведінки алгоритмів виявлення інсайдерів (за допомогою компонентів системи виявлення, що забезпечують балансування навантаження), а також збереження інформації в базі даних (за допомогою відповідних компонентів роботи з БД).

Етап 2. Застосування алгоритмів виявлення інсайдерів

На цьому етапі відбувається виявлення інсайдерів за допомогою розробленого комплексу алгоритмів, реалізованих у системі виявлення. Як вихідні дані використовуються дані, зібрані на Етапі 1. Етап 2 може бути поділений на наступні підетапи:

* побудова середовища для роботи алгоритмів після ручного запуску процесу оператором;
* виконання MapReduce для розпаралеленої обробки на декількох комп'ютерах з метою попередньої обробки даних (підрахунок кількості сесій, IP-пакетів, хостів тощо);
* занесення результатів обробки MapReduce до бази даних для оперативної роботи з ними алгоритмів виявлення інсайдерів;
* паралельний запуск алгоритмів із комплексу: на основі експертних правил (Rule-based) та методів машинного навчання (Machine learning);
* порівняння результатів роботи алгоритмів (об'єднання, перетин або вибір одного) для визначення варіації з найкращими показниками якості, за якою проводиться ідентифікація інсайдерів;
* Протягом роботи етапу 2 для роботи з MapReduce використовуються компоненти кореляції та індексування, для збереження результатів – компоненти роботи з базою даних.

Етап 3. Аналіз вихідних даних

На даному етапі відбувається безпосереднє виведення результатів оператора, який був отриманий на попередньому етапі. Етап може бути поділений на наступні підетапи, що виконуються:

* формування звіту, що систематизує та класифікує знайдених інсайдерів, включаючи позначки до сесій, зроблені алгоритмом на основі експертних правил;
* відображення результатів;
* збереження даних, що дозволяє ознайомлюватися з отриманими результатами;
* протягом роботи етапу для збереження результатів використовуються компоненти роботи з базою даних.

Для роботи методики необхідно: використання агентів збору інформації про функціонування КС, підтримка бази даних, можливість розподілених обчислень, налаштований метод машинного навчання (на наборах типової та інсайдерської поведінки користувачів), а також оболонка для візуалізації звітів.

Таким чином, вхідними даними методики є інформація про функціонування КС, проміжними даними – заповнена реальними даними модель представлення великих даних у форматі NoSQL, а вихідними даними – звіт про виявлені інсайдери.

Важливою особливістю методики є її налаштування під точні вимоги оператора шляхом виконання кроку першого етапу "Вибір параметрів роботи системи", суть якої полягає в наступному - результати вибору параметрів системи на Етапі 1 безпосередньо впливають на роботу елементів системи на Етапі 2.

Метод машинного навчання, застосований у методиці, може використовувати один із 8-ми класифікаторів, описаних раніше: DT, NB, k-NN, SVM, PV, WV, SV, Adaboost (перші 4 класифікатори є базовими, а останні 4 – їх комбінацією). Результати роботи алгоритмів на основі експертних правил і методів машинного навчання також можуть комбінуватися наступним чином: об'єднання, перетин, тільки 1-й, 2-й. Вибір класифікатора та підсумкової комбінації результатів впливає на якість виявлення інсайдерів, заходи якого були визначені як r, p, a, e, f. Отже, можливі такі різні групи заходів якості: 1 – під час роботи лише алгоритму з урахуванням експертних правил, 8 – під час роботи лише методу машинного навчання (для заданого класифікатора), та по 8 – для об'єднання та перетину їх результатів (1 алгоритм для кожного з 8-ми класифікаторів методу). Кожна з 25 груп (1+ 8 + 8 \* 2) матиме власні значення заходів, які можуть мати різну значущість для оператора. І хоча класичної, що використовується також у роботи, є F-міра (f), тим не менш, для інших випадків інші заходи можуть мати більш пріоритетне значення.

Кожен із заходів може бути обраний як визначальний для свого завдання: повнота – важливим є те, скільки з перевірених користувачів ми визначили, як інсайдерів; точність – важливим і те, скільки з виявлених нами інсайдерів реально є такими; акуратність – важливим є те, якою є частка правильних передбачень інсайдерів та законних користувачів серед усіх, помилка – коли важливим є те, якою є частка неправильних передбачень інсайдерів та законних користувачів серед усіх розглянутих. Природно, оскільки дані відносні заходи (мають сенс часток або ймовірностей) обчислюються на підставі абсолютних – TP, TN, FP та FN, – останні також можуть бути використані як критерій важливості; однак, робота з абсолютними значеннями не завжди є доцільною.

Розглянемо застосування розроблених моделей та алгоритмів, описаних раніше більш докладно у методиці виявлення інсайдерів у КС.

На етапі збору інформації:

* зібрані дані щодо поведінки користувачів поміщаються в модель уявлення великих даних про інсайдерські атаки для подальшої обробки;
* оператор проводить коригування вхідних даних, що беруться з моделі представлення великих даних про інсайдерські атаки;
* кориговані оператором дані зберігаються у базі даних; На етапі застосування алгоритмів виявлення інсайдерів:
* вихідні дані обробки за допомогою алгоритму розподілених обчислень MapReduce беруться з моделі бази даних;
* результати обробки алгоритмом розподілених обчислень MapReduce зберігаються у базі даних;
* усі вихідні дані, що надаються алгоритмам виявлення інсайдерів у КС, беруться із бази даних;
* обробка зібраних даних щодо поведінки користувача здійснюється алгоритмом на основі експертних правил;
* обробка зібраних даних про поведінку користувача здійснюється комплексом алгоритмів на основі експертних правил та методів машинного навчання;
* результати спільної обробки зібраних даних, а також ідентифіковані інсайдери зберігаються у базі даних;

На етапі аналізу вихідних даних:

* формування звіту для оператора проводиться на підставі даних про інсайдерську діяльність, занесених до бази даних алгоритмами виявлення;
* відображення результатів проводиться на підставі даних, що зберігаються в базі даних;
* фінальні дані за звітами та інша статистична інформація (час проведення методики, коригування оператора тощо) зберігаються у базі даних.

Одним із найважливіших елементів методики є застосування моделі MapReduce, призначеної для створення фреймворку для паралельних обчислень над великими даними. Також, методика включає запропоновані алгоритми і моделі, орієнтовані працювати з великими даними. Крім того, на останньому етапі методики за допомогою графів відбувається візуалізація великої кількості аналітичних даних - записів з моделі уявлення великих даних про інсайдерські атаки, - що входить у реалізацію бази даних OrientDB, що використовується для цього, і може бути віднесено до методів і технік аналізу великих даних.

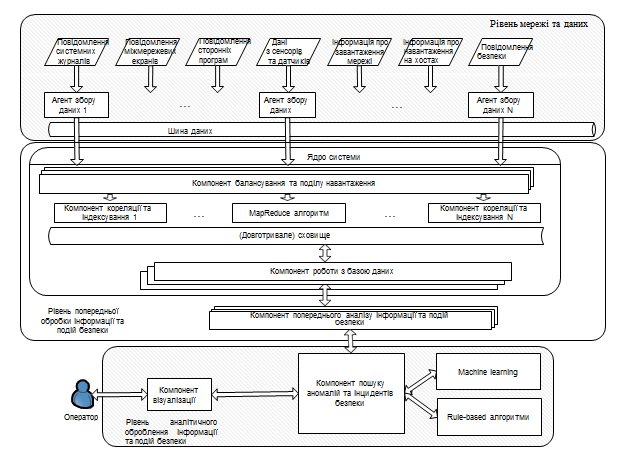
3.2 Архітектура та програмна реалізація системи виявлення інсайдерів у комп’ютерних системах

Наведемо опис компонентів кожного з рівнів та їх взаємодії. Рівень мережі та даних містить компоненти для збирання повідомлень та іншої інформації від багатьох джерел. До перших належать такі: повідомлення із системних журналів, що включають дані про час створення повідомлень та їх важливість; повідомлення із системних журналів міжмережевих екранів, що включають дані про TCP- та UDP-сесії (номер сесії, прапори TCP-повідомлень, час відкриття сесії, час завершення сесії); дані від сторонніх програм, наприклад, відомості про потенційно небезпечні програми від антивірусних програм. До інших відносяться: дані з сенсорів та датчиків – кількість підключених пристроїв, кількість портів, що використовуються, а також інформація про завантаження мережі – дані про кількість переданого та отриманого трафіку, статистика за використовуваними програмами; дані про навантаження на хостах, включаючи відомості про завантаження процесора, кількість запущених програм, завантаження жорсткого диска, завантаження оперативної пам'яті.

З кожним збирачем інформації пов'язаний окремий компонент рівня – агент збору даних, що перетворює інформацію на єдиний вид. Так, наприклад, агент для повідомлень системних журналів здійснює перетворення повідомлень з формату Syslog у формат csv, агент для даних із сенсорів та датчиків – забезпечує роздільний збір отриманої інформації за такими категоріями: кількість підключених пристроїв, кількість портів, що використовуються і т.д.

Отримана інформація відправляється на окремий компонент рівня – шину даних, призначену для поширення даних про події безпеки та їх гарантовану доставку. Через велику кількість вхідних даних можливі навантаження системи, для запобігання чого, зокрема, призначений наступний рівень.

Першим на рівні попередньої обробки інформації та подій безпеки розташований компонент балансування та поділу навантаження, що забезпечує рівномірну обробку інформації, зібраної датчиками на попередньому рівні. Цей компонент забезпечує розподіл інформації між рештою компонентів: кілька компонентів кореляції та індексування, включаючи перетворення даних за допомогою парадигми MapReduce. MapReduce забезпечує роботу розподілених обчислень над великими даними, що збираються, і складається з трьох кроків: класифікації даних, попередньої обробки зібраної інформації та їх згортки. Все це забезпечує довготривале зберігання даних (шляхом використання відповідного компонента).



Компонент роботи з базою даних

Компонент роботи з базою даних

Рисунок 3.1 – Архітектура системи виявлення інсайдерів на основі обробки мережевого трафіку

Отримані таким чином дані заносяться до бази даних, забезпечену відповідним компонентом рівня. Робота бази даних ґрунтується на запропонованій моделі уявлення великих даних про інсайдерські атаки. Також, з базою даних працює компонент попереднього аналізу даних та подій безпеки, який дозволяє зібрати необхідну вибірку подій та зробити первинний аналіз отриманої інформації для подальшого надання компонентам рівня аналітичної обробки інформації та подій безпеки.

Наступним здійснює роботу рівень аналітичної обробки інформації та подій безпеки, який можна вважати основним з точки зору виявлення інсайдерів, оскільки він містить всю логіку роботи алгоритмів, побудованих на базі експертних правил і методів машинного навчання. Рівень складається з чотирьох основних компонентів: пошуку аномалій та інцидентів безпеки; алгоритму на основі експертних правил, алгоритму на основі методів машинного навчання та компоненту візуалізації.

Перший компонент забезпечує узгоджену роботу алгоритмів у складі комплексу – підготовку, налаштування (наприклад, вибір класифікатора для методу машинного навчання) та подання в них даних, а також паралельне обчислення та узгодження результатів (наприклад, їх об'єднання).

Другий та третій компоненти забезпечують роботу алгоритмів, що входять до комплексу. З цього погляду архітектура може бути розширюваною за рахунок додавання нових алгоритмів, побудованих на базі експертних правил та машинного навчання, крім тих, що реалізовані на даний момент.

Четвертий компонент реалізує інтерфейс взаємодії із користувачем. Так, останній може налаштувати роботу комплексу алгоритмів (вибрати спосіб узгодження результатів та класифікатор для машинного навчання відповідно до отриманих заходів якості, наприклад, обравши їх перетин, а не об'єднання, а також класифікатор Adaboost). Внаслідок роботи системи виявлення для запропонованої архітектури оператор отримає звіт, що містить ідентифікатори виявлених інсайдерів, позначки про тип та важливість інсайдерської атаки та іншу інформацію.

Відповідно до розробленої архітектури був реалізований прототип системи виявлення інсайдерів у КС, що застосовується у відповідній методиці. Для перевірки працездатності прототипу та методики, а також для оцінки їх характеристик буде проведено відповідний експеримент.

Реалізація архітектури системи забезпечує роботу всіх її компонентів

* моделей, алгоритмів, методики, а отже побудована на утилітах, бібліотеках і фреймворках, призначених для роботи з великими даними. Крім того, для роботи програмного прототипу системи використовується інструментарій Hadoop та файлова система HDFS, що спочатку спроектовані для підтримки великих даних.

**Програмний прототип системи.** Для запуску програмного прототипу використано спеціальний стенд. При міжмережній взаємодії пристрої, що знаходяться у внутрішній мережі університету, взаємодіють з комутаторами, які копіюють трафік, що проходить через них, що генерується користувачами в КС на порти віртуальних машин в середовищі VMware vSphere (ESXi 6.5). Ці віртуальні машини складають скоординований кластер під управлінням операційних систем CentOS 7 та з встановленими на них продуктами компанії Apache Hadoop з реалізацією Cloudera – Apache Ambari. Кластер має такі характеристики: 18vCPU 1.2 GHz, 48 GB RAM, 1,2 TB HDD. П'ять комп'ютерів кластера виступають у ролі DataNode та відповідають за зберігання та обробку даних, один комп'ютер – NameNode – є менеджером для розподілу завдань та навантажень кластера, також зберігає таблиці імен файлів. Крім того, для виявлення інсайдера за допомогою алгоритму на основі експертних правил додатково використовуються дані, що надходять із сервера автентифікації авторизації та обліку, що розгорнуто на базі рішення Cisco ISE версії 2.0.

У наявному трафіку містяться дані мережевої активності користувачів мережі університету, серед яких присутні особливі учасники – інсайдери, тобто користувачі, які мають на меті завдати шкоди організації через свою діяльність у мережі (згідно з запропонованими сценаріями атак).

**Приклад роботи системи прототипу.** Потрапивши на кластер, дані піддаються обробці алгоритмом MapReduce, що дозволяє швидко розраховувати кількість входжень необхідних міток і сортування інформації в зручний вигляд. З бази даних NoSQL OriendDB оброблені дані проходять через алгоритм на основі методів машинного навчання (нормалізація, виділення ознак, кластеризація, класифікація, оцінка ефективності, підсумковий висновок) та алгоритму, що базується на експертних правилах.

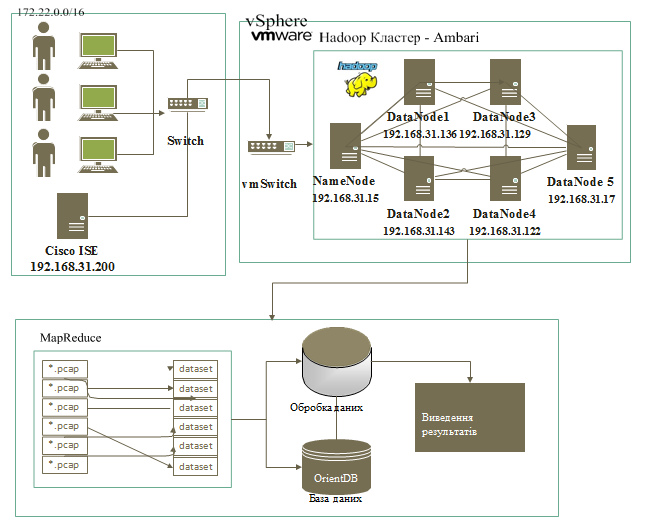
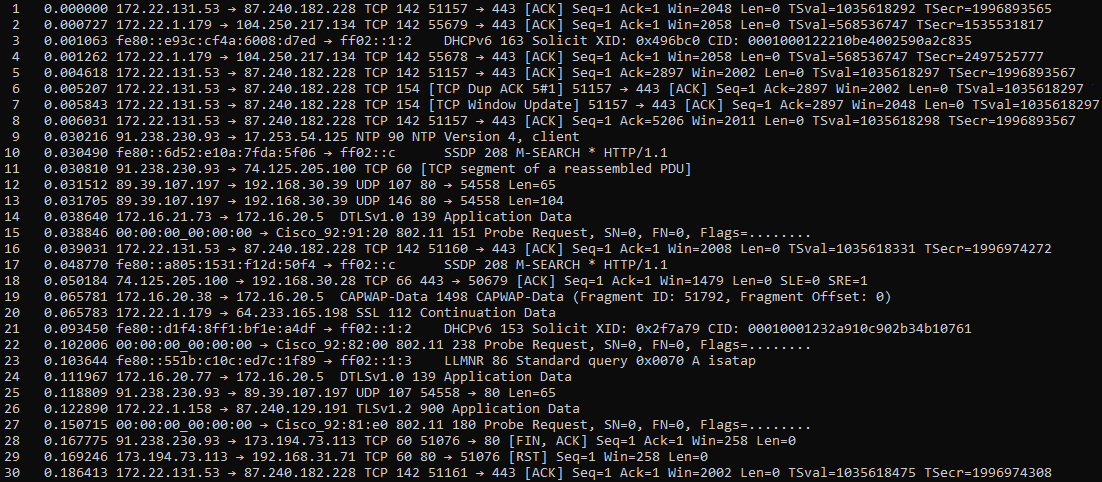


Рисунок 3.2 – Прототип програмного апаратного комплексу обробки трафіку

Як джерело даних виступають файли, що генеруються Wireshark, що мають розширення ".pcapng". Процес конвертації і двох етапів.

 Рисунок 3.3 – Дані на виході аналізатора пакетів tshark

На першому етапі відбувається зчитування дампи, що зберігається у файлах.pcapng. Оскільки файли .pcapng є бінарними, необхідно їх зчитування застосовувати аналізатор пакетів tshark, на виході якого виходять дані, представлені рис. 3.3.

Далі ці дані обробляються за допомогою програми, написаної мовою програмування python, на виході якої вони набувають вигляду, представленого на рис. 3.4. Отримані в такий спосіб дані записуються в csv-файл.

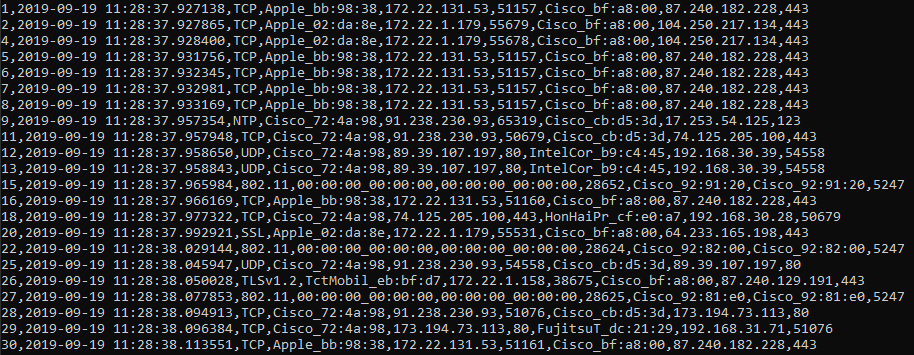


Рисунок 3.4 – Дані на виході програми, написаної мовою python

У цьому прикладі наведено значення дев'яти полів для тридцяти пакетів:

* порядковий номер пакета (нумерація починається кожного файла pcap, разом із ім'ям файла pcap це дозволяє однозначно ідентифікувати кожен пакет під час занесення їх у базу даних);
* час відправки;
* протокол;
* MAC-адреса відправника;
* IP-адреса відправника;
* порт відправника;
* MAC-адреса одержувача;
* IP-адреса одержувача;
* порт отримувача.

На рис. 3.5 представлено візуальне відображення взаємозв'язків між вибіркою IP-адрес, що включає 100 IP-адрес відправників і одержувачів трафіку. Цей рисунок був отриманий шляхом візуалізації вибірки за допомогою Apache Superset, встановленого на Apache Ambari. З рисунку видно, що найбільша кількість IP-з'єднань між IP-адресами 192.168.31.44 і 87.240.185.226. Це пояснюється тим, що за адресою 192.168.31.44 знаходиться кафедральна інфраструктура. Крім того, загальна кількість зв'язків з IP-адресою 172.16.228.22 перевищує середню кількість взаємозв'язків між IP-адресами у вибірці в 40 разів. Цей факт може свідчити про можливу DDoS атаку.

На рис. 3.6 представлено співвідношення типів трафіку. З рисунка видно, що TCP трафік займає найбільшу частку – близько 66%, TLSv1.2 – 12%, а 802.11 – 7% та UDP – 6%.

Алгоритми на основі експертних правил та методів машинного навчання реалізовані мовою Python та виконуються розподілено на DataNode-вузлах кластера.

3.3 Висновки до третього розділу

Запропоновано методику виявлення інсайдерів у КС, що використовує методи машинного навчання та обробки великих даних, що складається з послідовності етапів та їх кроків, що описують дії оператора та системи виявлення інсайдерів.

Розроблено архітектуру системи виявлення інсайдерів у КС, що забезпечує роботу відповідної методики; також реалізовано програмний прототип системи виявлення інсайдерів у КС.

Вибрано існуючі системи виявлення інсайдерів, близькі за функціоналом до розробленої, порівняння з якими дозволило визначити місце серед аналогів.

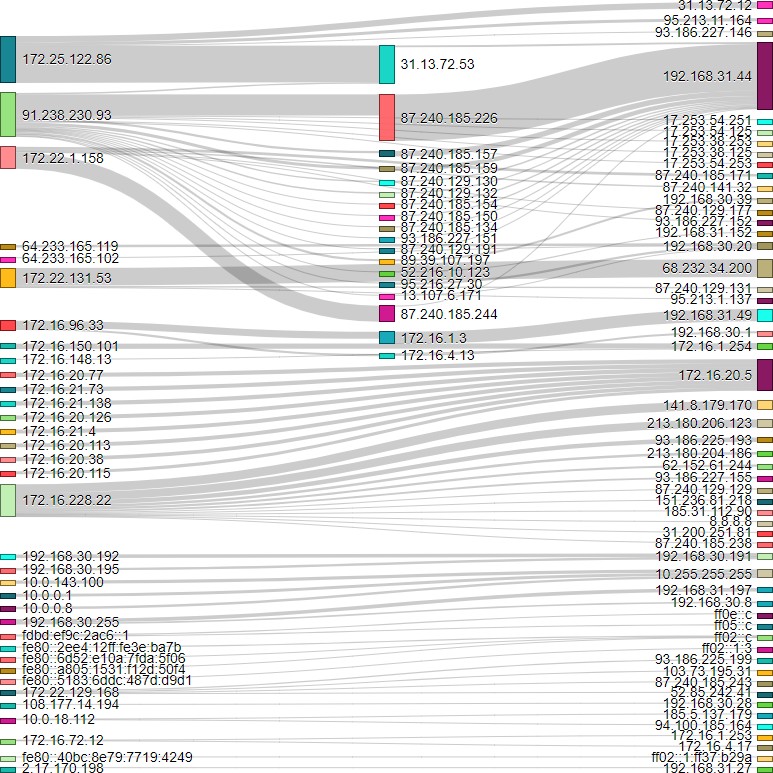


Рисунок 3.5 – Взаємозв'язки IP-адрес

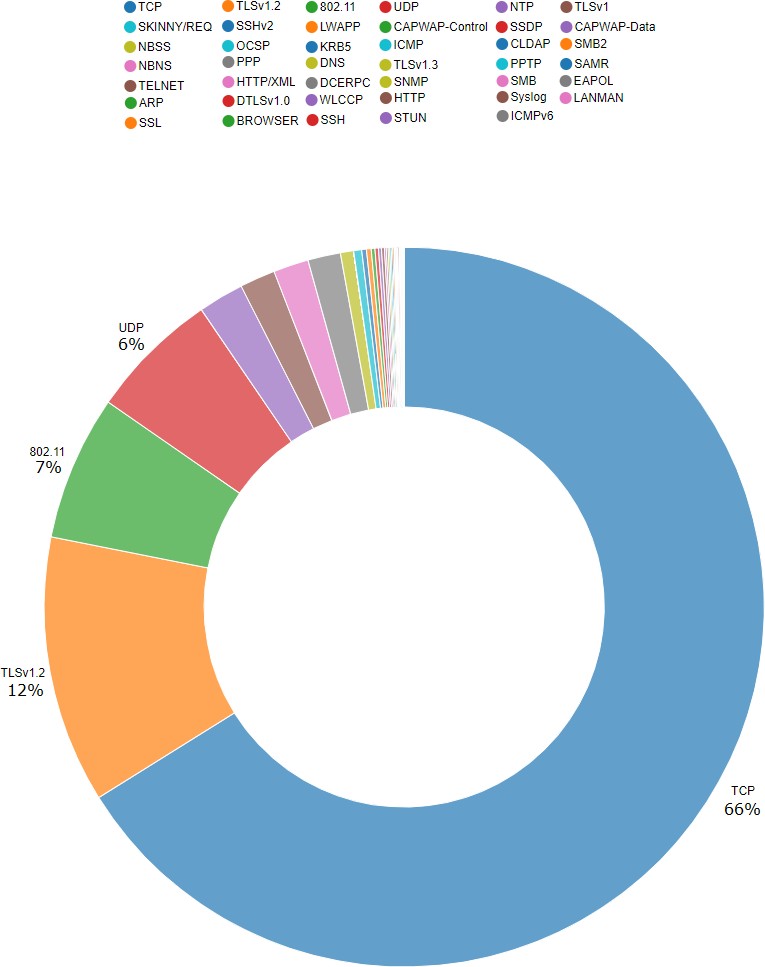


Рисунок 3.6 – Співвідношення протоколів у вибірці

ЕКСПЕРИМЕНТАЛЬНА ОЦІНКА РОЗРОБЛЕНОЇ МЕТОДИКИ ТА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СИСТЕМИ ВИЯВЛЕННЯ ІНСАЙДЕРІВ У КОМП’ЮТЕРНИХ СИСТЕМАХ

4.1 Вибір наявних аналогів систем виявлення інсайдерів

Зробимо вибір систем, близьких до розроблюваної та порівняємо їх ефективність. Поняття ефективності системи або процесу є досить багатогранним, що має різні трактування та способи обчислення. Досить відомим, що показало хорошу застосування на практиці визначенням ефективності, вважається сукупність трьох її показників – своєчасність, обґрунтованість та ресурсоспоживання; для лаконічності застосування, зручніше замість останнього іноді використовувати протилежний показник – ресурсомісткість, визначаючи таким чином загальне підвищення ефективності як підвищення всіх чи низки її показників. Особливість такого визначення полягає в тому, що підвищення одного з властивостей (без додаткових заходів) постійно веде до зниження іншого. Так, виявлення більшої кількості інсайдерів (підвищення обґрунтованості) може бути отримано за рахунок зниження швидкості виявлення (зниження своєчасності) та/або витрачання більшої кількості ресурсів (підвищення ресурсоспоживання). Отже, підвищення будь-якого з параметрів за умови збереження інших однозначно означатиме загальне підвищення ефективності системи. Цей принцип і буде використаний як основний критерій досягнення мети дослідження. Також, оскільки обґрунтованість системи не може розглядатися окремо від якості досягнення поставленого завдання, будемо під нею розглядати сукупність введених заходів: *r, p, a, e* та *f*. підвищення будь-якого з параметрів за умови збереження інших однозначно означатиме загальне підвищення ефективності системи. Цей принцип і буде використаний як основний критерій досягнення мети дослідження. Також, оскільки обґрунтованість системи не може розглядатися окремо від якості досягнення поставленого завдання, будемо під нею розглядати сукупність введених заходів: *r, p, a, e* та *f*. підвищення будь-якого з параметрів за умови збереження інших однозначно означатиме загальне підвищення ефективності системи. Цей принцип і буде використаний як основний критерій досягнення мети дослідження. Також, оскільки обґрунтованість системи не може розглядатися окремо від якості досягнення поставленого завдання, будемо під нею розглядати сукупність введених заходів: *r, p, a, e* та *f*.

Для порівняння показника обґрунтованості розробленої системи було обрано такі альтернативні системи.

**Cisco StealthWatch.** Компанія Cisco Systems Inc. по праву можна вважати одним із лідерів з виробництва телекомунікаційного обладнання. Як наслідок, вона також пропонує відповідні рішення в галузі інформаційної безпеки, одним з яких є Cisco StealthWatch. Цей продукт призначений для аналізу мережевого трафіку на наявність загроз інформаційній безпеці, включаючи аналіз різних пристроїв та сервісів у КС (маршрутизатори, сервери, віртуальні машини, користувацькі пристрої та ін.). Результатом обробки трафіку може бути виявлення різних аномалій у ньому, включаючи інсайдерські атаки. Основними можливостями продукту є такі:

* + 1. Виявлення активності інсайдерської діяльності (наприклад, сканування портів).
    2. Виявлення взаємодії заражених хостів із хостами зловмисника.
    3. Детектування некоректних мережних пакетів.
    4. Виявлення аномалій у мережевому трафіку.
    5. Перевірка виконання політик безпеки.

Узагальнена схема компонентів продукту представлена ​​рис. 4.1.

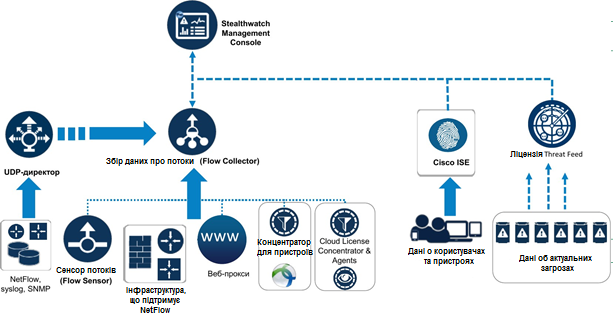


Рисунок 4.1 – Схема компонентів продукту Cisco StealthWatch

**PacketFence.**Альтернативою комерційним рішенням є рішення з відкритим вихідним кодом (Open Source продукти). Зокрема, одним із найбільш затребуваних у галузі інформаційної безпеки КС є рішення PacketFence, призначене для забезпечення контролю доступу до мережі. Можливості продукту схожі на Cisco StealthWatch і можуть бути доповнені такими функціями:

* облік та реєстрація нових пристроїв у мережі.
* виявлення аномального трафіку, пов'язаного з потенційно ворожою активністю.
* автоматична або ручна ізоляція проблемних хостів.
* вбудовані механізми пошуку уразливостей.

Аналогічно Cisco StealthWatch, даний продукт може бути використаний як у невеликих, так і у великих гетерогенних мережах. Мережева архітектура продукту представлена ​​на рис. 4.2.

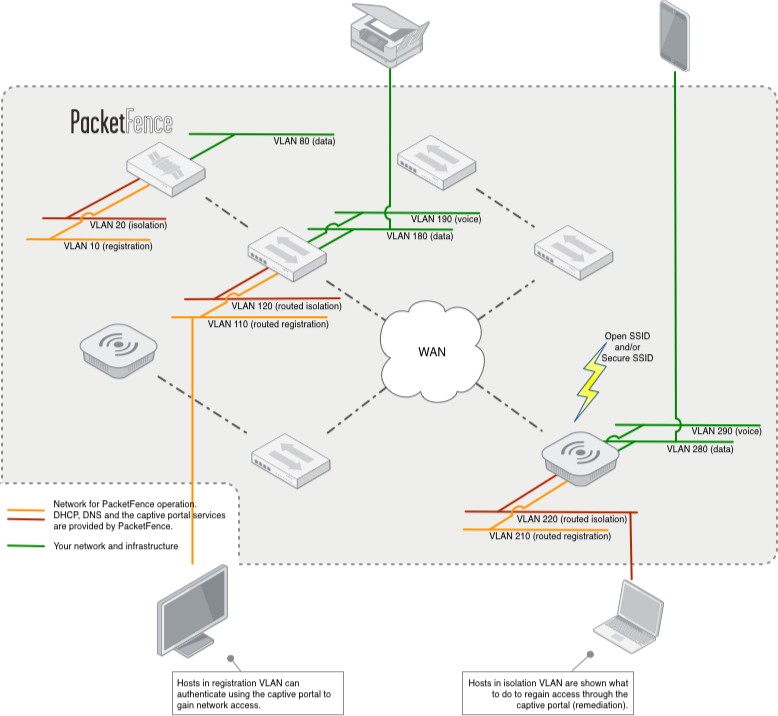


Рисунок 4.2 – Мережева архітектура PacketFence

Згідно з описом продуктів, кожен з них може бути застосований для вирішення поставленої задачі виявлення інсайдерів в КС і, отже, є найближчим аналогом системи, що розробляється.

4.2 Порівняння варіацій застосування алгоритмів

Перш ніж порівнювати ефективність розробленої системи виявлення інсайдерів з найближчими аналогами, необхідно вибрати найкращу варіацію алгоритму на основі експертних правил і методів машинного навчання, на яку впливає формула обчислення кінцевого результату вирішення задачі за отриманими результуючими множинами – їх об'єднання, перетин або вибір найкращого класифікаторів машинного навчання

Функціональна схема складається з наступних етапів та кроків:

Етап 1. Підготовка стенду

Крок 1.1. Вибрати 𝑁𝑆𝑐𝑒𝑛𝑎𝑟y типових сценаріїв атак, на яких буде проведено експериментальну оцінку.

Крок 1.2. Почати налаштування стенду для експерименту.

Крок 1.3. Налаштувати мережеве оточення.

Крок 1.4. Налаштувати генератор мережевих атак.

Крок 1.5. Налаштувати пристрої збирання мережевої інформації.

Етап 2. Налаштування алгоритмів

Крок 2.1. Згенерувати великий обсяг типового трафіку легальних користувачів.

Крок 2.2. Почати виконання кожного з 𝑁𝑆𝑐𝑒𝑛𝑎𝑟y типових сценаріїв атак.

Крок 2.3. Згенерувати мережевий трафік інсайдерів за кожним зі сценаріїв.

Крок 2.4. Вручну проаналізувати мережевий трафік та виявити мережеві сесії, пов'язані з інсайдерською діяльністю за кожним зі сценаріїв.

Крок 2.5. Почати налаштування методу машинного навчання, використовуючи згенерований мережевий трафік та виявлені у ньому сесії, пов'язані з атаками інсайдерів.

Крок 2.6. Здійснити налаштування методу машинного навчання.

Етап 3. Проведення вимірів

Крок 3.1. Розпочати процес вимірювань.

Крок 3.2. Згенерувати великий обсяг типового мережевого трафіку законних користувачів.

Крок 3.3. Згенерувати мережевий трафік інсайдерів по кожному із сценаріїв.

Крок 3.4. Запустити програмний комплекс системи виявлення інсайдерів у КС.

Крок 3.5. Здійснити відпрацювання всіх елементів програмного комплексу:

* збирання мережевої інформації;
* застосування алгоритму MapReduce;
* зберігання інформації у базі даних;
* виконання алгоритму з урахуванням експертних правил;
* виконання методу машинного навчання для кожного з його восьми класифікаторів;
* комбінування результатів роботи алгоритму на основі експертних правил та методів машинного навчання (25 варіацій): лише алгоритм – 1, лише метод – 8, перетин для алгоритму та методів – 8; об'єднання для алгоритму та методів – 8;

Крок 3.6. Обчислення заходів якості (повнота, точність, акуратність, помилка, F-міра) кожної з варіацій.

Крок 3.7. Порівняння та вибір найкращої варіації щодо сукупності заходів якості.

Таким чином, обрана варіація застосування алгоритмів та класифікаторів буде вважатися підсумковою для використання у методиці.

Зазначимо, що Етапи 1 і 2 необхідні для навчання другого алгоритму з комплексу і повинні бути проведені не тільки в рамках експерименту, але і для налаштування системи, що розробляється з метою її подальшого використання.

Інформаційна схема експерименту, тобто взаємозв'язок вихідних, проміжних і результуючих даних, що відповідає описаній функціональній схемі, представлена ​​на рис. 4.3.

Схема була реалізована на основі стенду з архітектурою, що складається з наступних компонентів:

1. Робоче місце оператора, що виконує запуск, керування та аналіз експерименту.
2. Сканер мережних пакетів.
3. Генератори сценаріїв мережевих атак.
4. Розроблена система виявлення інсайдерів у КС.

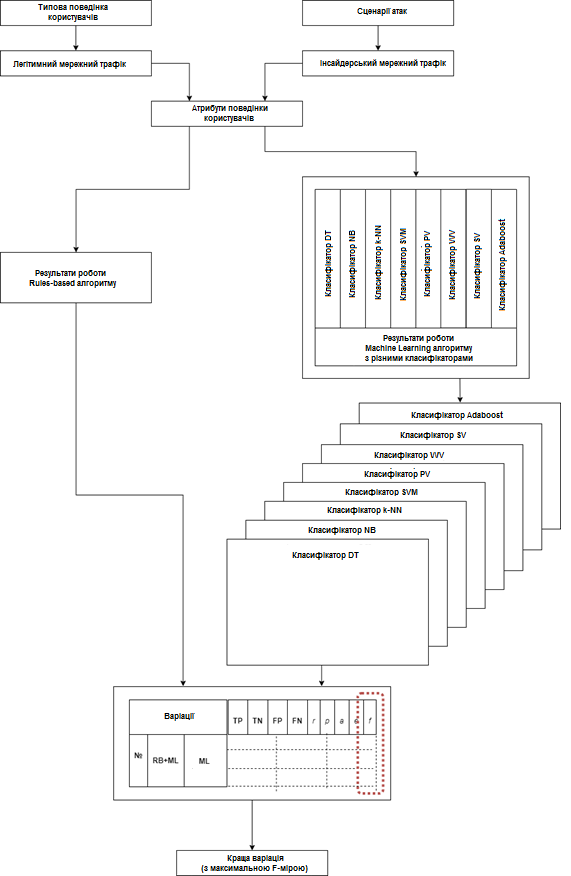


Рисунок 4.3 – Інформаційна схема експерименту щодо оцінки заходів якості системи виявлення інсайдерів у КС

Для налаштування роботи алгоритму на основі експертних правил граничне значення, що вказує ступінь довіри до користувача, було обрано рівним трьом (3 = 3). Так, у разі задоволення всіх умов алгоритму на базі експертних правил: відвідування підозрілих сайтів, початок або завершення сесії в неробочий час, наявність програми з підозрілою активністю, наявність нового периферійного пристрою, наявність нестандартних підключень, наявність нестандартного пристрою – лічильник (Counter) дорівнюватиме семи, у результаті сесія отримає позначку “Важливість – Критична”; у разі задоволення більше половини умов (Counter = 4, 5 чи 6) сесія отримає позначку – “Важливість – Висока”.

Налаштування методів машинного навчання проводилося так. Як навчальної вибірки було взято 100 000 записів, у тому числі 70 000 (тобто. 70%) відповідали законному трафіку користувачів, а 30 000 (тобто. 30%) пов'язані з інсайдерськими атаками. Експеримент з виявлення інсайдерів проводився на вибірці даних, що складається з 20 000 записів (тобто 20% від навчальної вибірки), число записів, що належать до інсайдерської діяльності, становило 10 000 (тобто 50%).

Також, сценарії атак були поділені на дві групи тестування: до першої увійшли 3 простих та 2 складних, а до другої – 2 комплексних. Такий поділ був пов'язаний із припущенням того, що найкраща якість роботи різних варіацій алгоритмів буде досягнута саме у разі комплексної атаки, що важко описується одним підходом до виявлення інсайдерів.

Результати проведення експерименту для 1-ї групи сценаріїв дозволили отримати наступні значення для заходів якості {*TP, TN, FP, FN*} а також {*r, p, a, e, f*} для кожної з варіацій алгоритмів, наведених у таблиці 4.1 (Клс .- Тип класифікатора машинного навчання).

Таблиця 4.1 - Порівняння заходів якості різних варіацій результатів виявлення інсайдерів у КС для простих та складних сценаріїв атак

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Варіації** | | | | | | | **Міри** | | | | |
| **№** | **Клс. ML** | **RB+ML** | **FP** | **FN** | **TP** | **TN** | **r** | **p** | **a** | **e** | **f** |
| 1 | NB | 𝐼𝑀𝐿 | 56 | 29 | 9951 | 9964 | 0.9971 | 0.9944 | 0.9958 | 0.0043 | 0.9957 |
| 2 | k-NN | 𝐼𝑀𝐿 | 81 | 38 | 9942 | 9939 | 0.9962 | 0.9919 | 0.9941 | 0.0060 | 0.9941 |
| 3 | SVM | 𝐼𝑀𝐿 | 43 | 49 | 9931 | 9977 | 0.9951 | 0.9957 | 0.9954 | 0.0046 | 0.9954 |
| 4 | PV | 𝐼𝑀𝐿 | 51 | 45 | 9955 | 9949 | 0.9955 | 0.9949 | 0.9952 | 0.0048 | 0.9952 |
| 5 | WV | 𝐼𝑀𝐿 | 50 | 33 | 9947 | 9970 | 0.9967 | 0.9950 | 0.9959 | 0.0042 | 0.9958 |
| 6 | SV | 𝐼𝑀𝐿 | 87 | 42 | 9938 | 9933 | 0.9958 | 0.9913 | 0.9936 | 0.0065 | 0.9936 |
| 7 | Adaboost | 𝐼𝑀𝐿 | 46 | 53 | 9947 | 9954 | 0.9947 | 0.9954 | 0.9951 | 0.0050 | 0.9950 |
| 8 | DT | 𝐼𝑀𝐿 | 75 | 42 | 9948 | 9935 | 0.9958 | 0.9925 | 0.9942 | 0.0059 | 0.9942 |
| 9 | NB | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 88 | 91 | 9985 | 9836 | 0.9910 | 0.9913 | 0.9911 | 0.0090 | 0.9911 |
| 10 | k-NN | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 94 | 91 | 9940 | 9875 | 0.9909 | 0.9906 | 0.9908 | 0.0093 | 0.9908 |
| 11 | SVM | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 90 | 93 | 9921 | 9896 | 0.9907 | 0.9910 | 0.9909 | 0.0092 | 0.9909 |
| 12 | PV | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 92 | 89 | 9933 | 9886 | 0.9911 | 0.9908 | 0.9910 | 0.0091 | 0.9910 |
| 13 | WV | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 89 | 88 | 9924 | 9899 | 0.9912 | 0.9911 | 0.9912 | 0.0089 | 0.9912 |
| 14 | SV | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 88 | 91 | 9891 | 9930 | 0.9909 | 0.9912 | 0.9911 | 0.0090 | 0.9910 |
| 15 | Adaboost | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 93 | 90 | 9934 | 9883 | 0.9910 | 0.9907 | 0.9909 | 0.0092 | 0.9909 |
| 16 | DT | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | 89 | 88 | 9916 | 9907 | 0.9912 | 0.9911 | 0.9912 | 0.0089 | 0.9912 |
| 17 | NB | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | 66 | 92 | 9908 | 9934 | 0.9908 | 0.9934 | 0.9921 | 0.0079 | 0.9921 |
| 18 | k-NN | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | 30 | 44 | 9956 | 9970 | 0.9956 | 0.9970 | 0.9963 | 0.0037 | 0.9963 |
| 19 | DT | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | 67 | 41 | 9959 | 9933 | 0.9959 | 0.9933 | 0.9946 | 0.0054 | 0.9946 |

Аналіз отриманих результатів (таблиця 4.1) дозволив зробити такі висновки. По-перше, будь-яких варіацій результатів роботи алгоритму з урахуванням експертних правил і методів машинного навчання всі заходи – тобто. повнота (r), точність (p), акуратність (a), помилка (e), F-заходи (f) – відповідають заданим вимогам. По-друге, міра помилки у разі поєднання результатів роботи алгоритмів має більше значення порівняно з їх перетином. По-третє, варіацією з найбільшим значенням F-заходи, що дорівнює 0.9963, є перетин алгоритму на базі експертного правила та методу машинного навчання з класифікатором NB (рядок під номером 17, позначений у таблиці червоним кольором). І, по-четверте, показники F-заходи для будь-яких комбінацій алгоритмів досить близькі (різниця між мінімальним та максимальним значеннями становить ~0.5%). Таким чином, найкращою з точки зору F-заходи варіацією для виявлення інсайдерів з простими та складними сценаріями атак є перетин результатів роботи алгоритму на основі експертних правил та методу машинного навчання при використанні класифікатора NB, проте перевагу не можна вважати гарантованим. Це пов'язано з тим, що при простих і складних сценаріях атак використовувані алгоритми показують приблизно однаковий результат з виявлення інсайдерів і, отже, зробити обґрунтований вибір найкращої комбінації алгоритмів та класифікатора неможливо. перевагу не можна вважати гарантованою. Це пов'язано з тим, що при простих і складних сценаріях атак використовувані алгоритми показують приблизно однаковий результат з виявлення інсайдерів і, отже, зробити обґрунтований вибір найкращої комбінації алгоритмів та класифікатора неможливо. перевагу не можна вважати гарантованою. Це пов'язано з тим, що при простих і складних сценаріях атак використовувані алгоритми показують приблизно однаковий результат з виявлення інсайдерів і, отже, зробити обґрунтований вибір найкращої комбінації алгоритмів та класифікатора неможливо.

Результати проведення експерименту для 2-ї групи сценаріїв дозволили отримати наступні значення для заходів якості {*TP, TN, FP, FN*}, а також {*r, p, a, e, f*} для кожної з варіацій алгоритмів, наведених у таблиці 4.2 (Клс – тип класифікатора машинного навчання).

Аналіз отриманих результатів (таблиця 4.2) дозволив зробити такі висновки. По-перше, лише перетину результатів роботи алгоритмів (рядки 17- 22 у таблиці) задовольняють вимогам F-заходи (позначено синім та червоним кольорами). По-друге, у середньому, міра помилки у разі поєднання результатів роботи алгоритмів має більше значення порівняно з їх перетином. По-третє, варіацією з найбільшим значенням F- міри, що дорівнює 0.95, є перетин алгоритму на базі експертного правила та методу машинного навчання з класифікатором SV (рядок під номером 22, позначений у таблиці червоним кольором). І, по-четверте, показники F-заходи для будь-яких способів комбінацій алгоритмів досить помітні один від одного (різниця між мінімальним та максимальним значеннями становить ~12%, а між найбільшим показником F-заходи та найближчим ~2%). Таким чином, найкращою з точки зору F-заходи варіацією для виявлення інсайдерів з комплексними сценаріями атак є перетин результатів роботи алгоритму на основі експертних правил та методу машинного навчання при використанні його класифікатора SV.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Варіації** | | | **Заходи** | | | | | | | | |
| **№** | **ML** | **RB+ML** | **TP** | **TN** | **FP** | **FN** | ***r*** | ***p*** | ***a*** | ***e*** | ***f*** |
| 1 | 𝐼𝑀𝐿 | DT | 9201 | 8111 | 1889 | 799 | 0.92 | 0.87 | 0.83 | 0.13 | 0.87 |
| 2 | 𝐼𝑀𝐿 | NB | 9341 | 8156 | 1844 | 659 | 0.93 | 0.88 | 0.84 | 0.13 | 0.88 |
| 3 | 𝐼𝑀𝐿 | k-NN | 9200 | 8109 | 1891 | 800 | 0.92 | 0.88 | 0.83 | 0.13 | 0.87 |
| 4 | 𝐼𝑀𝐿 | SVM | 9394 | 8190 | 1810 | 606 | 0.94 | 0.88 | 0.84 | 0.12 | 0.89 |
| 5 | 𝐼𝑀𝐿 | PV | 9378 | 8163 | 1837 | 622 | 0.94 | 0.88 | 0.84 | 0.12 | 0.88 |
| 6 | 𝐼𝑀𝐿 | WV | 9399 | 8170 | 1830 | 601 | 0.94 | 0.87 | 0.84 | 0.12 | 0.89 |
| 7 | 𝐼𝑀𝐿 | SV | 9362 | 8215 | 1785 | 638 | 0.94 | 0.88 | 0.84 | 0.12 | 0.89 |
| 8 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | Adaboost | 9822 | 7538 | 2462 | 178 | 0.98 | 0.86 | 0.80 | 0.13 | 0.88 |
| 9 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | DT | 9913 | 7603 | 2397 | 87 | 0.99 | 0.87 | 0.81 | 0.12 | 0.89 |
| 10 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | NB | 9728 | 7524 | 2476 | 272 | 0.97 | 0.88 | 0.80 | 0.14 | 0.88 |
| 11 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | k-NN | 9904 | 7501 | 2499 | 96 | 0.99 | 0.88 | 0.80 | 0.13 | 0.88 |
| 12 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | SVM | 9914 | 7660 | 2340 | 86 | 0.99 | 0.89 | 0.81 | 0.12 | 0.89 |
| 13 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | PV | 9969 | 7669 | 2331 | 31 | 1.00 | 0.88 | 0.81 | 0.12 | 0.89 |
| 14 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | WV | 9974 | 7780 | 2220 | 26 | 1.00 | 0.92 | 0.82 | 0.11 | 0.90 |
| 15 | 𝐼𝑅𝐵∨ 𝐼𝑀𝐿 | SV | 9901 | 7746 | 2254 | 99 | 0.99 | 0.87 | 0.81 | 0.12 | 0.89 |
| 16 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | Adaboost | 8724 | 9607 | 393 | 1276 | 0.87 | 0.88 | 0.96 | 0.08 | 0.91 |
| 17 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | DT | 8734 | 9717 | 283 | 1266 | 0.87 | 0.92 | 0.97 | 0.08 | 0.92 |
| 18 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | NB | 8831 | 9620 | 380 | 1169 | 0.88 | 0.92 | 0.96 | 0.08 | 0.92 |
| 19 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | k-NN | 8696 | 9801 | 199 | 1304 | 0.87 | 0.92 | 0.98 | 0.08 | 0.92 |
| 20 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | SVM | 8890 | 9859 | 141 | 1110 | 0.89 | 0.94 | 0.98 | 0.06 | 0.93 |
| 21 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | PV | 8967 | 9754 | 246 | 1033 | 0.90 | 0.94 | 0.97 | 0.06 | 0.93 |
| 22 | 𝐼𝑅𝐵∧ 𝐼𝑀𝐿 | WV | 8968 | 9989 | 11 | 1032 | 0.90 | 0.95 | 1.00 | 0.05 | 0.95 |

Таблиця 4.2 - Порівняння заходів якостей різних варіацій результатів виявлення інсайдерів у КС для комплексних сценаріїв атак

Необхідно відзначити, що запропонована методика виявлення інсайдерів у КС дозволяє використовувати будь-які із запропонованих класифікаторів та комбінацій результатів алгоритмів, що вибираються оператором на першому етапі. Так, наприклад, з позиції максимального значення повноти (r), найкращим вважатимуться поєднання алгоритмів (рядки з номерами 15 і 16).

Зробимо аналіз отриманих експериментальних результатів. По-перше, алгоритм на базі експертних правил хоча і виявляє велику кількість інсайдерів (TP) і вірно визначає частину законних користувачів (TN), водночас помилково визначає законних користувачів як інсайдерів (FP), а частина інсайдерів відповідно пропускається ( FN); по-друге, алгоритм на основі методів машинного навчання має схожу кількість виявлених та пропущених інсайдерів (TP, FN), проте він рідше помиляється на законних користувачах (TN вище, а FP нижче); об'єднання результатів роботи алгоритмів практично повністю виявляє всіх реальних інсайдерів (TP високий, FN низький), проте водночас у цю категорію потрапляє і більша кількість законних користувачів, які помилково приймаються за інсайдерів (TN низький, FP високий); перетин результатів роботи алгоритмів виявляє незначно меншу кількість інсайдерів, ніж об'єднання цих алгоритмів (TP нижче), але законні користувачі визначаються суттєво точніше (TN вище), а помилок першого роду стає менше (FP низький), кількість помилок ІІ-го роду несуттєво вища за аналогічний. числа помилок окремих алгоритмів (FN вище). Таким чином,

Тобто, кожен з алгоритмів має достатню кількість як пропусків інсайдерів, так і помилкових відносин числа законних користувачів до інсайдерів. Порівняно з роботою кожного з алгоритмів, поєднання їх результатів покращує виявлення інсайдерів, але водночас збільшує кількість хибних спрацьовувань. Перетин навпаки, погіршує виявлення інсайдерів, але водночас зменшує кількість хибних спрацьовувань. Однак, усереднений ефект від роботи перетину (тобто спільна оцінка з позиції повноти та точності) виявляється вищим; при цьому метод машинного навчання з класифікатором SV також виявляється із цієї позиції найкращим серед інших методів машинного навчання.

4.3 Оцінка параметрів системи

Оцінка обгрунтованності системи. Для порівняння обґрунтованості розробленої системи та її найближчих аналогів необхідно обчислити та порівняти введені заходи якості для кожної із систем.

Результати порівняння для 1-ї групи (прості та складні сценарії атак) та 2-ї групи (комплексні сценарії атак) наведені в таблиці 4.3.

Таблиця 3.3 – Заходи якості альтернативних систем виявлення інсайдерів у КС

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Назва**  **системи** | **FP** | **FN** | **TP** | **TN** | ***r*** | ***p*** | ***a*** | ***e*** | ***f*** |
| *1-а група (прості та складні сценарії атак)* | | | | | | | | | |
| Cisco  StealthWatch | 104 | 77 | 9923 | 9896 | 0.99 | 0.99 | 0.99 | 0.0091 | 0.9910 |
| PacketFence | 199 | 102 | 9898 | 9801 | 0.99 | 0.98 | 0.98 | 0.0151 | 0.9850 |
| *2-я група (комплексні сценарії атак)* | | | | | | | | | |
| Cisco  StealthWatch | 1066 | 766 | 9234 | 8934 | 0.92 | 0.90 | 0.91 | 0.09 | 0.91 |
| PacketFence | 1046 | 1157 | 8843 | 8954 | 0.88 | 0.89 | 0.89 | 0.11 | 0.89 |

**Оцінка своєчасності системи.** Перевіримо відповідність даного показника розробленої системи одному з нефункціональних вимог.

Для порівняння своєчасності розробленої системи та її найближчих аналогів необхідно обчислити та порівняти час виявлення інсайдерів для кожної із систем.

Результати порівняння середнього часу виконання наведено у таблиці 4.4.

Таблиця 4.4 – Показники своєчасності розробленої та альтернативних систем виявлення інсайдерів у КС

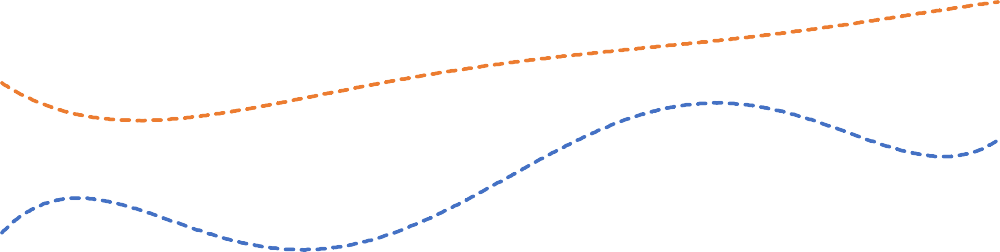
|  |  |  |
| --- | --- | --- |
| **Назва системи** | **Час (сек)**  **1-а група атак** | **Час (сек)**  **2-а група атак** |
| Розроблена система | 39 | 45 |
| Cisco StealthWatch | 42 | 48 |
| PacketFence | 46 | 52 |

Порівняльний аналіз значень своєчасності розробленої системи та її найближчих аналогів дозволяє стверджувати, що перша має найкращий показник ефективності.

Такий висновок можна обґрунтувати використанням у розробленій системі технології розподілених обчислень (MapReduce).

Результати вимірювань наведено на наступній діаграмі (рисунок 4.4).

Час роботи (сек.)



60

51

50

49

46

47

44

43

41

40

41

40

38

39

33

31

30

28

20

10

0

З 1

С2

С3

С4

Сценарії атаки

С5

С6

С7

Рисунок 4.4 – Час роботи розробленої системи для сценаріїв атак

**Оцінка ресурсоспоживання системи.** Перевіримо відповідність даного показника розробленої системи одному з нефункціональних вимог. Порівняння обчисленого показника ресурсоспоживання системи з необхідним значенням це підтверджує.

Для порівняння ресурсоспоживання розробленої системи та її найближчих аналогів необхідно обчислити та порівняти всі параметри в сукупності. Суть модифікації полягала у використанні лише обраної варіації алгоритмів та обчисленні параметрів ресурсоспоживання, що витрачається в процесі виявлення всіх інсайдерів, пов'язаних із сценаріями атак, що генеруються. Результати порівняння наведено у таблиці 4.5.

Таблиця 4.5 – Показники ресурсоспоживання розробленої та альтернативних систем виявлення інсайдерів у КС

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Назва системи** | **Кількість хостів (**𝑹𝒉) | **Середній мережний трафік (**𝑹𝒏),  Мб/сек | **обсяг**  **займаного простору SSD/HDD**  **(**𝑹𝒗), Гб | **Середнє наванта-ження на CPU (**𝑹𝒄) | **Середнє заванта-ження пам'яті (**𝑹𝑺) |
| Розроблена система | 6 | 100 | 900 | 40% | 45% |
| Cisco StealthWatch | 6 | 100 | 1000 | 40% | 45% |
| PacketFence | 6 | 100 | 750 | 45% | 50% |

Порівняльний аналіз значень ресурсоспоживання розробленої системи та її найближчих аналогів дозволяє стверджувати, що показники всіх трьох систем є приблизно рівними і можуть не враховуватися при порівнянні.

Такий висновок також можна обґрунтувати тим, що кожна система застосовує власні підходи та рішення, що мають досить високий рівень оптимізації ресурсосживання.

Виходячи з того, що показники своєчасності та ресурсоспоживання розробленої системи можна порівняти з аналогічними показниками для найближчих аналогів (Cisco StealthWatch і PacketFence), а показник обґрунтованості має перевагу (~5%), можна стверджувати, що дана система має кращу ефективність, а, отже, підвищує захищеність КС від атак інсайдерів.

4.4 Пропозиції щодо застосування системи виявлення інсайдерів у комп’ютерних системах та висновки до розділу

Розроблені у роботі моделі, алгоритми, методика та система можуть бути використані для наступних рішень.

По-перше, запропонована модель представлення великих даних може бути застосована не тільки для виявлення інсайдерів, а також для аналізу поведінки законних користувачів на користь підвищення ефективності роботи організації, оптимізації її бізнес-процесів та ін. Так, наприклад, індикація та виявлення закономірностей, пов'язаних з помилковими діями користувачів по роботі з внутрішніми документами може сигналізувати у тому, що посадові обов'язки співробітників є очевидними їм і вимагають роз'яснення. Часті пересилання невеликих обсягів даних між відділами можуть говорити про потрібність їх у використанні загальної бази даних, що може бути вирішено створенням внутрішнього інформаційно-довідкового сервера.

Потенційно перспективним застосуванням моделі може стати аналіз КС щодо дій співробітників, спрямований на оцінку поточного та прогнозування майбутнього стану організації в цілому – визначення її тренду розвитку. Наприклад, часте відвідування інформаційних сайтів співробітниками як у робочий час, так і поза ним, може говорити про їхню захопленість поставленим завданням та високою мотивацією роботи у фірмі. Зв'язок певних рішень керівництва компанії (випуск наказу про трудовий дисципліни, розпуск відділу і т.п.) з відвідуванням співробітниками сайтів про найм на роботу, очевидно, означає розчарованість співробітників в організації та прагнення змінити місце роботи, що має послужити сигналом для керівництва про високі ризики проектів.

По-друге, запропоновані модель та алгоритми комбінованого застосування експертних правил і методів машинного навчання, а також розроблена методика (після необхідної адаптації) застосовні також і для протидії зовнішнім мережевим атакам, оскільки їхнє основне ядро ​​є досить гнучким і не дуже залежним від специфіки КС. Наприклад, алгоритм на основі експертних правил може розглядати інсайдера як зовнішнього зловмисника і застосовувати подібні правила для його виявлення; а алгоритм з урахуванням методів машинного навчання може бути налаштований виявлення сценаріїв атак на організацію із боку відкритих мереж. При цьому алгоритми можуть працювати в комплексі в рамках розробленої методики, якій буде потрібно несуттєва модифікація в частині агентів збору даних. Природно, комплекс алгоритмів може бути доповнений іншими,

По-третє, запропонована система виявлення інсайдерів у КС може бути використана при розробці наступних, більших програмних комплексів захисту від загроз інформаційної безпеки – як основа для реалізації повноцінної SIEM-системи нового покоління, що здійснює не тільки виявлення інсайдерів, але й їхню нейтралізацію ще до настання суттєвої шкоди. Для цього буде потрібно узгодження моделей та алгоритмів розробленої системи з працюючими в SIEM-системах: необроблені дані мережі повинні спочатку піддаватися аналізу щодо інсайдерської діяльності; розроблена модель має бути джерелом даних для моделей захисту, що синтезують контрзаходи; мають бути реалізовані засоби оцінки захищеності КС від інсайдерських дій; алгоритми мають бути керовані оператором, а також враховувати у своїй роботі захищеність КС.

ВИСНОВКИ

У магістерській роботі з метою підвищення захищеності КС вирішено задачу розробки модельно-методичного апарату для виявлення інсайдерів у мережі на основі комбінованого використання експертних правил, методів машинного навчання та обробки великих даних, що має важливе значення для розвитку технологій у галузі інформаційної безпеки. У тому числі отримані такі наукові результати, що становлять підсумки дослідження:

1) проведено аналіз існуючих підходів до виявлення інсайдерів у КС, моделей, методик та алгоритмів виявлення інсайдерів у КС на основі методів машинного навчання та обробки великих даних;

2) розроблено модель представлення великих даних про інсайдерські атаки у форматі NoSQL (включаючи модель інсайдера);

3) розроблено алгоритм виявлення інсайдерів у КС, заснований на експертних правилах;

4) розроблено модель та алгоритми комбінованого застосування експертних правил та методів машинного навчання на користь виявлення інсайдерських атак;

5) розроблено методику виявлення інсайдерів у комп'ютерних мережах з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних;

6) розроблено архітектуру системи виявлення інсайдерів у комп'ютерних мережах з використанням комбінування експертних правил, методів машинного навчання та обробки великих даних та виконано її програмну реалізацію. Здійснено налаштування алгоритму на основі методів машинного навчання за допомогою набору даних, що характеризують дії інсайдерів за заданою множиною сценаріїв атак та експериментальна оцінка розробленої методики системи виявлення інсайдерів у КС.