ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ВІД ФІЗИЧНОГО ТА ПРОГРАМНОГО ВПЛИВУ ПІД ЧАС ІНСАЙДЕРСЬКИХ АТАК»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кушнір Д. І.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ — 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
“___”_____ 2021 року

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

Кушнір Дмитро Ігорович
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи: «Технологія захисту від фізичного та програмного впливу під час інсайдерських атак»

керівник бакалаврської роботи Марченко Віталій Вікторович, асистент
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2021 року №170.

2. Строк подання студентом бакалаврської роботи 15.12.2021 р.

3. Вихідні дані до бакалаврської роботи
науково дослідницька література;
програмні технології виявлення інсайдерських атак;
наукова та технічна література, експлуатаційна документація.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Провести аналіз виявлення інсайдерських атак та їх вплив на інформаційну систему організації;
2. Переглянути методи та засоби протидії інсайдерських атак;
3. Запропонувати технологію протидії під час із.

5. Перелік графічного матеріалу

1. Мета, об'єкт, предмет та задачі магістерської роботи
2. Аналіз виявлення інсайдерських атак
3. Статистика компрометації організації
4. Методи та засоби протидії від інсайдерських атак
5. Технологія протидії під час ІА
6. Висновок

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблем протидії інсайдерським атакам для організації	27.09.2021р.	
2.	Аналіз наукової та технічної літератури	14.10.2021р.	
3.	Аналіз методів та засобів протидії інсайдерським атакам	30.10.2021р.	
4.	Аналіз технологій протидії інсайдерам	15.11.2021р.	
5.	Розробка комплексної технології протидії від інсайдерських атак	01.12.2021р.	
6.	Висновки. Підготовка демонстраційного матеріалу	13.12.2021р.	
7.	Підготовка доповіді до захисту	15.12.2021р.	

Студент _____ Д. І. Кушнір
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ В.В. Марченко
(підпис) прізвище та ініціали

РЕЦЕНЗІЯ

на магістерську роботу

студента Кушніра Дмитра Ігоровича

на тему: ТЕХНОЛОГІЯ ЗАХИСТУ ВІД ФІЗИЧНОГО ТА ПРОГРАМНОГО ВПЛИВУ ПІД ЧАС ІНСАЙДЕРСЬКИХ АТАК

Актуальність: Технологія захисту від фізичного та програмного впливу під час інсайдерських атак. відіграє важливу роль у забезпеченні безпеки, які можуть бути використанідля протидії зловмисникам. Актуальним є питання визначення та протидії інсайдерам в організації. Тому тема бакалаврської роботи присвяченої дослідженню та розробці рекомендацій щодо захисту даних від інсайдерських загроз, є актуальною науковою задачею.

Позитивні сторони: Наукові положення, викладені в дипломній роботі, висновки та технологій мають теоретичне обґрунтування. Проведені дослідження свідчать про вміння автора працювати з науково-технічною літературою, проводити інженерний аналіз та узагальнювати матеріал. Матеріали роботи можуть бути використані при розробленні засобів захисту даних в різних сферах інформаційної діяльності.

Зауваження: рекомендується розширити ряд технологій для протидії інсайдерським загрозам.

Висновки: Вказані зауваження не суттєво впливають на якість виконаної роботи, яка заслуговує оцінки оцінку «відмінно», а її автор Кушнір Дмитро Ігорович повністю – присвоєння кваліфікації «магістр кібербезпеки за спеціальністю інформаційна та кібернетична безпека».

Якість бакалаврської роботи	
виконано на замовлення підприємства	
виконано за тематикою НДР	
виконано з макетом	
має практичну цінність	+

Підпис рецензента

_____ _____

(П.І.Б.)

_____

(посада, науковий ступінь, вчене звання)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Кушнір Д. І. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту від фізичного та програмного впливу під час інсайдерських атак»

Магістерська робота і рецензія додаються.
Директор інституту Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Кушнір Д. І. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) Черниш О.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Кушнір Д. І.*** обрав тему роботи, метою якої запропонувати комплексну технологію захисту від фізичного та програмного впливу під час інсайдерських атак. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Кушнір Д. І. показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Кушніра Дмитра Ігоровича на оцінку «**відмінно**» та присвоїти йому кваліфікацію магістр кібербезпеки за спеціальністю інформаційна та кібернетична безпека.

Керівник магістерської роботи В.В. Марченко
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про бакалаврську роботу

Магістерська робота розглянута. Студент Кушнір Д. І.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

Г.І. Гайдур
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 61 сторінок, 42 рисунків, 24 джерела.

Об’єкт дослідження — процес впливу інсайдерських атак та їх вплив на інформаційну систему організації.

Предмет дослідження — технологія протидії інсайдерським атакам на інформаційну систему організації.

Мета роботи — запропонувати комплексну технологію протидії інсайдерським атакам на інформаційну систему організації.

Для досягнення зазначеної мети необхідно вирішити наступні задачі:

1) проаналізувати типи інсайдерських атак та їх впливи на інформаційну систему організації.

2) дослідити методи та засоби протидії інсайдерським атакам.

3) запропонувати комплексну технологію протидії від інсайдерських атак.

Методи дослідження — опрацювати літератури за даною темою.

В роботі зроблено аналіз поведінки інсайдера та наведено статистику по їх загрозам. Проаналізовано фізичні та програмні методи захисту від загроз під час інсайдерських атак. Порівняння технологій доводить що не існує універсального захисту від інсайдерів та потрібно розвивати захист організації використовуючи різноманітні технології та методи протидії зловмисникам.

Розглянуто технології відомих компаній з протидії інсайдерським загрозам та створено технологію для захисту в організації.

Галузь використання — інформаційна та кібернетична безпека організації.

Апробація роботи. Основні результати роботи опубліковані на таких наукових конференціях та журналах як:

1. Кушнір Д.І. Загрози пов'язані з віддаленою роботою. Як зробити віддалену роботу ефективною та безпечною [Електронний ресурс] / Д.І. Кушнір // V міжнародна науково-практична конференція «Актуальні проблеми кібербезпеки». 27 жовтня 2021 року — К.: ДУТ. — 2021. — С. 35-39.
2. Бобровський О.О Методика вибору стратегії протидії інформаційному впливу на структуру віртуальної спільноти [Електронний ресурс] / О.О. Бобровський, Д.І. Кушнір, Т.М. Дзюба // Сучасний захист інформації №3(47), 2021 — С. 6-11.

ІНСАЙДЕР, ІНСАЙДЕРСЬКА АТАКА, ТЕХНОЛОГІЯ, UEBA, PAM, DLP, SIEM, INSIDER RISK MANAGEMENT SOLUTIONS, СТАТИСТИКА.

ABSTRACT

Master’s thesis: 61 pages, 42 figures, 24 sources.

Object of research – the definition of an insider in an organization.

Subject of research – technologies for counteraction to insider threats.

The aim of research – to propose the technology of counteracting insider threats.

Research methods – to work literature on this topic.

The physical and software methods of protection against threats during insider attacks are analyzed. Comparison of technologies proves that there is no universal protection against insiders and it is necessary to develop the protection of the organization using a variety of technologies and methods of counteracting intruders.

The technologies of well-known companies for counteracting insider threats are considered and the technology for protection in the organization is created.

Area of use - information and cyber security of the organization.

Approbation of work. The main results of the work are published at such scientific conferences and journals as:

1. Kushnir DI Threats are associated with remote work. How to make remote work effective and safe [Electronic resource] / D.I. Kushnir // V International Scientific and Practical Conference "Current Issues of Cyber Security". October 27, 2021 - K.: DUT. - 2021. - P. 35-39.

2. Bobrovsky OO Methods of choosing a strategy to counteract the information impact on the structure of the virtual community [Electronic resource] / OO Bobrovsky. Bobrovsky, DI Kushnir, T.M. Dziuba // Modern information protection №3 (47), 2021 - P. 6-11.

INSIDER, INSIDER THREAT, PREVENTION OF INFORMATION LEAKAGE, TECHNOLOGY, UEBA, PAM, DLP, SIEM, INSIDER RISK MANAGEMENT SOLUTIONS, STATISTICS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ — Інформаційна Безпека;

ІТ – Інформаційні технології;

ІЗ – Інсайдерська загроза;

CISO – Chief information security officer;

ІС – Інформаційна система;

ПЗ — Програмне забезпечення;

IP — Internet Protocol;

ОС — Операційна Система;

UEBA — User and Entity Behavior Analytics;

PAM — Privileged Access Management;

DLP — Data Loss Prevention;

SIEM — Security Information and Event Management;

IAM – Identity and Access Management.

ІА — інсайдерська атака

ВСТУП

В теперішній час, технології захопили кожний сектор організації, проте з ними працюють співробітники для яких властиво помилятися та створювати вектор атак який іменують «людський фактор». Саме людина є інсайдером для організації. Тільки людина може вивантажити конфіденційну інформацію та пронести її через необмежену кількість пропускних пунктів задля однієї мети – завдати шкоди організації або отримати вигоду для себе.

Дослідження різноманітних інститутів та кібероганізацій вказують, що нинішні або колишні співробітники є однією з найбільших загроз кібербезпеці. Це обумовлено тим, що більша частина традиційних засобів захисту, таких як антивіруси, міжмережеві екрани і системи аутентифікації не здатні забезпечити ефективний захист від внутрішніх порушників. Інсайдерська загроза існує завжди, адже інсайдером може стати будь-який співробітник з будь-яким організації з різним набором повноважень. Щоб розробити якісну модель протидії інсайдерам, необхідно провести класифікацію інсайдерів, визначити можливості кожного окремого класу і, відповідно до цього, визначити можливі заходи і засоби захисту.

Захист організації від ІЗ є дуже важливий в теперішніх реаліях віддаленої роботи та COVID-19 пандемії. Онлайн зустрічі не мотивують співробітника залишатися в компанії та не покращує його самопочуття, тому в нього можуть виникати думки про компрометацію даних, так як більшість інформації зберігається на електронних носіях, але є також паперові екземпляри даних та інші фізичні носії які співробітник може використати для своїх цілей. Основний виклик для адміністратора в організації це зменшення кількості конфіденційної інформації на фізичних носіях яку ми не можемо контролювати. Крок за кроком ми рухаємося до хмарних обчислень що збільшує кількість інформації на хмарних ресурсах та об’єму даних який потрібно структурувати та контролювати щоб попередити його витік як через мережу, так і на фізичні носії.

Адміністраторові складно оцінити дії кожного співробітника коли їх сотні або тисячі людей. Автоматизовані системи навчилися збирати, аналізувати та

знаходити інциденти до їх появлення. Попередити поширення даних та втрату їх конфіденційності для організації.

У цій роботі ми розглядаємо визначення та методи щодо захисту даних від інсайдерських загроз. Тому надаю технології та приклади програмних комплексів щодо захисту організації.

Основною метою магістерської роботи є створення технології захисту від фізичного та програмного впливу під час інсайдерських атак.

Для досягнення зазначеної мети необхідно вирішити наступні задачі:

1. Провести аналіз виявлення інсайдерських атак та їх вплив на інформаційну систему організації;
2. Переглянути методи та засоби протидії інсайдерських атак;
3. Запропонувати технологію протидії під час із.

РОЗДІЛ 1 АНАЛІЗ ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ АТАК ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ СИСТЕМУ ОРГАНІЗАЦІЇ

1.1 Аналіз типів інсайдерських атак

З кожним роком зростає кількість випадків атак з сторони інсайдерів, оскільки людський фактор був і буде найпростішим джерелом отримання інформації. Перед керівниками інформаційної та кібернетичної безпеки постає виклик створення заходів протидії фізичного та програмного впливу під час інсайдерських атак. Інсайдером може бути будь-хто, тому організаціям необхідно провести ретельну підготовку для протидії та мінімізації ризику від атак. Обмін інформацією призводить до більшого доступу та поширення конфіденційних даних, але важливо пам’ятати про фізичну безпеки. Антивірус та брандмауер не врятує якщо зловмисник вже всередині та планує викрасти надрукований каталог або незаблокований пристрій.

Інсайдер - особа, яка має або мав уповноважений доступ до критичних активів організації, де вони працюють та мають законний доступ до мережі компанії, які використовують їх доступ, зловмисно, або ненавмисно, діяв таким чином, щоб негативно вплинути на організацію [1].

Інсайдерська загроза (ІЗ) – ризик заподіяння шкоди організації людьми, які знаходяться всередині контуру організації. До таких людей – їх називають інсайдерами – можуть бути як колишні, так і нинішні співробітники самої компанії, і фахівці підрядників або партнерів, тобто кожен, хто має доступ до конфіденційної інформації і критичної інфраструктури компанії.

Інсайдерська атака (ІА) – це зловмисна атака, здійснена в мережі чи комп’ютерній системі особою, яка має дозвіл на доступ до системи.

Шкідливий інсайдер - це теперішній або колишній працівник, підрядник або діловий партнер, який має або мав уповноважений доступ до мережі організації, системи або даних, та навмисно перевищує або неправильно використовувати цей

доступ таким чином, щоб негативно вплинути на конфіденційність, цілісність або доступність інформації до інформаційних систем організації.

Ненавмисна інсайдерська атака - це теперішній або колишній працівник, підрядник або діловий партнер, який має або мав уповноважений доступ до мережі організації, системи або даних, а також через дію або бездіяльність без зловмисного наміру, завдає шкоди або істотно збільшувати ймовірність майбутньої шкоди конфіденційності, цілісності або доступності інформації до інформаційних систем організації.

Втім, і перше, і друге буває важко виявити, але обидва інсайдери представляють загрозу для інтелектуальної власності, яка є основним активом компанії. Встановлення прав на інтелектуальну власність і їх захист - найважливіший аспект будь-якого бізнесу. Тому витік такої інформації призводить до збитків, судових позовів, репутаційного збитку.

Жодного дня не проходить без обговорень, новин чи оновлень про кібербезпеку. Надійні паролі, шифрування, мережеві виправлення, злом даних тощо. Серйозні наслідки вторгнення даних змусили ради директорів і безпеку підприємства приділяти значний час і ресурси для усунення проблеми.

Компанії занадто далеко відійшли від базового «блокування та боротьби», на якому заснована безпека підприємства, що дозволило йому ефективно знизити ризики всередині підприємства. Ради директорів не розуміють важливу роль, яку фізична безпека все ще відіграє на підприємстві.

Основна причина зосередження на кіберпросторі полягає в тому, що на рівні зали засідань компанії це сприймається як набагато значніший ризик, ніж звичайні речей з робочого простору порушником. Проте менші інциденти можуть бути ознаками потенційно шкідливих інцидентів, особливо з інсайдерськими загрозами. Проблема внутрішньої загрози є багатогранною. Тобто ми часто думаємо, що інсайдерська загроза виникає в контексті викрадення інформації, даних або конфіденційної інформації. Але це також може бути особа, яка має доступ до ваших об’єктів або приміщень, яка завдає фізичну шкоду.

Співробітники все ще забирають друковані документи з підприємств, і це вимагає розслідування.

Хоча практично кожна людина відчує стресові події, більшість з них, не вдаючись до руйнівних або руйнівних актів. Для тих інсайдерів, які звертаються до шкідливої діяльності, дослідники виявили, що акти рідко спонтанні; Замість цього вони, як правило, є результатом навмисного діяння.

Дослідники інсайдерських загроз описують еволюцію від довіреної інсайдера до інсайдерської загрози як критичного шляху. На цій дорозі, особистісні схильності суб'єкта, які роблять їх сприйнятливими до спокуси шкідливого акту, взаємодіють з їх особистими стресорами та організаційним середовищем. Разом фактори рухають інсайдера на шлях до шкідливого інциденту.

Переміщення від ідеї до дії передбачає наступні кроки, показані на шляху над шкідливим інцидентом [2].

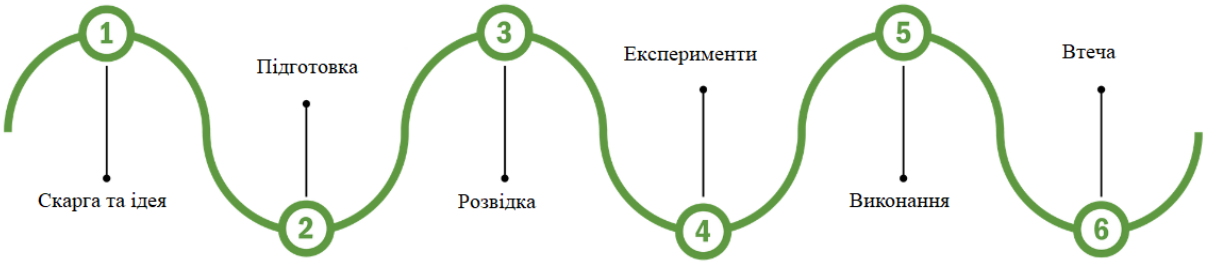

Рис. 1.1. Прогресування інсайдера до зловмисного інциденту

1. Скарга та ідея: висловлюючи ідеї через мову, твори, дії тощо.
2. Підготовка: проведення досліджень та розробки плану. Збір матеріалів, інструментів, обладнання тощо.
3. Розвідка: вербування співучасників (іноді); може бути точка перекидання.
4. Експерименти: проведення спостереження, розвідки та тестування.
5. Виконання: експлуатація довіреного доступу та інформації, включаючи використання слабких сторін та / або органів влади, щоб здійснити ворожий акт.

6. Втеча: спроба уникнути покарання або заплутувати сліди, щоб покрити свої інсайдерські дії

У більшості розслідувань, пов’язаному з можливим крадіжкою дуже конфіденційної інформації, успішні інтерв’ю підозрюваних співробітників привели до швидкого вилучення документів і зовнішніх електронних пристроїв зберігання, крім тих, які були виявлені під час судово-експертного аналізу. Це звичайне явище в галузі, коли працівники можуть відчувати почуття «власності» над інформацією та робочим продуктом, пов’язаним із проектами, до яких вони були призначені. І навпаки, люди, які отримали інсайдерський доступ до дуже конфіденційної інформації, іноді крадуть матеріал, на який вони взагалі не мають права. Людям надано доступ виконувати свою роботу, але іноді їм надають надмірний доступ. Доступ, який їм насправді не потрібен, що є проблемною зоною. Проблема виникає коли хтось бере цей авторизований доступ і перетворює його на несанкціоновану.

Компанія CERT узагальнили визначення та відійшли від спроби перелічити, які типи людей вважаються інсайдерами, які види інсайдерів мають доступ до активів, і які види шкоди могли бути зроблені для організації. Забезпечення узагальненого визначення дозволяє розширювати ці складні ідеї, щоб задовольнити конкретні потреби та пріоритети даної організації. Оскільки додаткові загрози адміністратори починають розглядатися як інсайдерські загрози та інші види впливу, результату від діяльності інсайдарів, це визначення все одно буде застосовуватися. Тим не менш, важливо, щоб ці ідеї були розширені та описані в визначенні, щоб забезпечити розуміння загрози та його потенційні наслідки. Щоб допомогти з цією метою, вони розробили наступну діаграму [2]:

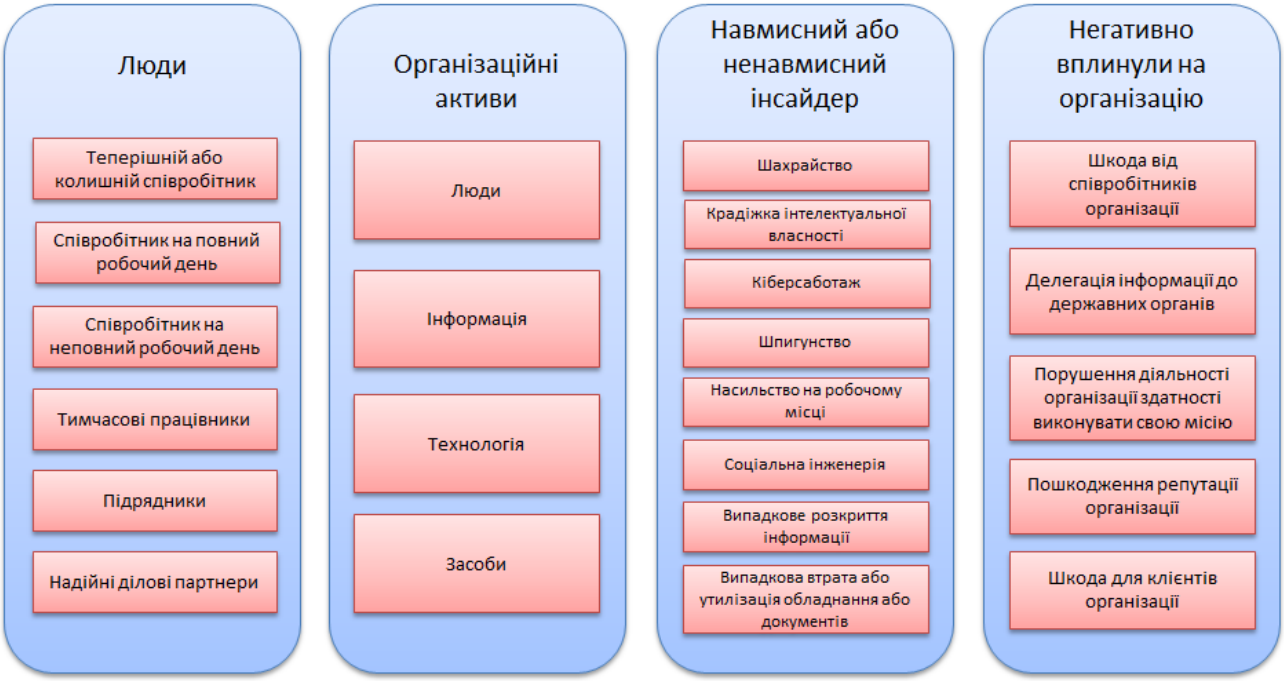

Рис. 1.2. Діаграма розподілення типів інсайдерів та їх впливів

Люди

- Теперішній або колишній співробітник
- Співробітник на повний робочий день
- Співробітник на неповний робочий день
- Тимчасові працівники
- Підрядники
- Надійні ділові партнери

Організаційні активи

- Люди
- Інформація
- Технологія
- Засоби

Навмисний або ненавмисний інсайдер

- Шахрайство
- Крадіжка інтелектуальної власності
- Кіберсаботаж

- Шпигунство
- Насильство на робочому місці
- Соціальна інженерія
- Випадкове розкриття інформації
- Випадкова втрата або утилізація обладнання або документів

Негативно вплинули на організацію

- Шкода від співробітників організації
- Делегація інформації до державних органів
- Порушення діяльності організації здатності виконувати свою місію
- Пошкодження репутації організації
- Шкода для клієнтів організації

1.2 Показники виявлення інсайдерських атак та їх наслідки

Загальні поведінкові показники (UBA) що наведені в “The CISO’s Guide to Managing Insider Threats" [3].

Найпоширенішим показником інсайдерської загрози є недостатня обізнаність. Наприклад, працівники з кмітливими навичками IT часто створюють обходи для вирішення технологічних проблем. Коли працівники використовують власні особисті пристрої для доступу до робочих електронних листів, вони часто створюють нові вразливості в межах фізичних процесів організації та IT-систем.

Головний співробітник інформаційної безпеки (CISO) повинен усвідомлювати ці зразки для виявлення підозрілих мотивів, що вимагає цілісного та шаруватого підходу до аналітики поведінки користувачів (UBA). Нижче наведено приклади показників поведінки:

- Завантаження значної кількості даних на зовнішні накопичувачі;
- Доступ до конфіденційних даних, які не стосуються ролі користувача;
- Надсилання конфіденційної інформації на особистий ресурси;
- Спроби обійти засоби безпеки;

- Запити на отримання дозволу або доступ вищого рівня без потреби;
- Частий доступ до робочої області поза звичайним робочим часом;
- Безвідповідальна поведінка у соціальних медіа;
- Можливість доступу до конфіденційних даних після завершення;
- Використання не санкціонованих зовнішніх пристроїв зберігання даних;
- Видиме незадоволення щодо роботодавців або колег;
- Хронічне порушення політики організації;
- Зниження результатів роботи;
- Використання мобільних пристроїв для фотографування або іншим способом запису комп'ютерних екранів, загальних робочих зон або центрів обробки даних;
- Надмірне використання принтерів та сканерів;
- Електронні комунікації, що містять надмірне використання негативної мови;
- Встановлення не підтвердженого програмного забезпечення;
- Спілкування з поточними або колишніми працівниками високого ризику;
- Подорожі до країн для передачі інтелектуальної крадіжки, або розміщення конкурентів;
- Порушення корпоративної політики [3; 4];
- Сканування мережі, зберігання даних або копіювання із внутрішніх сховищ;
- Аномалії в робочий час;
- Спроби доступу до обмежених територій;
- Ознаки розкішного життя співробітника не по засобах доходу.
- Обговорення відставки чи нових підприємницьких підприємств;
- Скарги на ворожу, ненормальну, неетичну чи незаконну поведінку.

Одним з найбільш тривожних висновків є те, що багато команд безпеки можуть не усвідомлювати фінансовий вплив інсайдерських атак на організацію. Більшість вважають, що для боротьби з інсайдерською атакою або посередництва

в ній буде коштувати менше 100 000 доларів. Але різноманітні дослідження показують, що ці типи атак значно дорожчі. Останні звіти підрахували, що середня вартість кіберінциденту сьогодні коливається від 270 000 доларів до понад 20 мільйонів доларів у великих організаціях. Окрім грошових втрат, адміністратори повинні мати справу з криміналістичними проблемами, щоб з'ясувати, як стався інцидент. Це вимагає значного часу від команд внутрішньої безпеки, щоб усунути інцидент, відібравши час на більш стратегічні дії. Вам необхідно провести додаткове навчання, потенційно найняти зовнішніх консультантів і навіть замінити нове обладнання, щоб закрити будь-які лазівки. У поєднанні все це призводить до несподіваних витрат для організації.

На рисунку наведено графік, який показує гістограму інцидентів 204 компаній за останні 12 місяців. Як показано, 60 відсотків компаній пережили в середньому понад 30 інцидентів на рік [5].

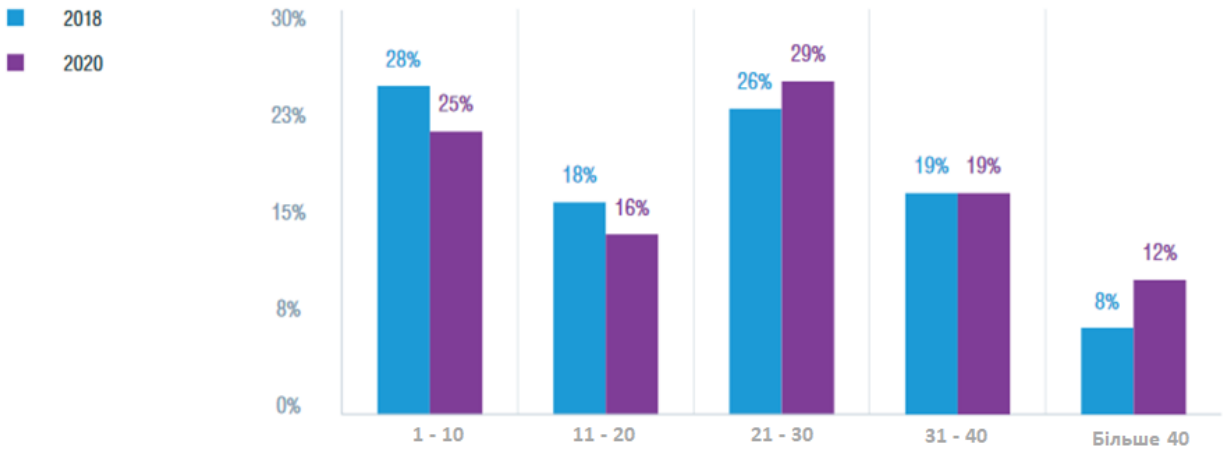

Рис. 1.3. Відсоткова частота інсайдерських інцидентів на кожну компанію

Всі типи інсайдерських загроз неухильно зростають. Неважливо це теперішній або колишній співробітник чи шкідливий або злочинний інсайдер – кількість інцидентів з року в рік неухильно збільшується.

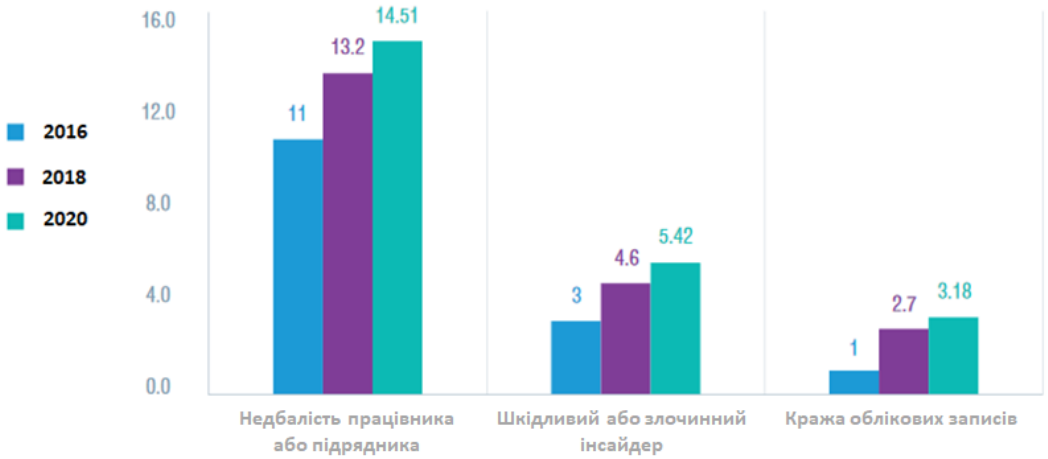

Рис. 1.4. Частота для трьох профілів інсайдерських інцидентів

Як показано на рисунку, з 2016 року середня кількість інцидентів, пов'язаних з працівником або недбалість підрядника збільшився з 10,5 до 14,5 у 2020 році. Середня кількість інцидентів з кражою даних на кожну компанію зросла з 1 в 2016 року до 3,18 в 2020 році [5].

На вершині циклічних змін у технологіях та загрозах, глобальна пандемія перетворилася на роботу догори ногами для бізнесу та споживачів по всьому світу. Спеціалісти компанії IBM в своєму досліджені виявили, що більшість організацій (76%) передбачали, що віддалена робота буде відповідати потенційним порушенням даних набагато складнішим випробуванням [6].

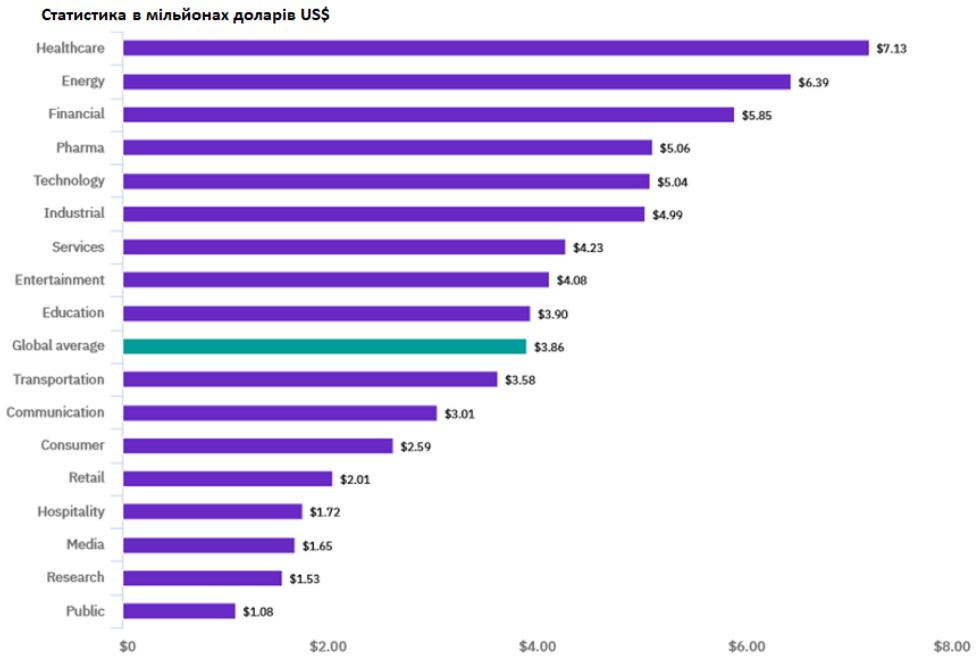

Рис. 1.5. Середня загальна вартість порушення даних галузі

Організації, що підлягають більш суворим нормативним вимогам, мали високі витрати на порушення даних. Як показано на рисунку, охорона здоров'я, енергетика, фінансові послуги та фармацевтична галузь зазнали середньої загальної вартості порушення даних значно вище, ніж менш регульовані галузей, таких як гостинність, медіа та дослідження. Організації державного сектору традиційно мають найнижчу вартість порушення даних у цьому дослідженні, оскільки вони навряд чи зазнають значної втрати клієнтів внаслідок порушення даних.

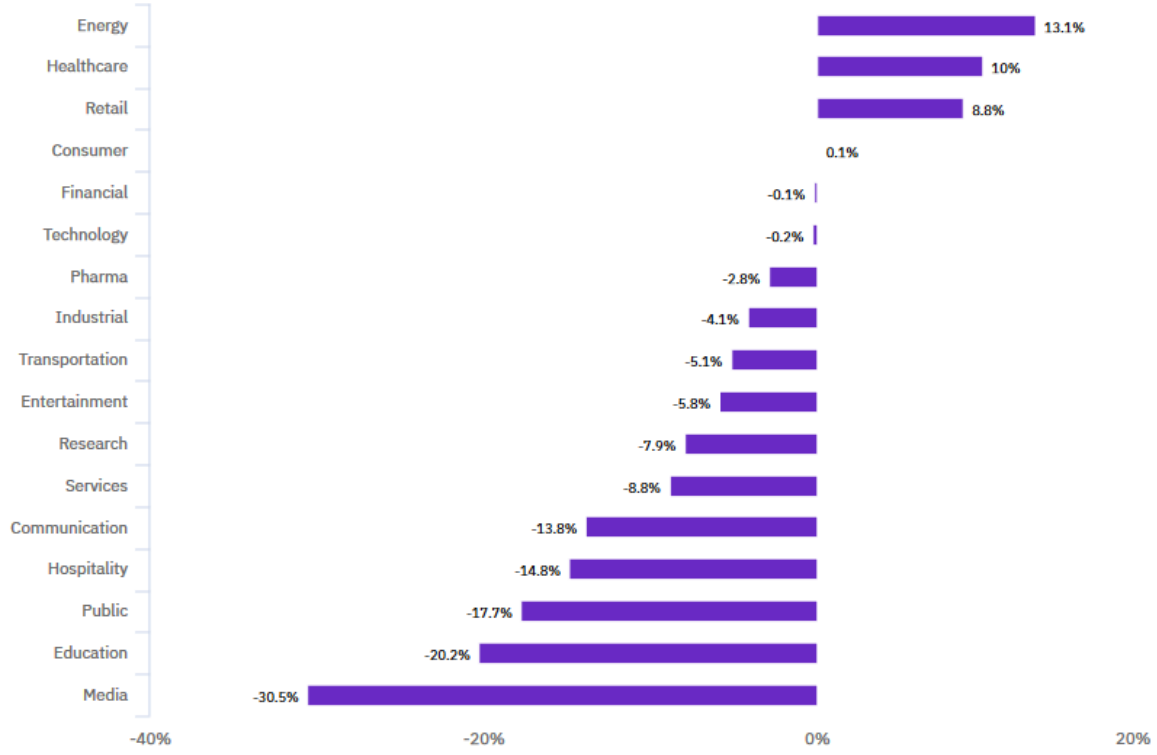

Рис. 1.6. Зміна відсотків середньої загальної вартості промисловості, 2019-2020 роки [6]

На рисунку показано, що збільшення витрат на порушення даних відбулося лише у чотирьох з 17 галузях промисловості між дослідженням 2019 року та дослідження 2020 року. Енергетика, охорона здоров'я та роздрібна торгівля зазнала найвищого збільшення середньої загальної вартості, тоді як державний сектор, освіта та засоби масової інформації найбільше зменшується.

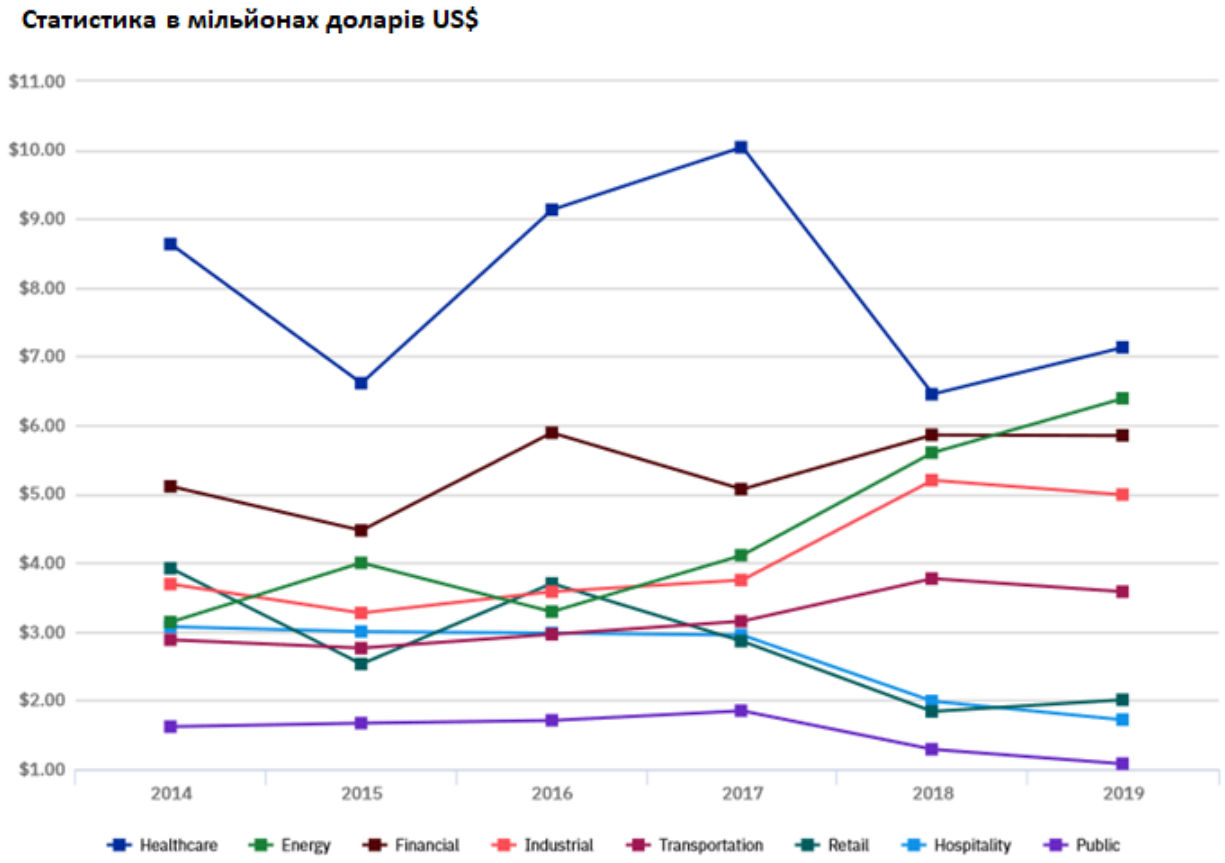

Рис. 1.7. Тенденція середньої загальної вартості порушення даних у восьми галузях промисловості

На рисунку представлений графік для кожного з восьми секторів промисловості за останні шість років. Охорона здоров'я постійно мала найвищу вартість втрат, проте громадський сектор послідовно найнижчу вартість втрат [6].

Викрадені або скомпрометовані облікові дані та хмара помилковість були провідними початковими векторами загрози, кожен з яких відповідає 19% від здорових порушень. Вразливості на сторонніх програм було первинним вектором загрозу у 16% зловмисних порушень, згідно з рисунком. При цьому атаки з сторони шкідливого інсайдера займають всього 7 % від усіх атак [6].

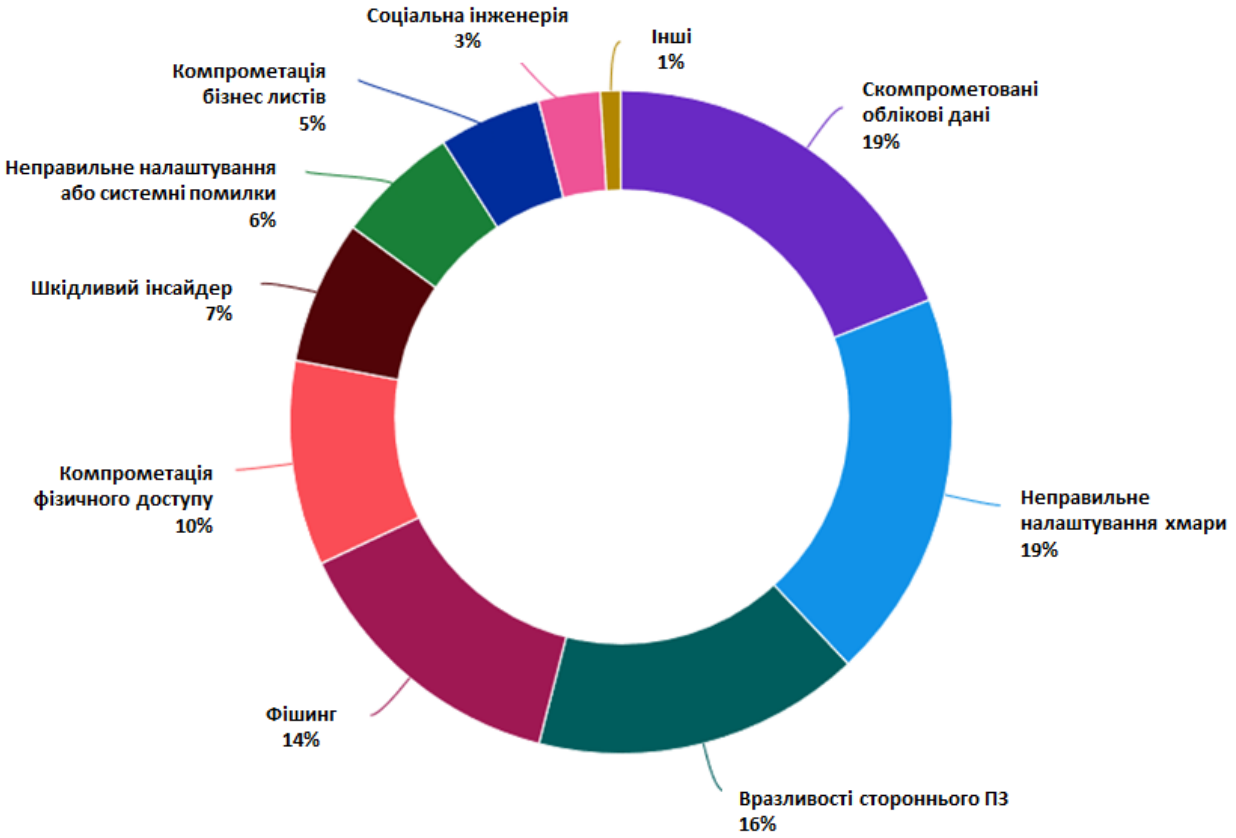

Рис. 1.8. Діаграма розподілу шкідливих причин порушення даних по секторах

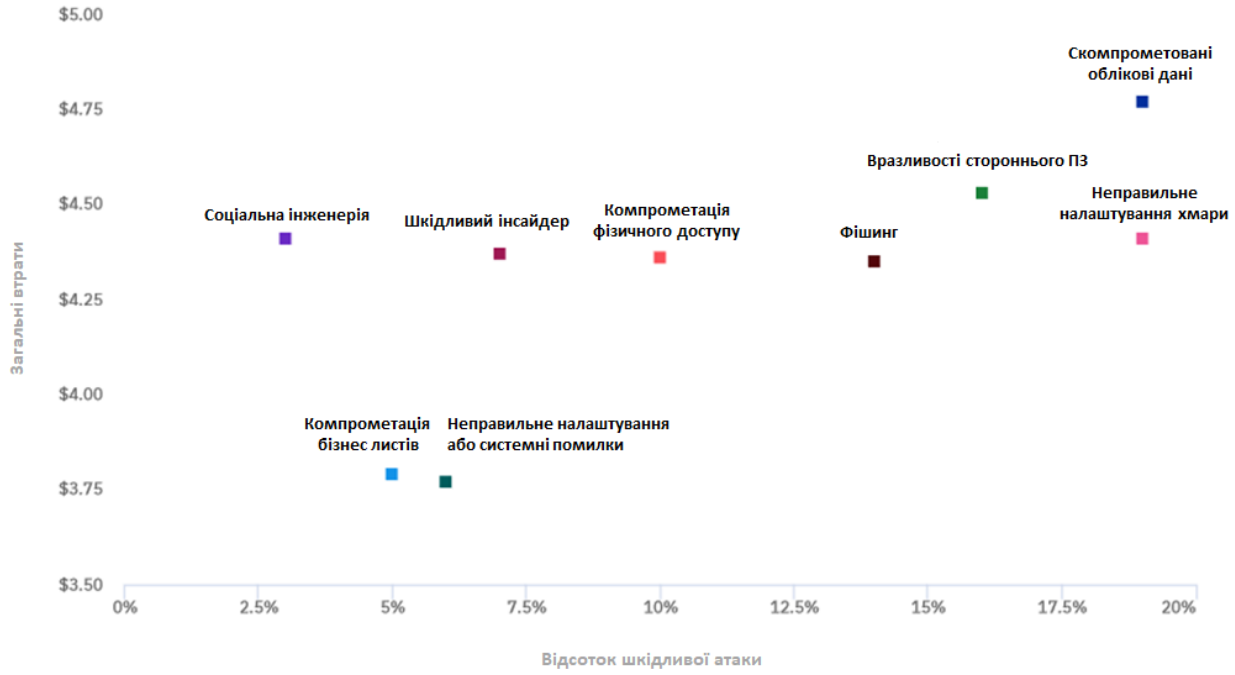

Рис. 1.9. Середня вартість та частота шкідливих порушень передачі даних

На рисунку показані дев'ять первинних векторів загрози у шкідливих порушеннях на ділянці розсіювання, з відсотками порушень, представлених на осі X та середню загальну вартість на осі Y. Компрометовані облікові дані - це вектор загрози, яка є найголовнішою у верхньому правому куті графіка, що показує його потужну комбінацію частоти та витрат у зловмисних порушеннях даних. Хоча й інсайдерські загрози виникають всього в 7% випадків, проте вони не поступаються по загальній ціні втрат від таких атак.

Спеціалісти компанії Proofpoint базуючись на даних з Ponemon Institute створили глобальний звіт в якому описали загальну вартість втрат від інсайдерських атак [5].

На рисунку показано розподіл інсайдерських інцидентів у порядку висхідного порядку, або розміром компаній-учасників. Як видно, вихідний схил свідчить про те, що частота інсайдерських інцидентів позитивно співвідноситься з організаційним розміром. Кореляція найбільш важлива для великих компаній.

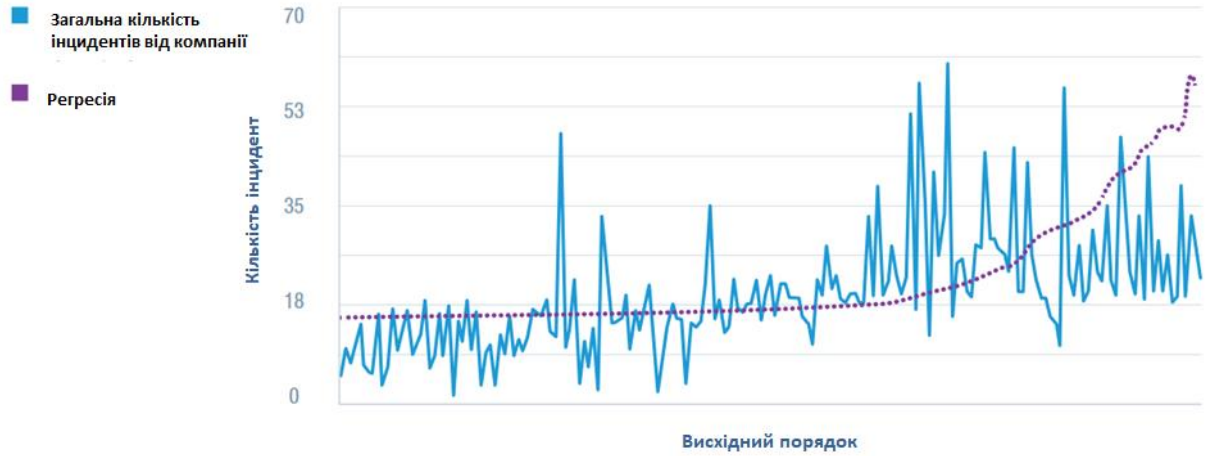

Рис. 1.10. Кількість ІА в порядку зростання в залежності від розміру компанії

Загальна кількість річних витрат, скоригованих для погляду на посібник компаній, повідомляється на рис. 11. Компанії з 25,001 та 75 000 працівників пережили найбільшу загальну вартість втрат у розмірі 17,92 мільйонів доларів, тоді як ті, хто має 500 до 1000 співробітників, мали найнижчу ціну втрат від атак інсайдерів на 6,92 мільйона доларів.

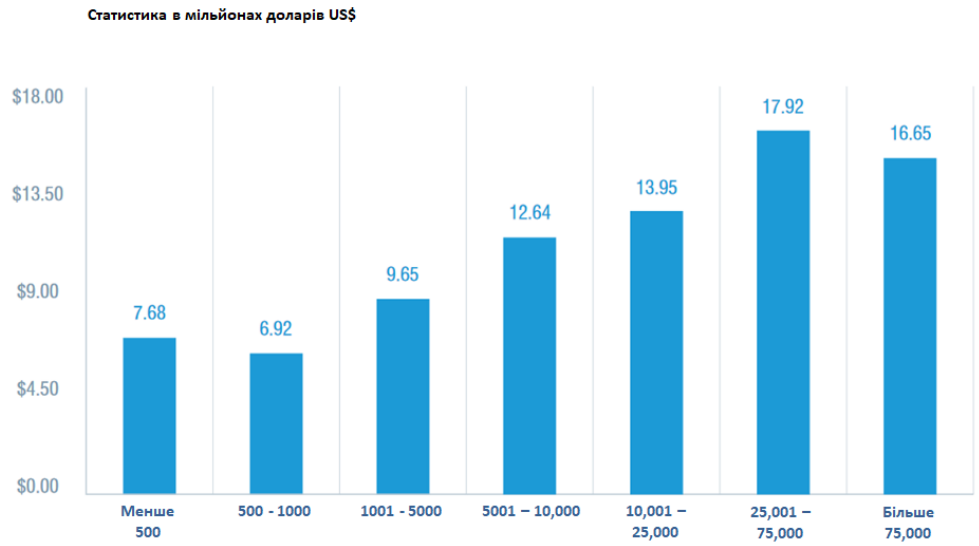

Рис. 1.11. Середня вартість діяльності

1.3. Статистика компрометації організації по типу актива

У рамках постійних зусиль компанія CERT визначила ряд параметрів - власник активів, тип активів та класифікацію, що можливо використовувати для сукупності та аналізу цілей інсайдерських інцидентів.

Наведена нижче діаграма показує розміри центральної інсайдерської загрози інцидентного корпусу цільової таксономії [7].

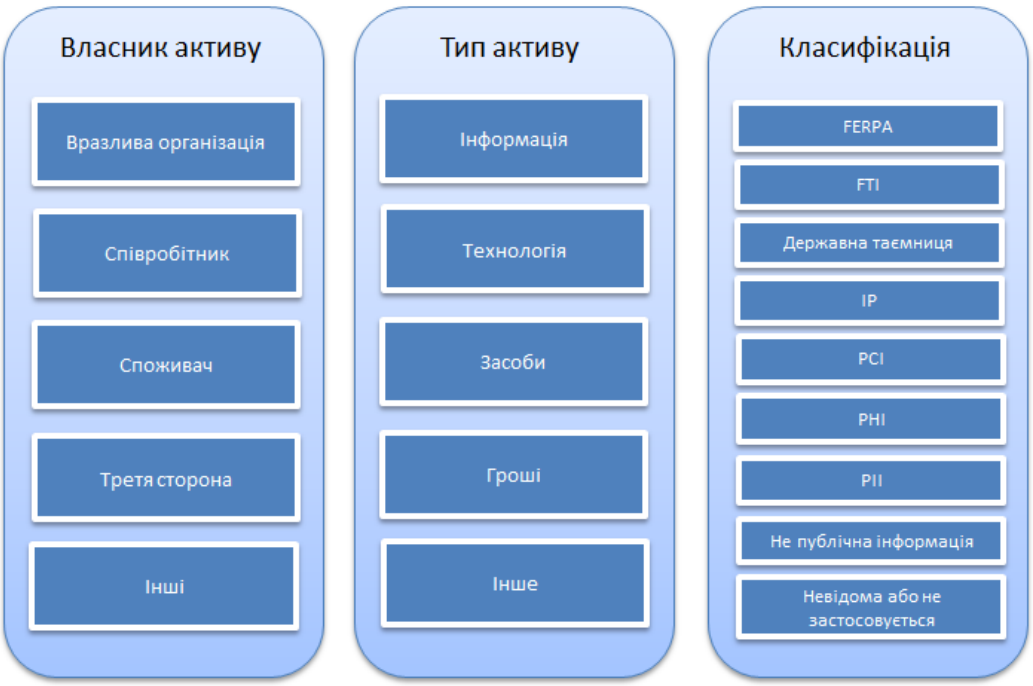

Рис. 1.12. Діаграма розподілення власника активу до його типу та класифікації

Власник активу відповідає суб'єкта, відповідальному за управління активами або суб'єкту активу. Наприклад, працівник буде власником своїх даних, збережених у системах роботодавця, таких як інформація про людські ресурси або особисті файли, збережені на робочих пристроях. Клієнт буде власником інформації про оплату клієнтів. Категорії власників активів поінформовані моделлю управління сертифікатом (CERT-RMM), що визначає та керуюче домен (ADM).

Можливо, не дивно, найпоширеніший власник активів через типи загрозу інсайдерської загрози - шахрайство, крадіжка IP, саботаж та інші - це організація потерпілого. Зазвичай набагато менше цільових активів, що належать працівникам, третій стороні або іншім. Наведений нижче графік показує активи в центрі інсайдерської загрози, розбита за власником та типом випадків.

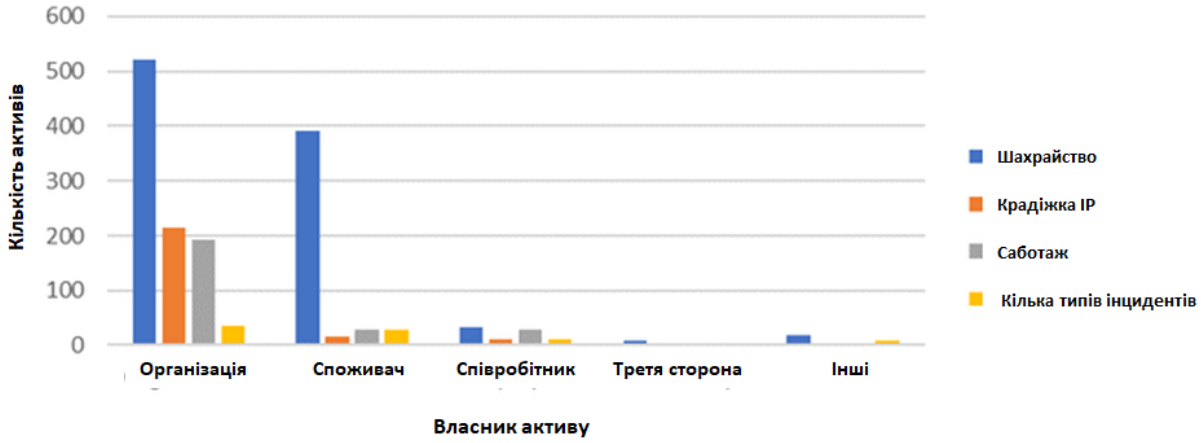

Рис. 1.13. Графік співвідношення власника активу до типу випадків

Інциденти шахрайства, які складають більшість випадків інцидентів, були пов'язані з найбільшою кількістю цільових активів, що належать, перш за все, організаціям та споживачами [7].

Тип активу - це середовище, в якому існує актив. Як видно на графіку, інформація є найчастіше цілеспрямованим типом активів у всіх типах інцидентів. Гроші орієнтовані виключно в інцидентах шахрайства. Можна визначили основні випадки, на які були спрямовані інсайдерські загрози.

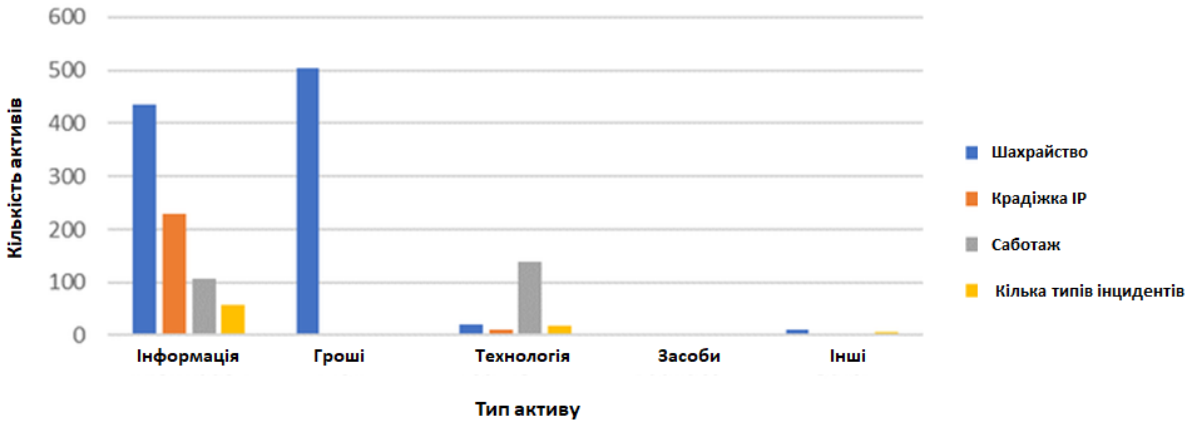

Рис. 1.14. Графік співвідношення актива до типу випадків

Класифікації, що використовуються в системній таксономії центру CERT, відносяться до конкретних видів конфіденційних даних. Цей вимір відноситься до будь-яких захисту або позначення, які будуть надані до активу. Інсайдерська загроза класифікації включають наступні категорії:

- Сімейні освітні права та Закон про конфіденційність (FERPA): відноситься до типу даних, таких як студентські освітні записи
- Урядова податкова інформація (FTI): регульований клас інформації, з конкретним керівництвом, наданим публікацією внутрішніх доходів (IRS) 1075.
- Інтелектуальна власність (IP): може посилатися на ряд різних видів активів, але полягає в тому, що може бути захищений через патент, авторське право, товарний знак тощо.
- Інформація про платіжну картку (PCI): будь-яка інформація про обліковий запис або іншу особисту інформацію (PII), пов'язану з транзакцією платежу або зберіганням таких даних. Організації повинні дотримуватися стандарту безпеки даних про безпеку платіжної картки (PCI DSS), якщо вони були процесором таких даних.
- Захищена інформація про здоров'я (PHI): інформація, що підлягає захисту закону про збереження інформації та підзвітності (HIPAA).
- Особисто ідентифікована інформація (PII): інформація про людину (або особи), що, при використанні окремо або в комбінації, може бути використана для

ідентифікації конкретної людини. Загальні приклади PII включають ідентифікатори, такі як назва, народження, та номер соціального страхування.

- Невизначені данні: як правило, дані, що беруть участь у інсайдерських інцидентах, де інші класифікації не застосовуються.

Наведений нижче графік показує лише цільові інформаційні активи, розбиті за класифікацією та відомим типом інциденту. Найчастіше визначена класифікація була недержавною. Рідше була вплинула інформація FERPA, що відображає невелику кількість інцидентів у нашому корпусі, що впливає на освіту.

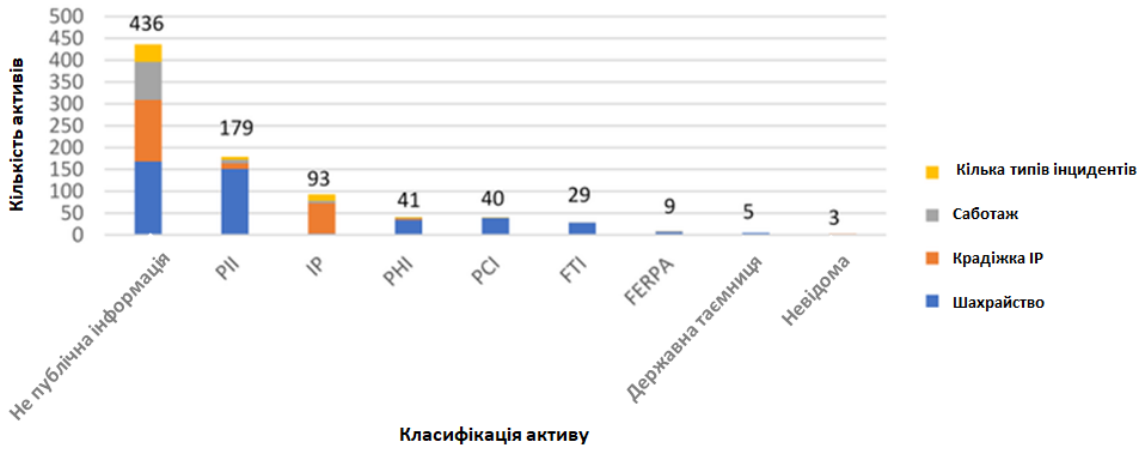

Рис. 1.15. Графік співвідношення класифікації активу до типу випадків

Четвертий, менш жорсткий, розмір таксономії є конкретним активом або активами, орієнтованими на інсайдер. З 1,643 загальної цілей через 1262 інцидентів, компанія CERT виявила 105 конкретних активів.

Як видно на графіку, інсайдер, орієнтовані між 1 і 10 активами на інцидент.

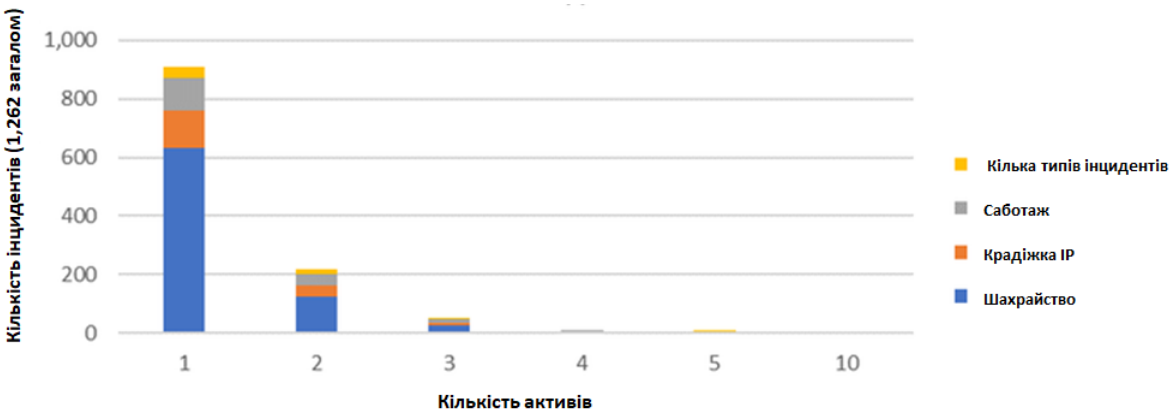

Рис. 1.16. Графік співвідношення кількості випадків до їх виду [7]

Понад три чверті - 76,2% інсайдерів, спрямованих лише на один актив. Менше 17,8% інсайдерів націлені на два активи. Приблизно 5,2% інсайдерів цільові цілі активи або більше. Тільки один інсайдер, у викраденій інциденті, орієнтований на 10 активів. Найбільш поширеними цільовими активами в інцидентах шахрайства були фонди компанії (193 цілі, 24,6% випадків шахрайства), PII (141 цілі, 18,0%) та випущені чеки (137 цілей, 17,5%). З огляду на характер шахрайських інцидентів, можливо, було лише один вид активу, але ці активи можуть задіяти кілька записів або екземплярів.

1.4. Статистика компрометації організації по пристроям

В центрі Cert National Insider Center, збирається, аналізується та класифікуються інсайдерські інциденти, щоб заповнити програму інсайдерської загрози інсайдера, та моніторинг еволюційного ландшафту загроз. Нещодавно розширили таксономію класифікованих пристрої, які впливають на інсайдерів.

Термін "уражений пристрій" вткористовується, щоб описати систему, яка була змінена або запущена під час інцидент інсайдерської загрози. Вплив на ці пристрої можуть варіюватися від незначних модифікацій системних журналів для передачі шкідливого коду, який приймає сервер в автономному режимі. Намір і мотив може змінюватися також: інсайдер може безпосередньо націлюватися на систему або пристрій, випадково вплинуло на це по ходу нападу, або змінити його, щоб приховати атаку.

В цілому, найчастіше ураженими пристроями в CERT - є серверами баз даних [8].

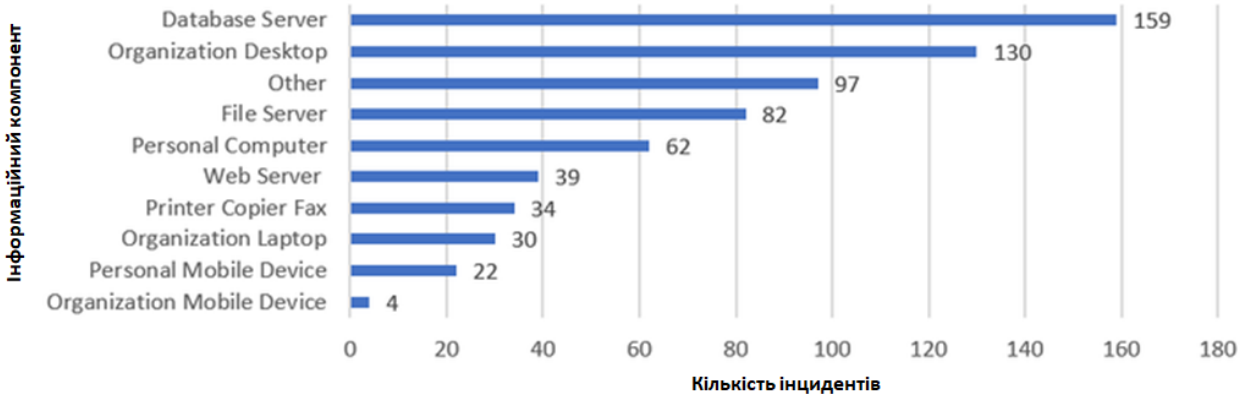

Рис. 1.17. Графік співвідношення кількості випадків до уражених інформаційних компонентів

Ми можемо ще більше зламати вищезгадані дані, щоб показати розподіл уражених пристроїв у кожному з чотирьох основних типів інсайдерських інцидентів: шахрайство, крадіжка інтелектуальної власності (ІП), саботаж та неправильне використання [8].

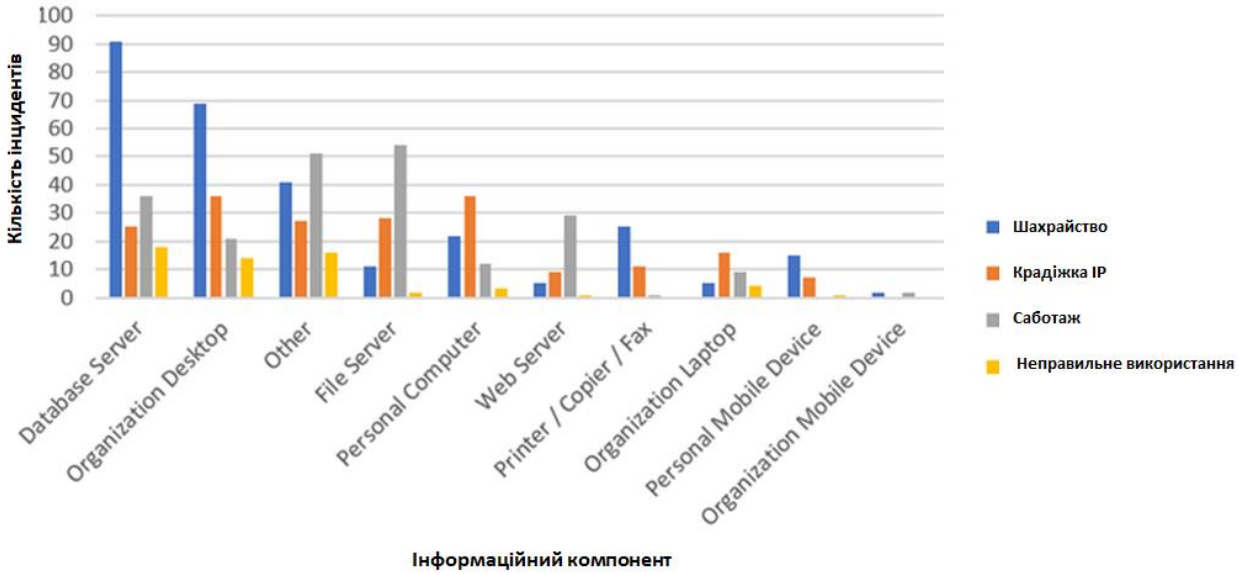

Рис. 1.18. Графік співвідношення уражених інформаційних компонентів до типу випадків

Спеціалісти компанії Fortinete в своєму звіті підтверджують що злочинці вважають більшу можливість у націленні на бази даних (56%) та корпоративні файлові сервери (54%), що представляють найвищий ризик, з подальшим кінцевими точками (51%) та мобільними пристроями (50%).

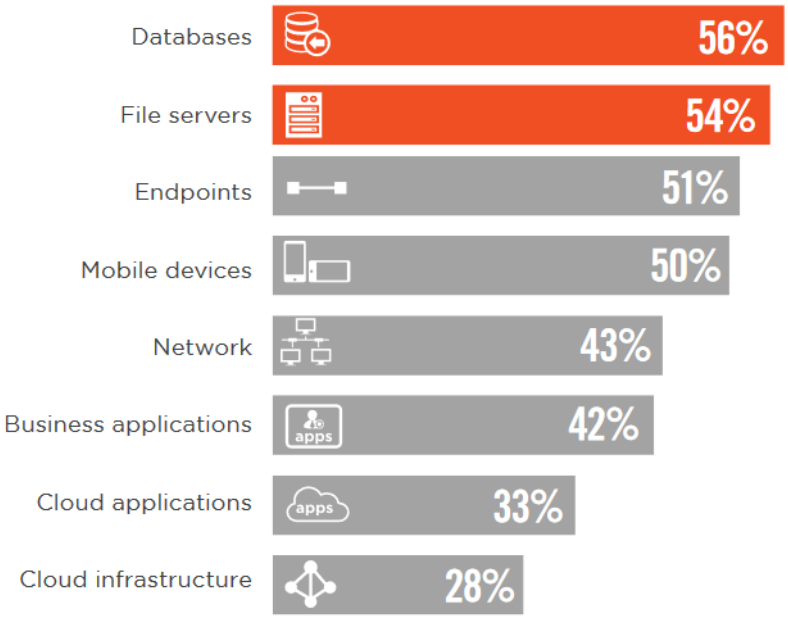

Рис. 1.19. Найбільш вразливі інформаційних компонентів до інсайдерських атак [9]

Підсумки для найбільш часто постраждалих пристроїв від інсайдерів та їх цілей такі:

- Шахрайство: сервери баз даних, а потім настільні комп'ютерів. Ці пристрої можуть впливати, коли інсайдер змінюють організаційні записи, щоб приховати відсутні кошти.
- Крадіжка IP адреси: персональні комп'ютери та організаційні настільні комп'ютери. Інсайдер може зберігати вкрадений IP на робочих місцях організації, перш ніж екфільтрувати дані до своїх особистих пристроїв для подальшого використання.
- Неправильне використання: сервери баз даних. Інсайдери можуть неправильно використовувати організацію доступу до бази даних, щоб порушити конфіденційність даних [8].
- IT саботаж: файлові сервери. У багатьох випадках інсайдери видаляють критичні дані з файлових серверів, щоб перевести систему до автономного режиму.

Кожен тип випадку включає в себе ряд інших уражених пристроїв, які не вписуються в таксономію та можуть бути використані інсайдером.

Висновок до розділу 1

Причин для інсайдерських загроз може бути декілька з різним джерелом виникнення. В деяких випадках люди використовують свій доступ до конфіденційної інформації для особистої чи фінансової вигоди. В інших, інсайдери узгодили з третіми сторонами, такими як інші організації або зловмисні групи, і діють від їх імені, щоб отримати доступ зсередини мережі та ділитися власною або конфіденційною інформацією.

Найчастіше інсайдери впливають на файлові сервери та сервери баз даних. При цьому все ще залишається небезпека друку та винесення інформації на фізичних носіях через спеціальні або особисті пристрої.

З кожним роком втрати від ІЗ зростають та необхідно вдосконалювати та побудувати стійкий захист проти цих загроз.

РОЗДІЛ 2 МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ ІНСАЙДЕРСЬКИХ АТАК

Ефективність організації в багатьох випадках залежить від збереження конфіденційності, цілісності та доступності інформації. В даний час однією з найбільш актуальних загроз у сфері інформаційної безпеки є витік конфіденційних даних від різного роду інсайдерів.

2.1 Методи та засоби протидії від інсайдерських атак фізичного впливу

Антивіруси, міжмережеві екрани і системи аутентифікації та більша частина традиційних засобів захисту не здатні забезпечити ефективний захист від внутрішніх інсайдерів.

Можемо виокремити основні фізичні проблеми безпеки [10]:

1. Інфільтрація/ексфільтрація фізичної властивості - такі заходи, як винесення змінних носіїв за об'єкт які можуть містити конфіденційну інформацію. Один з таких яскравих прикладів такого роду атак відбувся в США, коли Едвард Сноуден виступив в ролі інсайдера та оприлюднив злочини з стеження владою США перед своїм народом. Інформацію він виніс за периметр всередині кубика-рубика, записану на MicroSD карті.
2. Неправильне припинення фізичного доступу працівника або доступу по карті. Дуже часто в невеликих бізнес центрах вам достатньо буде сказати назву організації для того щоб потрапити за турнікет або скористатися незаблокованим пропуском колишнього співробітника цієї організації.
3. Несанкціонований доступ до об'єкту - співробітники, що пропускають неуповноважених осіб, що йдуть через відкриті двері за картою працівника, також відомий метод як «piggybacking». Зазвичай коли ми бачимо що людина несе наперед себе велику коробку з приладдя або інструментами - ми підсвідомо допомагаємо людині в такій ситуації та притримуємо двері або турнікет. Цим можуть скористатися зловмисники для проникнення всередину периметру.

4. Слабка фізична безпека. Загальні питання, такі як недостатнє покриття «сліпих зон» або недостатнє розділення обов'язків для фізичного контролю доступу. Компанії можуть економити на кількості та густоті розміщення відеокамер спостереження що призводить до збільшення кількості зон які ми не можемо розгледіти.

5. Співробітник використав несанкціоновану робочу станцію – це співробітники, які здатні фізично увійти в інший офіс або робоче місце і отримати доступ до їх робочої станції. Зазвичай жертва такого співробітника навмисно або з необережності залишає увімкнений комп’ютер або пароль в полі зору на робочому місці. Це значною мірою спрощує процес використання станції жертви для злоякісних цілей.

6. Злом і проникнення або фізичне знищення - співробітники вриваються на підконтрольні об’єкти та крадуть фізичне обладнання. Основна мета таких дій – завдання матеріального збитку та спроба заволодіння конфіденційною інформацією на фізичних пристроях.

7. Кадрові питання - технічний персонал, який викрадає конфіденційну інформацію або направлений на порушення фізичної безпеки. Поширена практика не тільки в Україні а й по всьому світу коли охоронці чи прибиральниці крадуть інформацію та перепродають її зловмисникам.

8. Неправильне видалення або знищення інформації в організації. Дуже часто призводить до можливості відновити початкові данні та відшукати компрометуючі матеріали на організацію або виявити облікові данні користувачів які були записані на звичайному листку паперу [10; 11].

Сильний фізичний контроль безпеки важливий як фізичне здоров’я кожної людини що допомагає запобігти деяким проблемам. Фізичний контроль безпеки включають в себе запобігання несанкціонованого фізичного доступу до захищених сегментів організації, а також запобігання прямої фізичної крадіжки. Щоб пом'якшити ризики та захищати критичні активи від інсайдерських загроз, організації повинні встановити ефективну програму інсайдерської загрози, повністю інтегрована в стратегію управління ризиками, беручи до уваги цифрові

та фізичні простори, одночасно. Крім того, застосування фізичного контролю безпеки повинна бути структурована в шарах, що у багатьох випадках перекриваються. Методи ідентифікації ризику включають мозковий штурм, інтерв'ю, контрольні списки, статистичні дані, історичні дані та використання та використання та методи моделювання, такі як атаки дерев та моделювання загрози. Визначені закономірності після аналізу та оцінки ризику повинні використовуватися для поліпшення загальної програми інсайдерських загроз. Конвергенція їх та фізичної безпеки з аналітикою повинна спільно працювати над цілями після програми управління ризиками та чітко визначеною політикою безпеки. Наприклад, зусилля з метою забезпечення доступу до баз даних, електронної пошти та організаційних мереж об'єднуються з системою контролю та спостереження за доглядом, а всі разом є частиною аналітичного підходу до доставлення відповідної інформації та стимулювати рішення, що керуються даними.

Розглянемо основні варіанти вирішення фізичних проблем безпеки:

1. Інфільтрація/ексфільтрація фізичної властивості. Для індентифікування на фізичному рівні організації встановлюють пункти контролю які сканують працівників та особисті речі на наявність прихованих пристроїв чи змінних носіїв. На програмному рівні ефективність застосування компаніями превентивних заходів контролю набагато вища за фізичні. Наприклад, блокування доступу по USB до робочої станції та використання програмних комплексів контролю переміщення файлів для індентифікації, аудиту та видимості інцидентів винесення інформації на сторонні носії інформації.

2. Неправильне припинення фізичного доступу працівника або доступу по карті. Зазвичай організації використовують «безликі» ключ карти які не закріпляються за працівником. В такому разі після звільнення співробітника здавалося достатньо забрати пропуск, проте якщо в інсайдера є RFID сканер, то він зможе відтворити N-ну кількість пропусків. Тому, першочерговим варіантом для протидії доступу буде видання іменних ключ карт з закріпленням за обліковим записом співробітника в системі з можливістю аудиту входів та

виходів з приміщення. Додатковим засобом є встановлення системи розпізнання обличчя на критично важливих ділянках організації.

3. Несанкціонований доступ до об'єкту - «piggybacking». Основним та першочерговим способом протидії є навчання та постійні тренінги співробітників з моделювання ситуацій при яких вони зробили висновок, що допомагаючи людині притримавши двері або турнікет – ви стаєте співучасником інсайдерської загрози.

4. Слабка фізична безпека. Компанії з низьким бюджетом економлять на видимості та покритті сліпих зон при орендуванні вже готових приміщень та пунктів контролю, тим самим збільшують бюджет на розвиток і врешті решт з часом приходять до процесу покращення фізичної безпеки. В період карантину коли співробітники працюють віддалено, адміністраторам важче проконтролювати фізичну безпеку, тому вони розраховують на програмні методи шифрування інформації та створення процедур використання захищених каналів передачі інформації.

5. Співробітник використав несанкціоновану робочу станцію. Ситуацію можливо швидко визначити через камери спостереження в приміщені та застосувати запобіжні фізичні заходи. Як спосіб протидії такому інцидентові, розмежовувати робочі простори відділів, департаментів, керівників. Обов’язковим та найефективнішим запобіжним заходом є проведення тренінгів для співробітників. З програмної сторони захисту, можливе впровадження систем доступу до робочих станцій по ключ-картах або тільки з підтвердженої особи шляхом сканування його обличчя через веб-камеру.

6. Злом і проникнення або фізичне знищення. Для забезпечення безпеки організаціям потрібно розприділити робочі простори різних відділів, тим самим, ускладняється процес фізичного проникнення. Щоб зберегти конфіденційну інформацію всередині компанії, адміністратори повинні першочергово використовувати шифрування дискових масивів для робочих станцій та серверів. Іншим варіантом мінімізації втрат для організації від даного виду загрози є використання тонких клієнтів для роботи користувачів організації, які будуть

підключатися до термінальних серверів під час робочого процесу. Тому, якщо інсайдер викрадає фізичний пристрій, інформація залишається в рамках організації.

7. Кадрові питання. Технічний персонал може отримати доступ в будь-яку кімнату в організації, тому важливо навчити співробітників не залишати конфіденційну або компрометуючу інформацію у відкритому вигляді та утилізувати її шредерами. При цьому камери спостереження залишаються нашими очима для аудиту будь-яких дій співробітників.

8. Неправильне видалення або знищення інформації в організації. Утилізація інформації важлива. Зловмисник перебираючи тони сміття може віднайти або відновити пароль користувача чи адміністратора і це може відкрити додатковий вектор для атаки. Жорсткі диски не затирають данні а тільки видаляють посилання на файл, тому будь-яку інформацію можливо відновити. Для фізичних матеріалів, в тому числі конфіденційних даних організації використовують шредер. Для програмних файлів, наприклад інформація на жорстких дисках, кращим методом буде по-бітовий перезапис хаотичними даними.

Розглянувши основні фізичні проблеми захисту інформації, можливо виокремити ключові міри захисту під час інсайдерських атак:

- Тренінги співробітників
- Встановлення камер відео-спостереження
- Система пропусків з закріпленням смарт-карти за особою
- Розмежування робочого простору між різними департаментами
- Використання засобів знищення інформації

2.2 Методи та засоби протидії від інсайдерських атак програмного впливу

В еру цифрових технологій кожний із нас використовує електронний пристрій від смартфона, планшета та смарт годинників до розумних асистентів,

мікрохвильових печей та холодильників. Проте, чи задумувався хоч хтось з нас яку інформації збирають ці системи, де вони її зберігають та чи не передають на сторонні ресурси. Як в повсякденному житті, так і в середині компанії, кожного пристрою, можуть відкритися різноманітні способи передачі інформації на зовні. Елітні хакерські групи з усього світу можуть спонсорувати інсайдерів під покровом всесвітньої паутини націлюючись на великі організації та різноманітними способами намагаються отримати доступ до секретів компаній. Набагато простіше це зробити в добу цифровізації коли тобі не потрібно виходити з дому чи штаб квартири.

Основні вектори атак під час інсайдерських загроз можуть виникати на наступні компоненти:

- Бази даних
- Файлові сервери
- Кінцеві точки (робочі станції)
- Мобільні пристрої
- Взаємодія на мережевому рівні
- Бізнес застосунки
- Хмарні застосунки
- Хмарна інфраструктура.

При цьому інсайдер може використовувати різноманітні способи для проникнення та отримання конфіденційної інформації. Фішинг, зловживання привілейованим доступом, цілenаправлене вивантаження інформації з робочого компютера – це все приклади способів отримати несанкціонований доступ до конфіденційної інформації та передати її третім особам. Співробітник, адміністратор, системний інженер, підрядник або аудитор – це може бути будь-хто і кожен з них матиме величезний спектор можливостей, тому доцільним рішенням буде описати технології протидії їх діям.

Основні правила для забезпечення всебічного захисту від інсайдерських загроз:

1. Використання шифрування дисків на робочих станціях та серверах.

2. VPN сервіси для безпечного підключення в середину організації та на зовні.
3. Системи поведінкового аналізу (UEBA)
4. Системи протидії витоку інформації (DLP)
5. Системи контролю привілейованого доступу (PAM)
6. Керування ідентифікацією та доступом (IAM)
7. Системи розслідування інцидентів ІБ (SIEM)
8. Аудит інфраструктури

Кожна компанія використовує численні засоби для захисту від зовнішніх атак, але куди більшу шкоду здатний нанести людина, що працює всередині системи. Відповідно, виникає питання про внутрішню безпеку, яку необхідно ретельно продумати.

1) Шифрування дисків важливий компонент комплексу заходів протидії інсайдерським загрозам. Він рятує організації від фізичного впливу з сторони інсайдерів які викрали робочу станцію та намагаються вилучити жорсткий диск для отримання конфіденційної інформації. Перш за все це протидія фізичним інсайдерам але як на рахунок загрози з середини організації. Прикладом такої атаки може бути адміністратор до якого звернувся працівник з несправністю в робочій станції. Адміністратор щоб не тратити час замінив повільно працюючий жорсткий диск та поклав зламаний на полицю. Під час інвентаризації, адміністратор в ручному режимі передивлявся вміст дисків, перевіряв їх справність та знайшов конфіденційну інформацію співробітника або комерційну таємницю компанії. Якщо б інформація була зашифрована, то для адміністратора був тільки 2 варіант – очищення диска, що призвело б до затирання даних або утилізація диска.

Для Windows систем вбудованою утилітою шифрування дисків є BitLocker, для MacOS – FileVault2, для Linux/Unix систем – eCryptfs або його аналоги. Іншим спеціалізованим та вільним для використанням ПЗ якому віддають перевагу спеціалісти ІБ є TrueCrypt або його аналог VeraCrypt.

Програма VeraCrypt здатна заховати ваші файли в надійний контейнер або навіть у секретний контейнер усередині іншого захищеного контейнера. VeraCrypt може:

- створювати зашифровані контейнери для шифрування інформації;
- створювати приховані контейнери всередині інших контейнерів;
- робити шифрування окремого диску на пристрої.
- Шифрувати дискові масиви

Для користувачів у VeraCrypt є можливість використовувати наступні алгоритми шифрування: AES, Serpent, та Twofish. Додатково доступні 5 комбінацій цих алгоритмів: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES і Twofish-Serpent. Втілені криптографічні хеш-функції: RIPEMD-160, SHA-256, SHA-512 та Whirlpool.

Таким чином, VeraCrypt надає стійкий захист даних на дисках. Крім цього компанії можуть використовувати готові корпоративні рішення безпеки відомих брендів як ESET Endpoint Encryption або McAfee Drive Encryption.

2) На теперішній час звичайною практикою є використання VPN сервісів для приховання трафіку з зовні та мінімізації прямих хакерських атак. Для співробітників в період карантину стало нормою використання VPN сервісів в щоденній роботі, тому аналізуючи трафік ми можемо дізнатися які сайти відвідували співробітники та чи шукав хтось з них роботу, оскільки наступним кроком може бути винесення таємниць компанії разом з собою. VPN вирішують наступні питання ІБ:

1. Аналіз трафіку та його заборона.
2. Аудит входів в систему на робочі станції або сервери.
3. Попередження про вивантаження файлів на сторонні ресурси.

Таким чином, ми можемо отримати ціну інформацію про шлях співробітника всередині організації від робочої станції до сервера та куди вивантажувалася інформація з нього на сторонній ресурс чи домашній компютер.

3) Ви можете легко вкрасти ім’я користувача та пароль працівника, але набагато складніше імітувати нормальну поведінку людини. Коли користувач

входить у систему і його поведінка відрізняється від типової, то починають надходити сповіщення UEBA. Система працює, переглядаючи відхилення у поведінці користувача або активу порівняно з попередніми діями або групами рівноправних користувачів. Рішення UEBA мають три основні компоненти, які мають вирішальне значення для їх функціонування:

1. аналітика даних що використовує дані про "нормальну" поведінку користувачів та організацій, щоб створити профіль того, як вони зазвичай діють. Потім можуть застосовуватися статистичні моделі для виявлення незвичної поведінки та попередження системних адміністраторів.

2. інтеграція даних означає, що системи UEBA здатні порівнювати дані з різних джерел - таких як журнали, дані захоплення пакетів та інші набори даних - з існуючими системами безпеки.

3. представлення даних - це процес, за допомогою якого системи UEBA повідомляють свої висновки. Зазвичай це робиться шляхом надсилання запиту аналітику безпеки для розслідування незвичної поведінки.

Основний фактор UEBA полягає в тому, що він дозволяє автоматично виявляти широкий спектр кібератак. Сюди входять інсайдерські погрози, компрометовані акаунти, атаки з перебору паролів, створення нових користувачів та порушення даних.

4) Важливо реалізувати ефективну стратегію, щоб захистити чутливу інформацію вашої організації від порушення злочинців або випадкового витоку недбайливими користувачами. Багато витоків даних є результатом того, що користувачі відгукуються на фішинг-повідомлення або підводне повідомлення про фішинг, у якому відправник видає себе за особу, уповноважену отримувати дані. Дані також можуть просочуватися зловмисними програмами та вірусами, які читають приватні дані, а потім передають їх хакеру. Запобігання втратам даних або DLP - це термін, що позначає стратегії запобігання витоку або знищенню даних компанії, особливо конфіденційних даних.

Ефективна система DLP сканує всі вихідні електронні листи та інший мережевий трафік, шукаючи заздалегідь визначені шаблони, які можуть вказувати на конфіденційні дані.

В рамках створення таких систем вирішуються завдання:

- запобігання витоків конфіденційної інформації по основних каналах передачі даних.
- витікаючий веб-трафік (HTTP, FTP, P2P та ін.)
- внутрішня та зовнішня електронна пошта
- системи обміну миттєвими повідомленнями та локальний чи мережевий друк
- контролю доступу до пристроїв і портів введення та виведення, до яких відносяться: дисководи, CD-ROM, USB — пристрої, інфрачервоні, принтерні (LPT) і модемні (COM) порти.

Після виявлення програмне забезпечення DLP може зупинити відхід конфіденційних даних, виконавши одну з наступних дій:

1. Блокування дій користувача: Коли внутрішній користувач намагається отримати доступ або надсилати дані, які слід зберігати в таємниці, системи DLP можуть блокувати їх у цьому. Деякі системи DLP унеможливлюють копіювання даних у буфер обміну свого комп'ютера для копіювання та вставлення.
2. Повторна реакція: відредагувати щось означає приховати чи усунути. Наприклад, перероблені юридичні документи матимуть певний текст, прихований для приховування інформації. У системі запобігання втратам даних система DLP може видалити або приховати конфіденційну інформацію, виявлену в даних, замінивши її на нульове значення або серію безглуздих символів, наприклад "****".
3. Токенізація: Токенізація - це процес, який замінює значення даних маркером, що відповідає цьому значенню. Маркер можна використовувати так само, як і реальне значення, і таким чином фактичне значення не піддається впливу.

Щоб захистити свої критичні дані від атак та аварій, компанії використовують багатошарову стратегію запобігання втратам даних. Жоден інструмент DLP для підприємства не може вирішити всі проблеми безпеки даних; DLP вимагає комплексного процесу. Для початку оцініть прокласифікувати дані та знати де знаходиться конфіденційна інформація.

5) В сучасних реаліях не складає великих труднощів проконтролювати звичайних користувачів але ще складніше створити рівень контролю за адміністраторами які можуть мати різноманітний набір прав що дозволить їм вишуканим способом провести атаку. До них належать працівники, підрядники, віддалені або навіть автоматизовані користувачі. Деякі з цих користувачів, а точніше адміністратори, можуть замінити існуючі протоколи безпеки. Це велика вразливість якщо адміністратор може зробити несанкціоновані зміни в систему, отримати доступ до заборонених даних, а потім приховати свої дії та уникнути проблеми. Велика загроза якщо зловмисник може отримати доступ до системи через облікові данні адміністратора. Привілейований доступ також може бути отриманий за допомогою інших засобів. Наприклад, користувач, який має фізичний доступ до комп'ютера, зазвичай може перезавантажити комп'ютер з накопичувача пам'яті DVD або USB та виконати будь-які потрібні операції на комп'ютері. Таким чином, користувачі з фізичним доступом також іноді можуть вважатися привілейованими користувачами.

Керування привілейованим доступом (PAM) відноситься до систем та процесів, що дозволяють організаціям краще контролювати та контролювати можливості того, хто може отримати привілейований доступ до комп'ютера чи інформаційної системи.

Рішення PAM пропонує безпечний, спрощений спосіб авторизувати та контролювати всіх привілейованих користувачів для всіх відповідних систем. PAM дозволяє:

- Надати привілегії користувачам лише для систем, на які вони авторизовані та мають працювати з ними кожного дня.

- Надати доступ лише тоді, коли це потрібно та скасувати доступ, коли необхідний термін дії закінчиться.
- Уникати необхідності у привілейованих користувачів мати або потребувати локальних або прямих системних паролів.
- Центрально та швидко керувати доступом через різний набір різнорідних систем.
- Створити незмінний слід аудиту для будь-якого привілегійованого входу.

Рішення привілейованого управління доступом відрізняються за своєю архітектурою, але більшість пропонують такі компоненти, що працюють узгоджено. Менеджер доступу - Цей модуль PAM регулює доступ до привілейованих облікових записів. Це єдиний пункт визначення політики та застосування політики для управління привілейованим доступом. Привілейований користувач запитує доступ до системи через менеджер доступу. Менеджер доступу знає, до яких систем користувач може отримати доступ та на якому рівні привілеїв. Такий підхід знижує ризик того, що колишній працівник збереже доступ до критичної системи. Сейф паролів - найкращі системи PAM не дають привілейованим користувачам знати фактичні паролі для критичних систем. Це запобігає, наприклад, ручний підбір фізичного паролю. Менеджер сесій – ситуація коли контролю доступу недостатньо. Вам потрібно знати, що насправді привілейований користувач робив під час адміністративного сеансу. Менеджер сесій відстежує дії, здійснені під час сеансу привілейованого облікового запису. Найбільшою перевагою PAM для організації є безпека даних. Хакерам надзвичайно просто переміщатися бічно по мережі. PAM будує барикади у вашій мережі, які можуть містити та забороняти рух інфільтраторів по вашій мережі. Це барикади прав доступу. Хакера не зупинятимуть, але вони будуть обмежені. Хакерам потрібно буде викрасти кілька облікових записів, щоб викрасти дані, що робить їх зусиллями вагомими, і це купує вам час для виявлення та нейтралізації їх зусиль.

6) Керування ідентифікацією та доступом (IAM) гарантує, що потрібні люди та посадові ролі у вашій організації (ідентифікації) зможуть отримати доступ до інструментів, необхідних для виконання своєї роботи. Системи керування ідентифікацією та доступом дозволяють організації керувати додатками співробітників, не входячи в кожну програму як адміністратор. Системи керування ідентифікацією та доступом дозволяють організації керувати низкою ідентифікаційних даних, включаючи людей, програмне та апаратне забезпечення, як-от робототехніка та пристрої інтернету речей. IAM потрібен компаніям, щоб забезпечити безпеку в Інтернеті та підвищити продуктивність співробітників [12].

- Безпека. Традиційна безпека часто має один момент збою - пароль. Якщо пароль користувача зламано або, що ще гірше, адреса електронної пошти для відновлення пароля, ваша організація стає вразливою для атаки. Служби IAM звужують точки збоїв і підтримують їх за допомогою інструментів, щоб уловити помилки, коли вони зроблені.
- Продуктивність. Після того, як ви ввійдете на свій головний портал IAM, вашому співробітнику більше не доведеться турбуватися про правильний пароль або правильний рівень доступу для виконання своїх обов’язків. Кожен співробітник не тільки отримує доступ до ідеального набору інструментів для своєї роботи, його доступом можна керувати в групі або ролі, а не окремо, зменшуючи навантаження на ваших IT-фахівців.

Системи IAM забезпечують таку основну функціональність:

- Керуйте ідентифікаторами користувачів. Системи IAM можуть бути єдиним каталогом, який використовується для створення, зміни та видалення користувачів, або він може інтегруватися з одним або кількома іншими каталогами та синхронізуватися з ними. Керування ідентифікацією та доступом також може створювати нові посвідчення для користувачів, яким потрібен спеціалізований тип доступу до інструментів організації.
- Ініціалізація/деініціалізація користувачів. Визначення інструментів і рівнів доступу (редактор, переглядач, адміністратор) для надання користувачеві

називається наданням . Інструменти IAM дозволяють IT-відділам надавати користувачів за ролями, відділами чи іншими групами за погодженням з менеджерами цього відділу. Оскільки визначення доступу кожної особи до кожного ресурсу займає багато часу, системи керування ідентифікацією дозволяють надавати доступ за допомогою політик, визначених на основі контролю доступу на основі ролей (RBAC). Користувачам призначається одна або кілька ролей, зазвичай на основі посадових функцій, і система RBAC IAM автоматично надає їм доступ. Надання також працює у зворотному порядку; Щоб уникнути ризиків для безпеки, які виникають із-за колишніх співробітників, які зберігають доступ до систем, IAM дозволяє вашій організації швидко заблокувати їх доступ.

- Аутентифікація користувачів. Системи IAM аутентифікують користувача, підтверджуючи, що він є тим, за кого себе видає. Сьогодні безпечна аутентифікація означає багатофакторну аутентифікацію (MFA) і, бажано, адаптивну автентифікацію [12] .

- Авторизація користувачів. Керування доступом гарантує, що користувачеві надається точний рівень і тип доступу до інструменту, на який він має право. Користувачів також можна розділити на групи або ролі, щоб великій групі користувачів могли надаватися однакові привілеї.

- Звітність. Інструменти IAM створюють звіти після більшості дій, здійснених на платформі (наприклад, час входу, доступ до системи та тип аутентифікації), щоб забезпечити відповідність та оцінити ризики безпеки.

- Єдиний вхід. Рішення керування ідентифікацією та доступом з єдиним входом (SSO) дозволяють користувачам аутентифікувати свою особу за допомогою одного порталу замість багатьох різних ресурсів. Після аутентифікації система IAM діє як джерело правди ідентифікації для інших доступних користувачеві ресурсів, усуваючи вимогу, щоб користувач пам’ятав кілька паролів.

7) Сигнатури безпеки внутрішньої загрози та управління подіями (SIEM) була розроблена для виявлення можливої зловмисної інсайдерської діяльності,

яка може призвести до IT-саботажу. Мета полягає в тому, щоб виявити особу зловмисника, який використав протокол віддаленого підключення і чи відбувається діяльність поза звичайним робочим часом, на основі емпіричних даних зловмисної інсайдерської діяльності . За відсутності єдиного стандартизованого формату реєстрації подій сигнатур представлений у двох найбільш помітних загальнодоступних форматах: Common Event Format (CEF) та Common Event Expression (CEE). Через обмеження цих форматів SIEM, описаний у детальному звіті, використовує оперативну версію запропонованих сигнатур в середовищі ArcSight. Сигнатура базується на таких ключових полях: ім’я користувача, ім’я облікового запису VPN, ім’я хосту зловмисника та те, чи використовує зловмисник SSH , Telnet чи RDP .

- Common Event Format (CEF) — це стандарт взаємодії подій, розроблений ArcSight . Метою цього стандарту є покращення сумісності інфраструктурних пристроїв шляхом встановлення загального формату виводу журналу для різних постачальників технологій. Це гарантує, що подія та її семантика містять всю необхідну інформацію. Використовуючи цей стандарт і ключові показники, визначені під час аналізу бази даних, можливо розробити дві сигнатури SIEM на основі CEF для продуктів Microsoft і Snort , щоб ідентифікувати підозрюваних зловмисників.
- Архітектура Common Event Expression (CEE) визначає відкритий і практичний стандарт журналу подій, розроблений MITRE . Як і CEF, метою CEE є покращення процесу аудиту та здатності користувачів ефективно інтерпретувати й аналізувати журнал подій та дані аудиту. Він стандартизує відношення журналу подій, нормалізуючи спосіб запису, спільного використання та інтерпретації подій. Використовуючи формат CEE, можливо розробили сигнатури на основі ключових показників інсайдерського IT-саботажу. Сигнатура ідентифікує підозрюваного зловмисника, який використовує віддалене підключення для входу у внутрішню систему організації поза звичайним робочим часом, а також реєструє час, коли подія була записана.

База даних CERT® Insider Threat Center наразі містить понад 550 випадків фактичних зловмисних інсайдерських злочинів. Майже всі інсайдери, причетні до дій IT-саботажу, перед скоєнням злочинів мали поведінкові відхилення. Приклади таких поведінкових індикаторів включають, але не обмежуються ними: конфлікти з колегами або керівниками, неналежне використання інформаційних активів організації, порушення правил та/або порушення безпеки. Ці індикатори можуть бути використані, щоб визначити, які користувачі вимагають цільового моніторингу за допомогою цих сигнатур.

Сучасні системи можуть не тільки аналізувати підключення, а ще й об’єднувати та аналізувати інформацію з різних джерел за допомогою спеціальних конекторів та універсальному формату логів CEF та CEE. Тим самим, SIEM вважається передовим продуктом який повинен бути в кожній великій організації, але не першим якщо ми говоримо про протидію інсайдерських загроз.

8) Аудиту інфраструктури приділяють не так багато уваги як іншим рішенням в організації, проте він не менш важливий для неї. Відповідність міжнародним стандартам, перевірка взаємодії компонентів, знаходження потенційних векторів атак та багато іншого можливо знайти за допомогою аудиту. Зазвичай, компанії кожного року можуть проходити аудит інформаційної безпеки — системний процес одержання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки компанії у відповідності з визначеними критеріями та показниками безпеки. При цьому вони отримують одноразовий список недоліків які потрібно усунути для безпечного функціонування організації. Аудит інформаційною системи (ІС) - це постійний системний процес отримання та оцінки об'єктивних даних про поточний стан ІС, дії і події, що відбуваються в ній, що встановлює рівень їх відповідності певному критерію (внутрішнім стандартам підприємства, вимогам національних і міжнародних стандартів). В записах аудиту знаходиться інформація про зміни з ІС, даними та налаштування ІС. Адміністратор запросто може переглянути дані та визначити співробітника який змінив властивість файлу, бази даних та інше. Кожна система веде власний журнал в який записує всі зміни, але якщо в адміністратора велика

кількість різноманітних систем які потрібно контролювати, то своєчасне визначення змін та подій дещо ускладнює процес пошуку. Тому для спрощення роботи адміністратору, розробники ПЗ пропонують готові рішення для збору аудиту локальних та хмарних систем.

Висновок до розділу 2

Традиційних засоби захисту такі як: антивіруси, міжмережеві екрани і системи аутентифікації - не здатні забезпечити ефективний захист від внутрішніх інсайдерів.

Перш ніж будувати свій захист необхідно провести аудит наявної інфраструктури та переглянути всі шляхи захисту ресурсів компанії на фізичному та програмному рівнях. Не варто забувати про навчання персоналу щоб попередити майбутні інциденти та мінімізувати вплив інсайдерів на співробітників. Оцінка використовуваних систем вкаже на їх актуальність та можливість протидії ІЗ на сьогодні та на майбутні роки щоб вона не втрачала своєї актуальності впродовж довгого часу.

РОЗДІЛ 3 КОМПЛЕКСНА ТЕХНОЛОГІЯ ПРОТИДІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК

Інциденти з внутрішньою загрозою можливі в будь-якому секторі чи організації. У своїй нинішній чи колишній ролі особа має або мала доступ до мережевих систем, даних або приміщень організації та використовує їхній доступ (іноді мимоволі). Для боротьби з інсайдерською загрозою організації можуть запровадити активну, зосереджену на запобіганні програму пом'якшення для виявлення та ідентифікації загроз, оцінки ризику та управління цим ризиком – до того, як станеться інцидент.

Інформація та ресурси, доступні в Агентстві з кібербезпеки та безпеки інфраструктури (CISA), допоможуть окремим особам, організаціям і спільнотам створити або покращити існуючу програму пом'якшення внутрішніх загроз. Організації, які впроваджують таку програму на практиці, повинні залишатися адаптованими. Оскільки інфраструктурні спільноти працюють над захистом від внутрішньої загрози та діляться набутими уроками, вони можуть захистити націю. І якщо виникнуть зриви з боку внутрішньої загрози, організації зі зрілими програмами можуть виявитися стійкими [2].

Рис. 3.1. Ключові кроки для пом'якшення внутрішньої загрози

Цілісна програма пом'якшення інсайдерських загроз поєднує фізичну безпеку, обізнаність персоналу та принципи, орієнтовані на інформацію. Правильно написана програма протидії ІЗ має на меті зрозуміти взаємодію інсайдерів в організації, контролювати цю взаємодію у відповідних законодавчих межах і втручатися, щоб керувати взаємодією, коли поведінка інсайдера загрожує

організації. Успішні програми пом'якшення внутрішніх загроз досягають цих цілей, дотримуючись трьох основних принципів, які застосовуються до організацій будь-якого розміру та рівня зрілості:

- Сприяти розвитку культури захисту та підтримки в усій організації;
- Захист організаційних цінностей, захист приватності, прав і свобод.
- Залишатися адаптивним, оскільки організація розвивається та змінюється її толерантність до ризику.

Програми зменшення внутрішньої загрози розроблені різноманітними державними інститутами, консультативними агенствами з кібербезпеки та окремими розробниками прогрпамного забезпечення, щоб допомогти організаціям втрутитися до того, як особа з привілейованим доступом або розумінням організації зробить помилку або вчинить шкідливий або ворожий вчинок. Розробка програми повинна охоплювати всю організацію і служити системою допомоги індивідам, а не бути агресивною програмою примусового виконання чи «боротьби».

Компанія Deloitte в обличчі Craig Astrich запропонувала побудову цілісної програми протидії ІА.

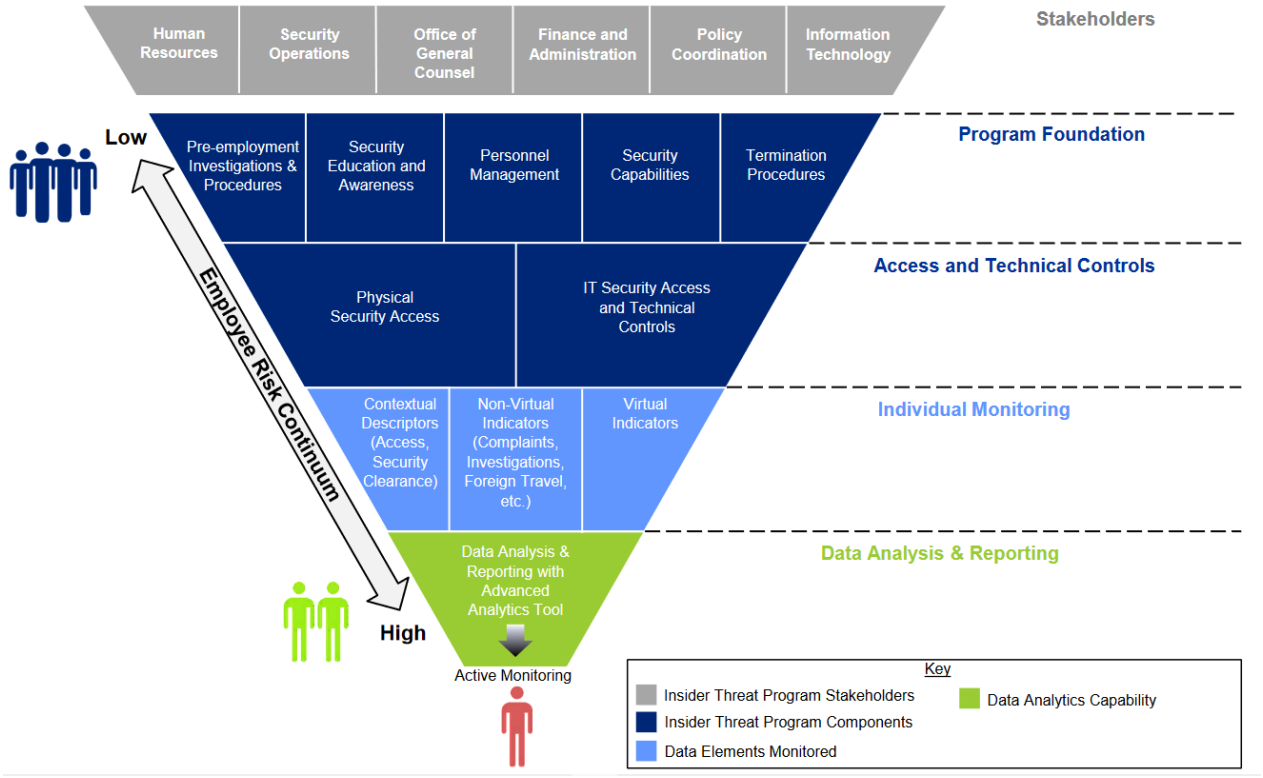

Рис. 3.2. Програма протидії ІЗ від компанії Deloitte [13]

На даній структурі ми можемо бачити рівень зростання ризику від групи співробітників з індикатором «LOW» до конкретної зацікавленої особи що може заподіяти шкоди з індикатором «HIGH». В даному трикутнику описано які програми, політики, регуляції можуть повпливати на зменшення кількості інсайдерів та їх знаходження в організації за певними ідентифікаторами з подальшим спостереженням за можливим порушником. Розглянемо дану структуру:

1. Insider Threat Program Stakeholders – мультидисциплінарні зацікавлені групи координуються та забезпечують зв’язок та зустрічі на повторюваній основі. До таких груп входять особи з наступних напрямків:

- Human Resources
- Security Operations
- Office of General Counsel
- Finance and Administration
- Policy Coordination
- Information Technology

2. Insider Threat Program Components – програмні компоненти протидії ІЗ

- Program Foundation. Політика безпеки, процедури та технології забезпечують основу для пом'якшення ІЗ. Перевірка, керування та випуску персоналу належним чином захищає дані та інформацію в системах. До цього процесу входить:
  - Дослідження перед розслідуванням та процедурний процес
  - Освіта та обізнаність працівників
  - Управління персоналом
  - Можливості забезпечення безпеки
  - Процедури припинення дії інсайдерів

3. Access and Technical Controls. Розмежування доступу та технічний контроль служить як бар'єр для доступу до персоналу та вимагає подальшої

переоцінки необхідного доступу. У разі виникнення інциденту, стійкості (наприклад, система та процедури резервного копіювання даних) є критичним завданням. До цього процесу входить:

- Безпечний фізичний доступ
- Доступ до безпеки та технічний контроль

4. Individual Monitoring. Процес стеження за особою збираючи агрегативні дані від безрозсудні, але відповідні джерела даних забезпечують покращене розуміння профілів ризику окремих працівників. Тип зібраних даних включатиме PII і повинно бути захищені в повному обсязі. Доступ до цієї інформації безпеки буде обмежена. До цих індентифікаторів входять:

- Контекстні дескриптори (доступ, оформлення безпеки)
- невірні показники (скарги, розслідування, іноземні подорожі тощо)
- Віртуальні показники

5. Data Analysis & Reporting. Дані з різноманітних джерел об'єднуються для виявлення окремих ризикованих працівників. Додатковий інструмент аналітики забезпечує автоматизований аналіз та звітність на основі алгоритму ризику, який вирівнюється з толерантністю до ризику організації. Сюди входить аналіз даних та звітність з додатковим інструментом аналітики.

Чотири ключові компоненти надають основу для оцінки загальної здатності організації, щоб запобігти, виявити та пом'якшити інсайдерські загрози. Використання цих чотирьох компонентів створює цілісну основу для вивчення вразливості інсайдерської загрози та визначити пріоритети з високим рівнем ризику.

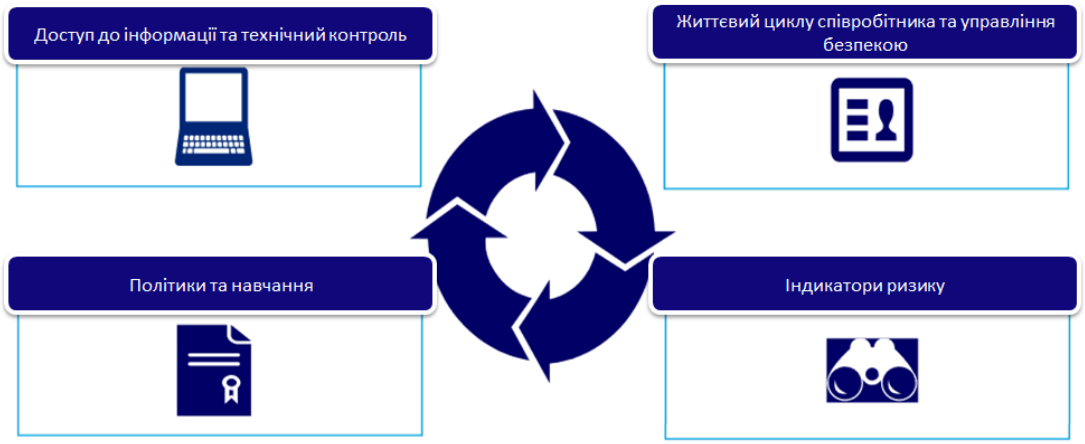

Рис. 3.3. Компоненти для оцінки протидії ІА [13]

• Інформаційний доступ та технічний контроль доступу до ролі співробітника, безперервні програми моніторингу та ІА, пов'язані з мережею, забезпечують профілактичні можливості та можливості щодо виявлення.

• Життєвий цикл співробітника та управління безпекою – це процедури, пов'язані з вербуванням, перевіркою, найманням, відставкою, припиненням та процедурами передачі протягом усього життєвого циклу працівника.

• Індикатори ризику під час ІЗ впливають на поєднання віртуальних, невіртуальних та організаційних чинників. Поведінка людини по кожному пункту повинна бути оцінена та зважена на основі ідентифікаторів ризику.

• Політика та навчання є нетехнічним контролем та тренінги, які регулюють пом'якшення ІЗ, встановлюють очікування та забезпечують послідовне дотримання політик компанії [13].

Для ефективної протидії ІА від фізичного та програмного впливу компанії використовують різноманітні підходи та програми для забезпечення безпеки. За статистикою компанії ProofPoint, компаній розгортають навчання та тренінги користувачів – 55% від загальної кількості опитуваних компаній. На другому місці системи протидії витоку інформації (DLP) – 54%, далі компанії обирають системи аналізу поведінки користувачів (UBA) – 50% для запобігання ІЗ, як показано в таблиці.

Table 3. Tools and activities that reduce insider Security tools & activities	Frequency of companies	Percentage of companies
User training & awareness	112	55%
Data loss prevention (DLP)	110	54%
User behavior analytics (UBA)	102	50%
Employee monitoring & surveillance	96	47%
Security incident & event management (SIEM)	91	45%
Incident response management (IRM)	89	44%
Strict third-party vetting procedures	87	43%
Threat intelligence sharing	85	42%
Privileged access management (PAM)	80	39%
Network traffic intelligence	77	38%

Рис. 3.5. Інструменти зменшення впливу підчас ІА [5]

Згідно з рисунком 3.5, компанії можуть заощадити в середньому 3,4 мільйона доларів та 3,1 мільйони при розгортанні UBA та привілейованого управління доступом (PAM) рішення. Найчастіше розгорнуті інструменти та заходи показані на рисунку 3.5. Відповідно, 112 компанії проводять навчальні програми для підвищення усвідомлення працівника про ІЗ. Кількість компаній, які використовують системи протидії витоку інформації 110 і 102 компанії, що розгорнуть системи аналізу поведінки користувачів для визначення підозрілі мережеві активності [5].

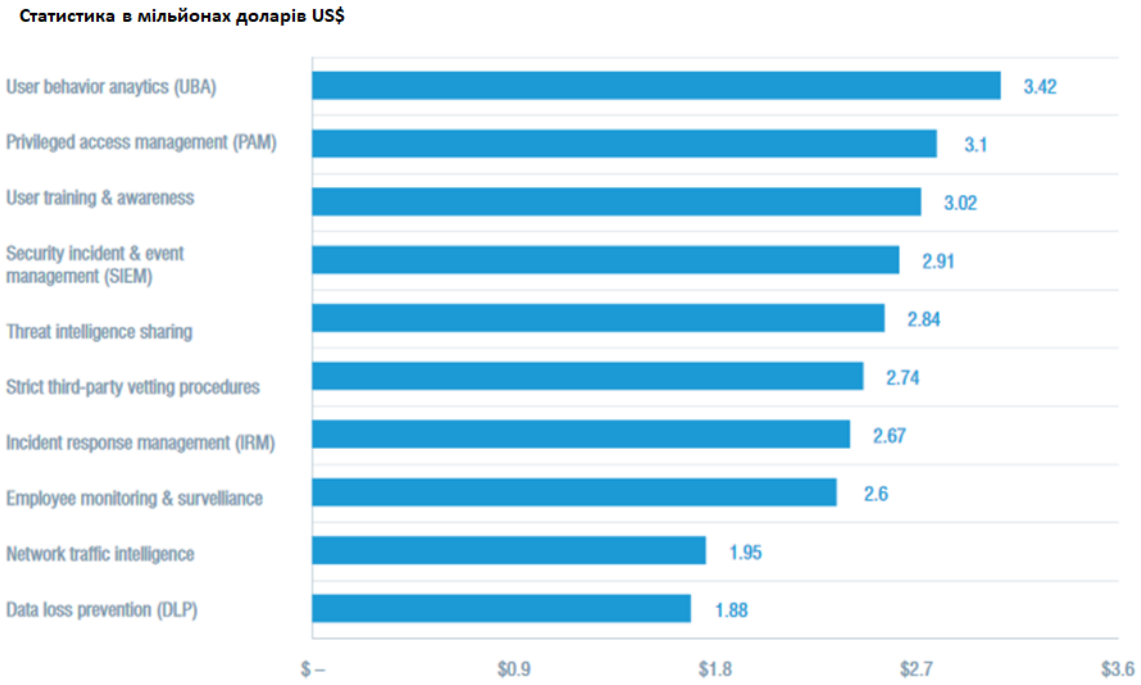

Рис. 3.6. Економія коштів, як результат впровадження інструментів протидії ІА

За статистикою компанії Fortinet, три найбільш ефективні інструменти безпеки та тактики розгорнуті організаціями для захисту від інсайдерських загроз, - це системи запобігання витоку даних (DLP) - 54%, ідентичність та управління доступом (IAM) - 52% та політики навчання - 49%. Майже половина - 46% організацій використовують аналітику поведінки користувачів (UEBA) та управління безпекою з управлінням подіями (SIEM), щоб зміцнити та підвищити ефективність своїх програм протидії інсайдерам [9].

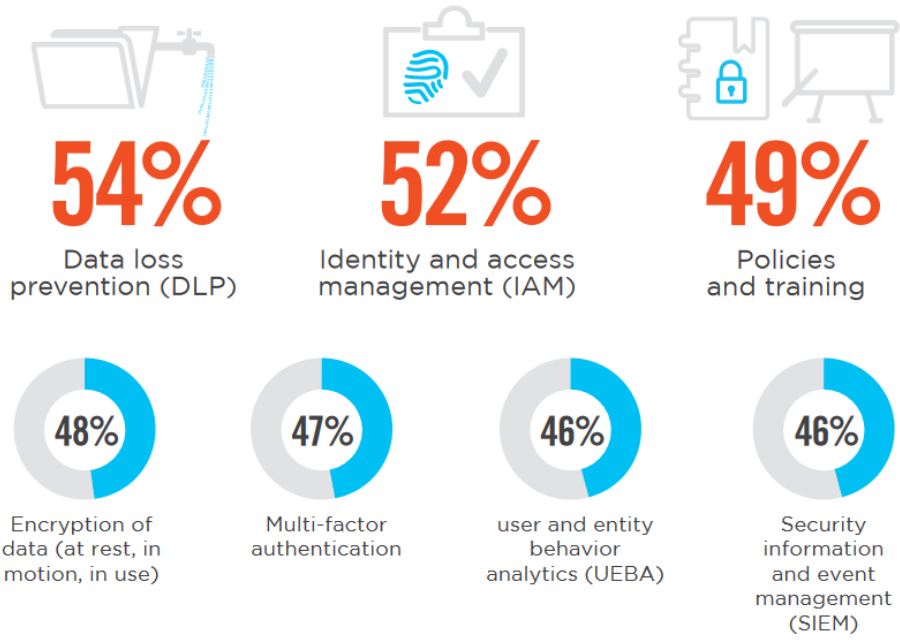

Рис. 3.7. Найбільш ефективні інструменти безпеки та тактики для захисту від ІА

На питання про рішення протидії інсайдерським загрозам, більшість організацій все ще оцінюють рішення - 36% або активно реалізують їх - 32%. Тільки невелика частина організацій - 5% кажуть, що вони не мають рішень в організації і не планує їх реалізувати [9].

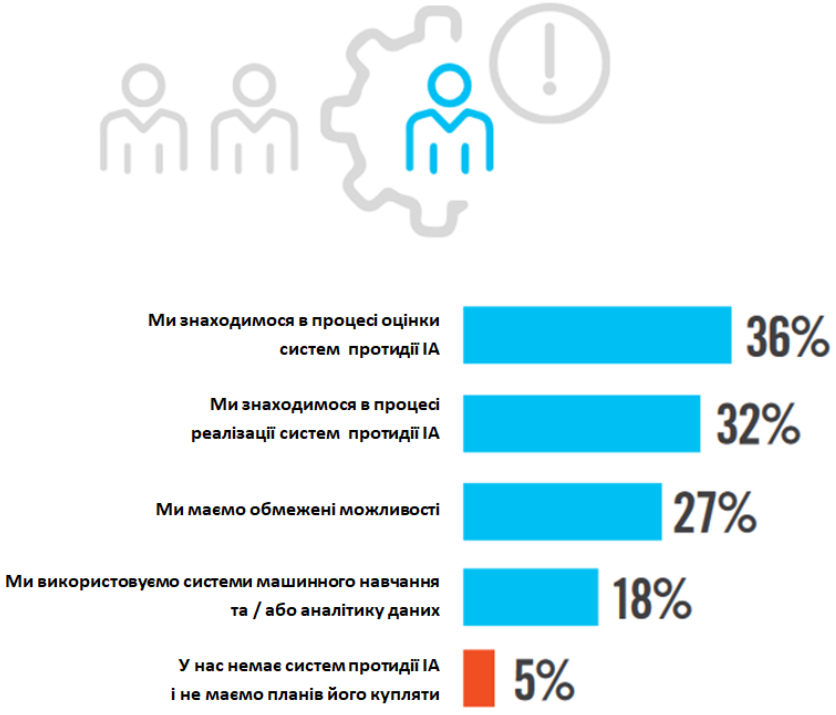

Рис. 3.8. Використання систем протидії ІЗ в опитуваних організаціях

Кожне з досліджень доводить що інциденти стаються людський фактор і компаніям потрібно організувати правильну політику навчання співробітників шо не стати ненавмисним інсайдером який через необережність або необдумані дії став інсайдером або допоміг одному з них. Кожна компанія створює та проводить тренінги з кібербезпеки з певною періодичністю. Кожного місяця або квартала компанія встановлює самостійно, основна ж задача при цьому щоб співробітники які працюють та яких тільки найняла організація мали однаковий рівень обізнаності в сфері кібербезпеки відповідно до займаної посади.

На другому місці серед продуктів та показників ефективності посідає система аналізу поведінки людей. UEBA зазвичай використовує різноманітні підходи для аналізу та пророкування дій співробітників та базується на готових правилах або штучному інтелекту. Тому, більшість розробників програмного забезпечення включають UEBA до своїх продуктів. Від мережевого моніторингу до агентів на робочих станціях.

Для визначенням з рішенням DLP для організації розгляну ринок програмного забезпечення в Україні та лідерів квадрата Gartner [14; 15].

Рис. 3.9. Лідери Gartner Magic Quadrant систем DLP

Безперечним лідером на ринку України та квадраті Гартнера є система Symantec DLP. Розглянемо його структуру та можливості.

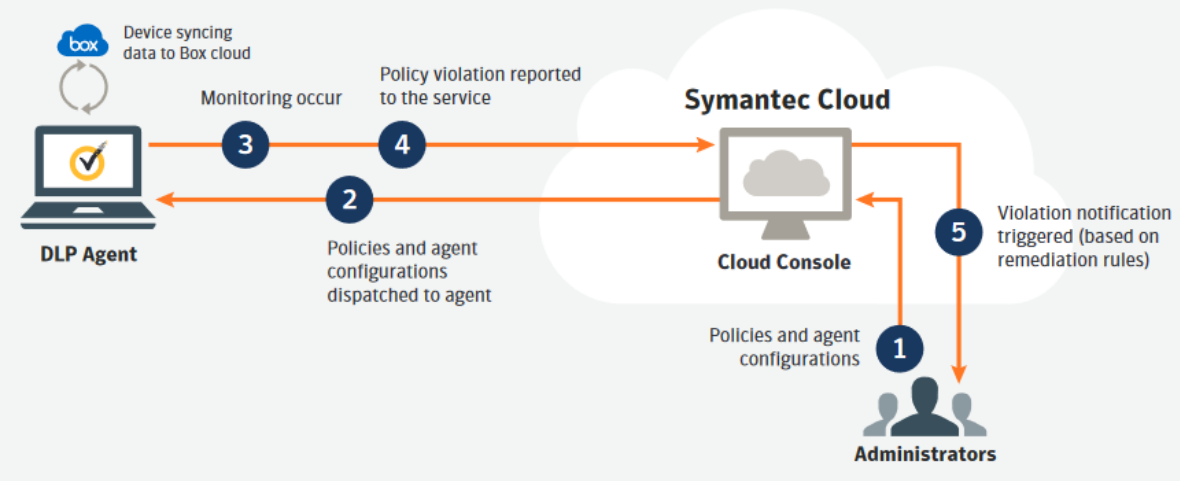

Рис. 3.10. Принцип роботи Symantec DLP [16]

Для функціонування система достатньо створити політику для агента що встановлюється на робочий комп'ютер працівника та встановити агента. Якщо працівник порушує встановлені правила, то адміністратору приходить сповіщення на пошту та доступна аналітика в Symantec Cloud. Основні метрики для збору даних:

- Браузери - Chrome, Firefox, Internet Explorer & Edge
- Хмарні додатки - Box, Dropbox, Google Drive, OneDrive, інші
- Поштові сервіси - Outlook
- Мережеві протоколи - HTTP, HTTPS, FTP
- Зовнішні носії - MSC devices, MTP devices
- Інші - Print, Network Share, Clipboard, etc.

Для визначенням з рішенням PAM для організації розгляну ринок програмного забезпечення в Україні та лідерів квадрата Gartner [17; 18].

Рис. 3.11. Лідери Gartner Magic Quadrant систем PAM

Наступним лідером на ринку України та квадраті Гартнера є система Safeguard PAM від One Identity. Розглянемо його структуру та можливості.

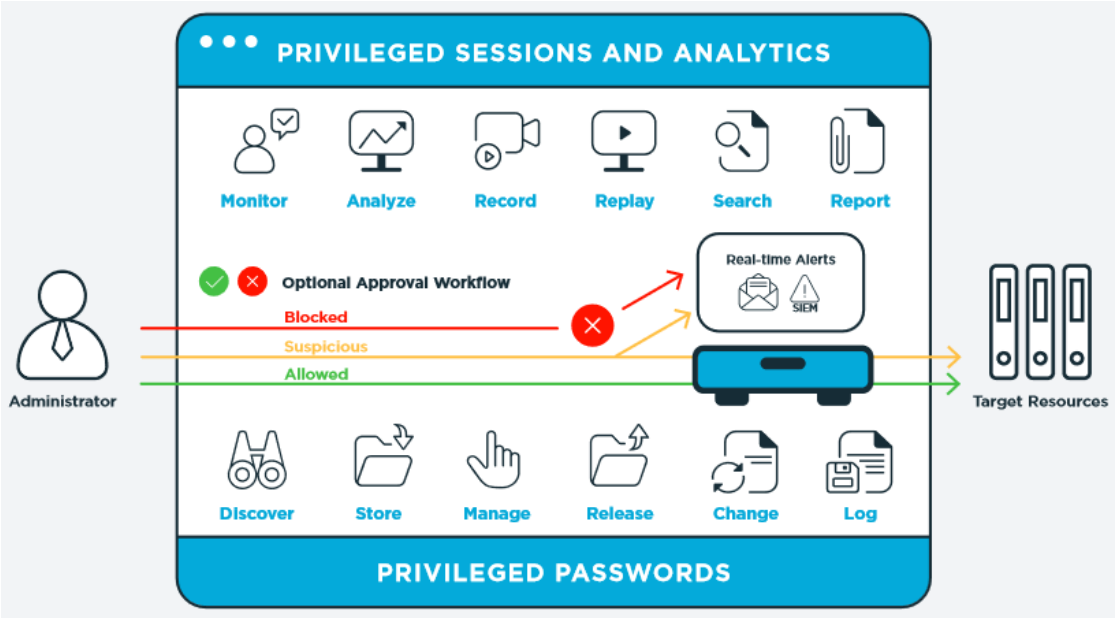

Рис. 3.12. Принцип роботи Safeguard від One Identity [19]

Для функціонування система достатньо створити політику для користувача що дозволяє або забороняє доступ відповідно до політик компанії. За ним

ведеться моніторинг та аналітика його дій підчас віддалених сесій на робочі станції або сервери. Якщо працівник порушує встановлені правила, то адміністратору приходить сповіщення на пошту та доступна аналітика в Safeguard for privileged sessions and analytics. Основні метрики для збору даних:

- Тривалість сесії та час входу
- Натискання на клавіатуру та кліки миші
- Входи на робочі станції
- Незвичні входи
- Відхилення від норм аналітики встановленою UEBA.

Для визначенням з рішенням SIEM для організації розгляну ринок програмного забезпечення в Україні та лідерів квадрата Gartner [20].

Рис. 3.13. Лідери Gartner Magic Quadrant систем SIEM

Наступним лідером на ринку України та квадраті Гартнера є система Qradar SIEM від IBM. Розглянемо його структуру та можливості.

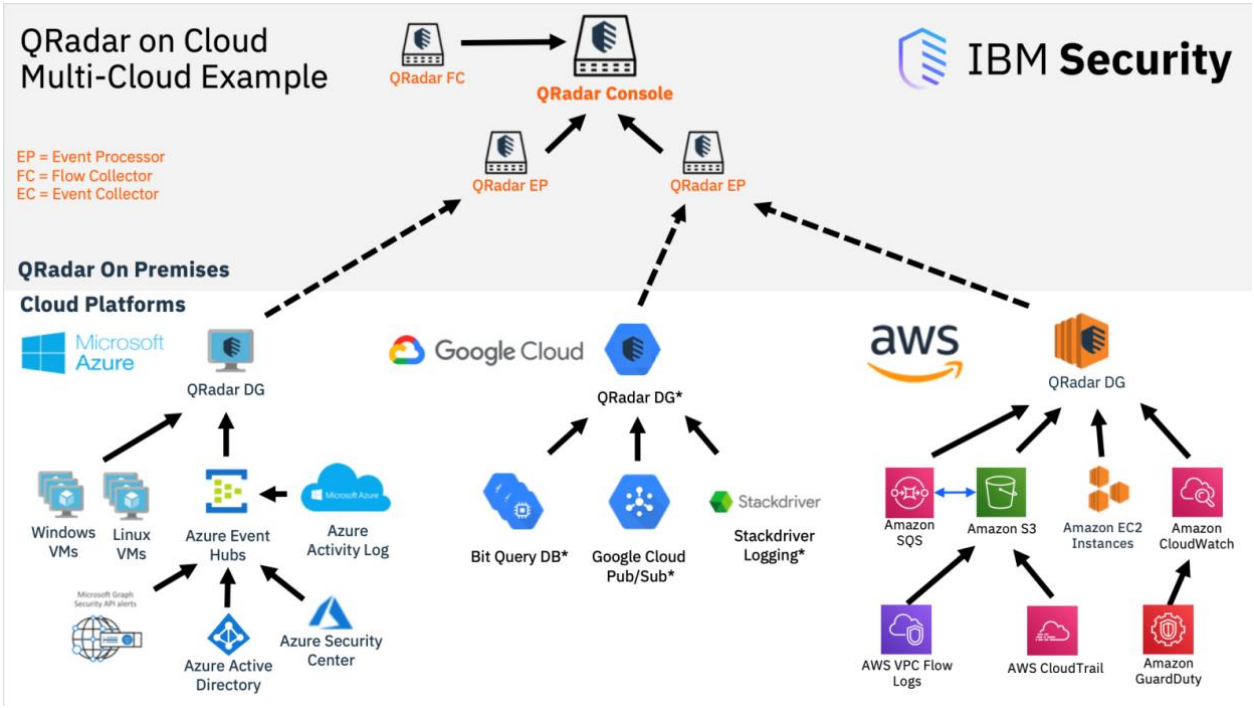

Рис. 3.14. Структура Qradar та можливості інтеграції з іншими системами [21]

Завдяки колосальним можливостям інтеграції, система Qradar може агрегувати дані з локальних та хмарних середовищ для моніторингу та аудиту дій користувачів як з середини так і ззовні організації. Завдяки цьому ми можемо отримувати наступну аналітику UBA.

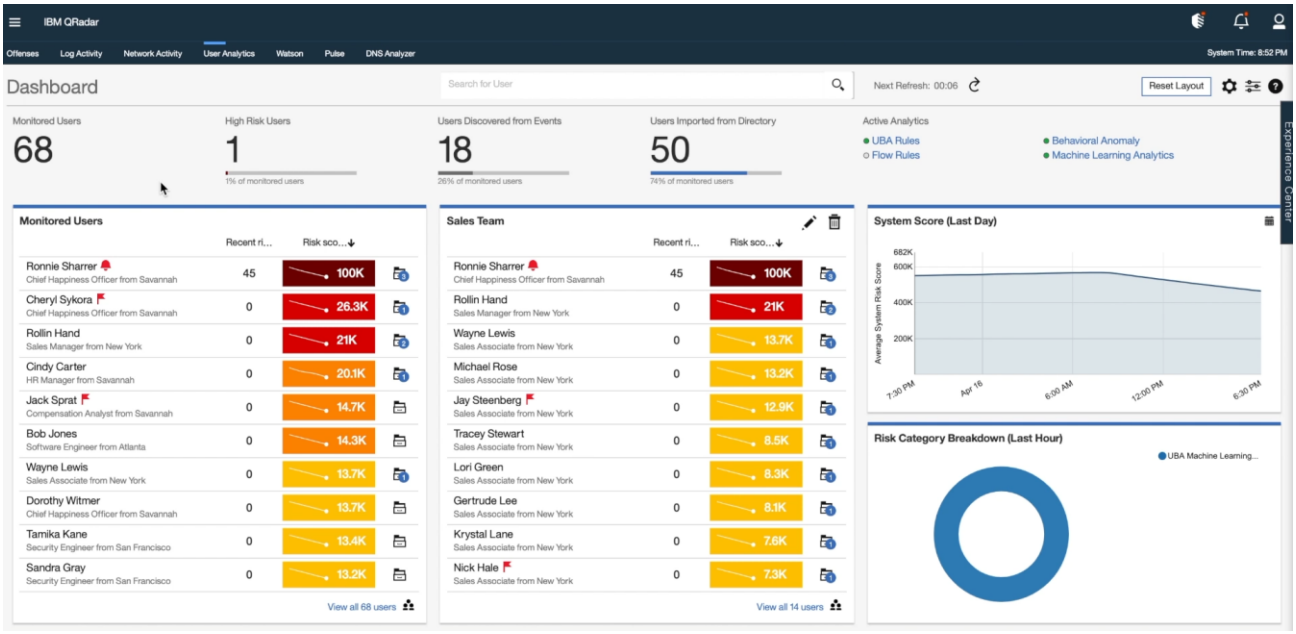

Рис. 3.15. Аналітика користувачів в IBM Qradar

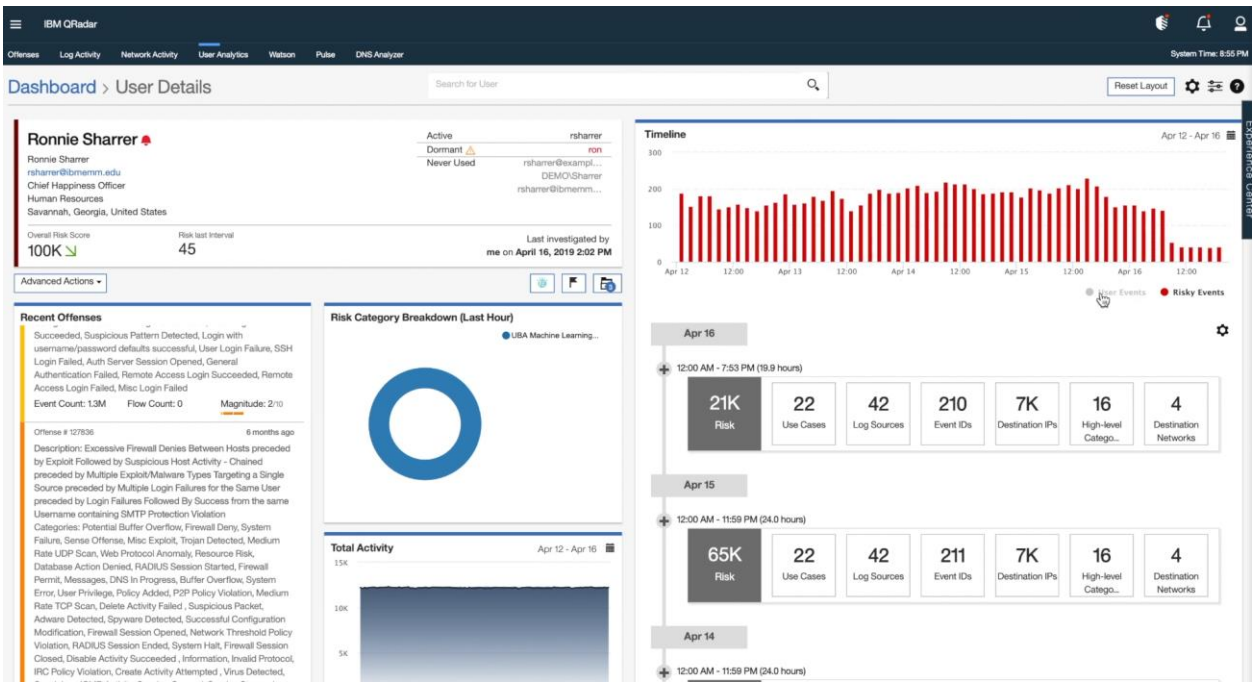

Рис. 3.16. Аналітика окремого користувача в IBM Qradar

Компанії можуть використати вже готове програмне рішення Varonis Data Security Platform для протидії IA яке є передовим в категорії «Insider Risk Management Solutions» в квадраті Gartner [22].

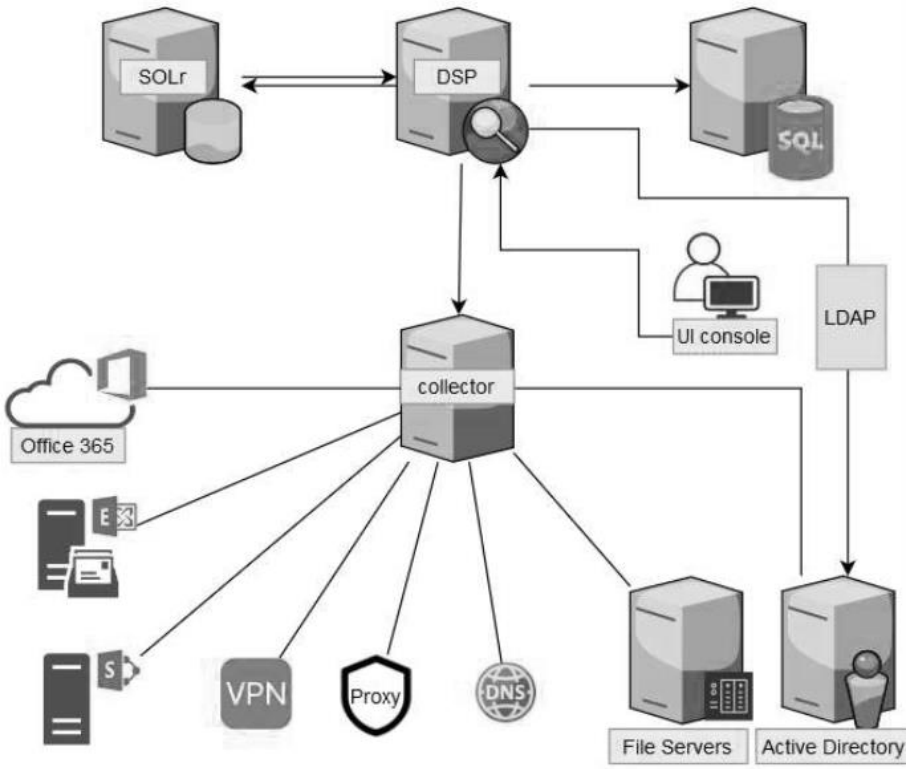

Рис. 3.17. Структура Varonis та можливості інтеграції з іншими системами [23]

Система Varonis може інтегруватися з локальними та хмарними середовищами для знаходження змін з файлами, папками, даними користувачів як з середини так і ззовні організації. Завдяки цьому ми можемо отримувати аналітику про пересування користувача всередині периметру та його дії з даними.

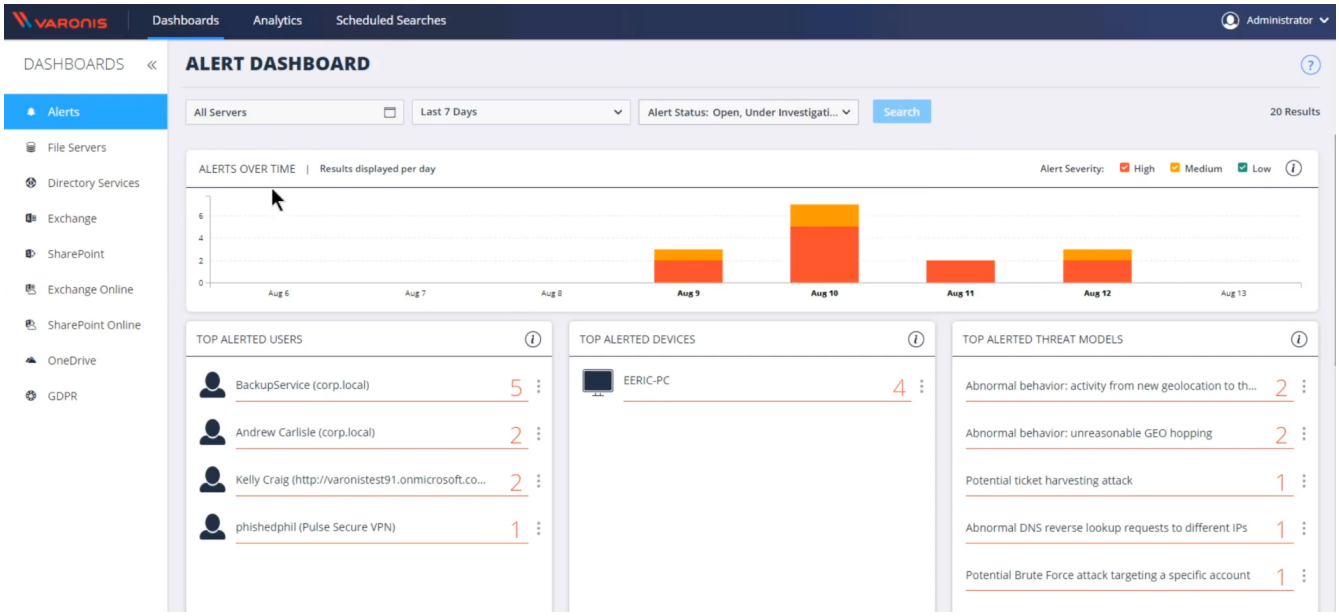

Рис. 3.18. Сповіщення користувачів в Varonis

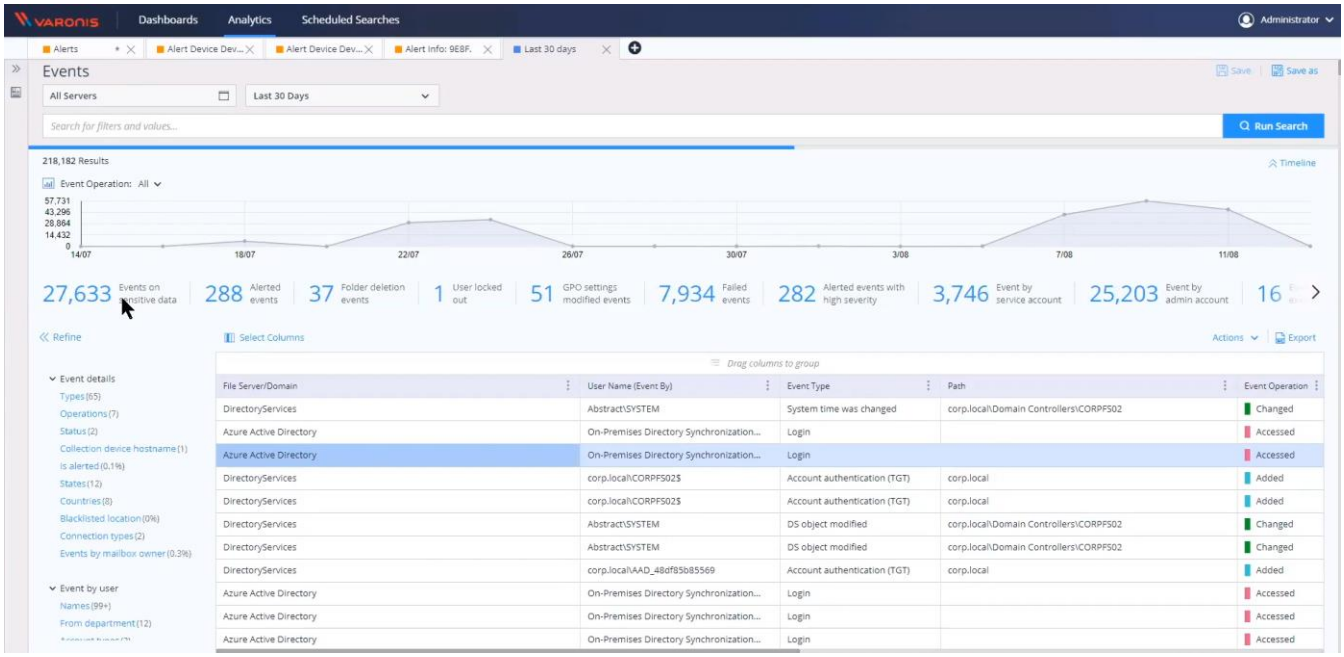

Рис. 3.19. Аналітика подій в системі Varonis за місяць

Переглядаючи аналітику, адміністратор може швидко індентифікувати потенційний інцидент кібербезпеки та прийняти запобіжні заходи або система вже зробила це за нього за допомогою автоматичних реакцій на сповіщення.

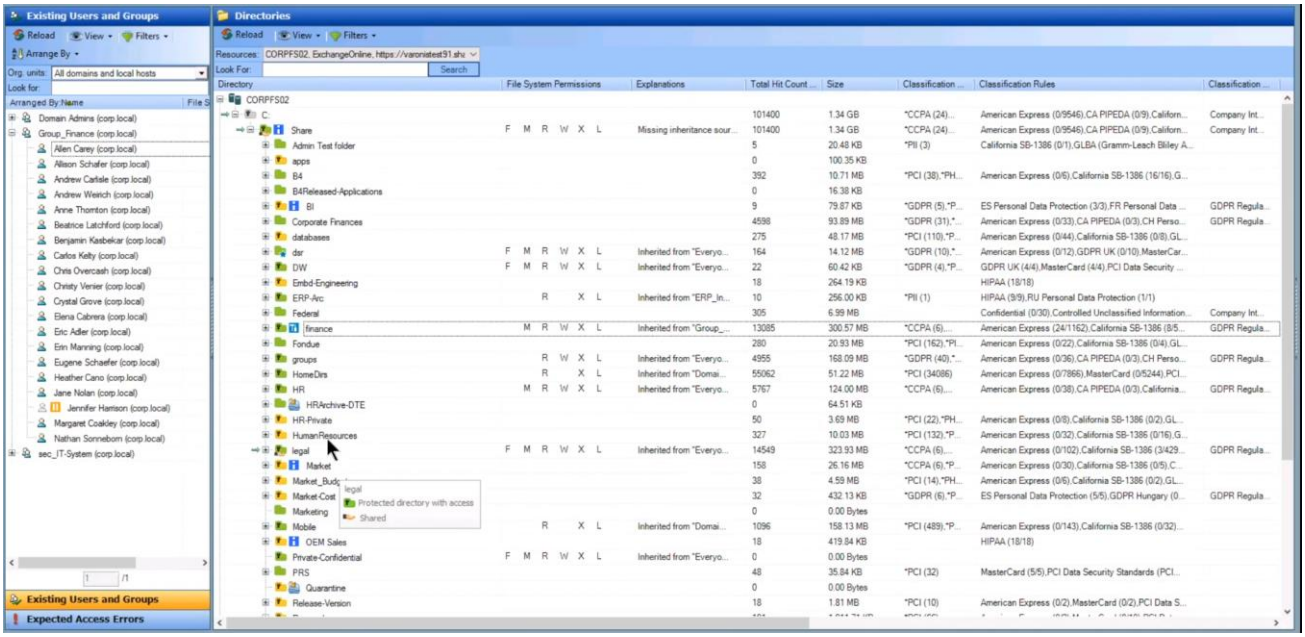

Рис. 3.20. Матриця доступу в системі Varonis

Також, адміністратор завжди може відповісти на питання де зберігається чутлива інформація, таємниці організації та хто має доступ до них, до якого файлу та коли він його використовував [23].

Система Varonis складається з наступних модулів:

- DATADVANTAGE (Data Audit & Protection) - DatAdvantage відображає, хто може і хто має доступ до даних у файлових і електронних системах. Показує, де користувачі мають занадто великий доступ, і безпечно автоматизує зміни в списках і групах контролю доступу. Візуалізує ризики, конфіденційні дані та надає повну видимість і контроль над локальними та хмарними сховищами даних в рамках однієї платформи.
- DATALERT (Security Analytics) - виявляє підозрілу активність і запобігає злому даних на різних платформах, візуалізує ризики та визначає пріоритети розслідування.

- VARONIS EDGE (Perimeter Telemetry) –аналізує пристрої в периметрі , такі як DNS, VPN та веб-проксі, застосовуючи змішаний контекст аналітики до активності в мережі та сповіщень від основних сховищах даних.
- AUTOMATION ENGINE (Automated Remediation) - механізм автоматизації виявляє непомічені прогалини в безпеці та автоматично усуває їх: усуває приховані вразливості безпеки, як-от неузгоджені списки керування доступом та глобальний доступ до конфіденційних даних [23].
- DATA CLASSIFICATION ENGINE (Sensitive Content Discovery) - механізм класифікації даних виявляє та ідентифікує конфіденційні, регульовані та застарілі дані за допомогою вбудованих шаблонів, попередньо визначених категорій, настроюваних регулярних виразів і словників.
- DATAPRIVILEGE (Data Access Governance) - дає бізнес-користувачам можливість переглядати та керувати дозволами, групами та сертифікацією доступу, автоматично запроваджуючи бізнес-правила.
- DATA TRANSPORT ENGINE (Data Retention And Migration) - автоматично знаходить, переміщує, архівує, поміщає в карантин або видаляє дані на основі типу вмісту, віку, активності доступу тощо.
- DATANSWERS (Enterprise Search And Discovery) - аналізує вміст, активність файлової системи, дозволи та інші метадані, щоб надати відповідні результати пошуку.

Технологія протидії впливів підчас ІА

Інформація в організації зберігається в цифровому вигляді на локальних носіях чи хмарних системах збереження інформації, тому першочерговою задачею для організації буде захист даних від вивантаження з носіїв та подальший контроль цих даних. Для реалізації використаємо зв’язку продуктів IBM Qradar з Varonis DatAdvantage та Symantec DLP.

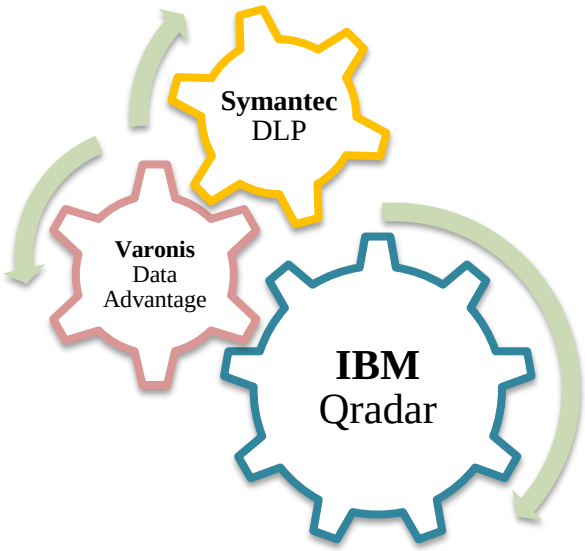

Рис. 3.21. Технологія протидії ІЗ

За основу слугуватиме Qradar для накопичення, кореляції та обробки логів з мережевих пристроїх в тому числі логів з систем аудиту входів працівників. На його базі буде будуватися аналітика та правила сповіщень з інших двох продуктів. Varonis відіграватиме роль централізованої системи накопичення та передачі логів про зміни на серверах, поштових сервісах, фермах сайтів SharePoint, інформація про права доступу користувачів та об'єднання як локальної та хмарної інфраструктури для аудиту та в SIEM.

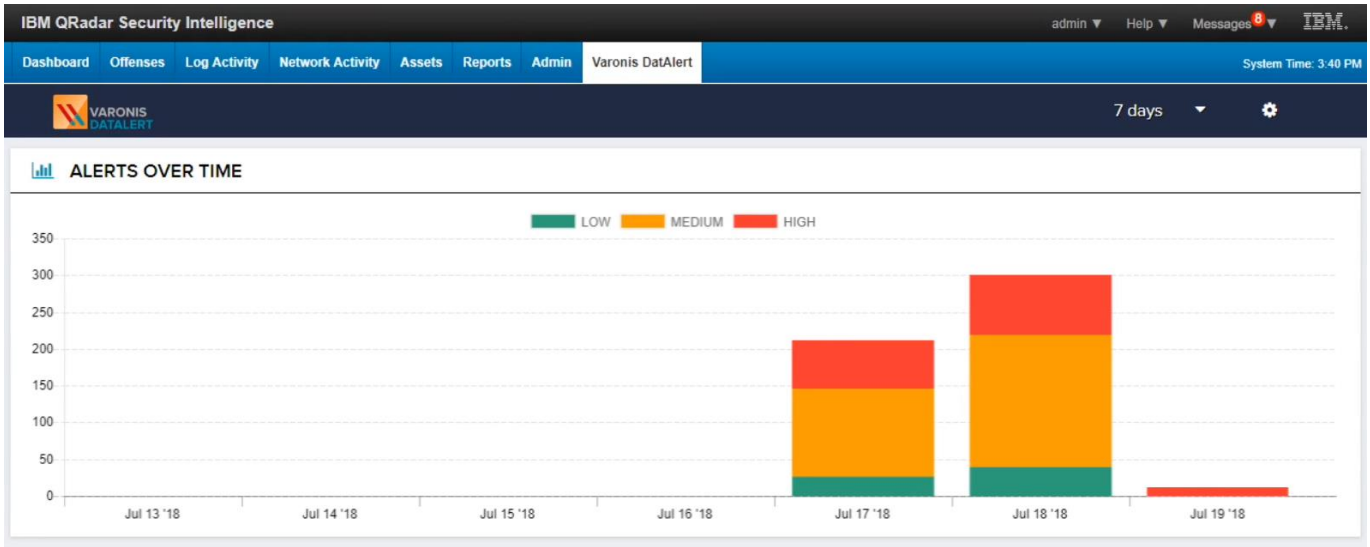

Рис. 3.22. Вигляд графіку сповіщень в консолі IBM Qradar при інтеграції з Varonis DatAdvantage [24]

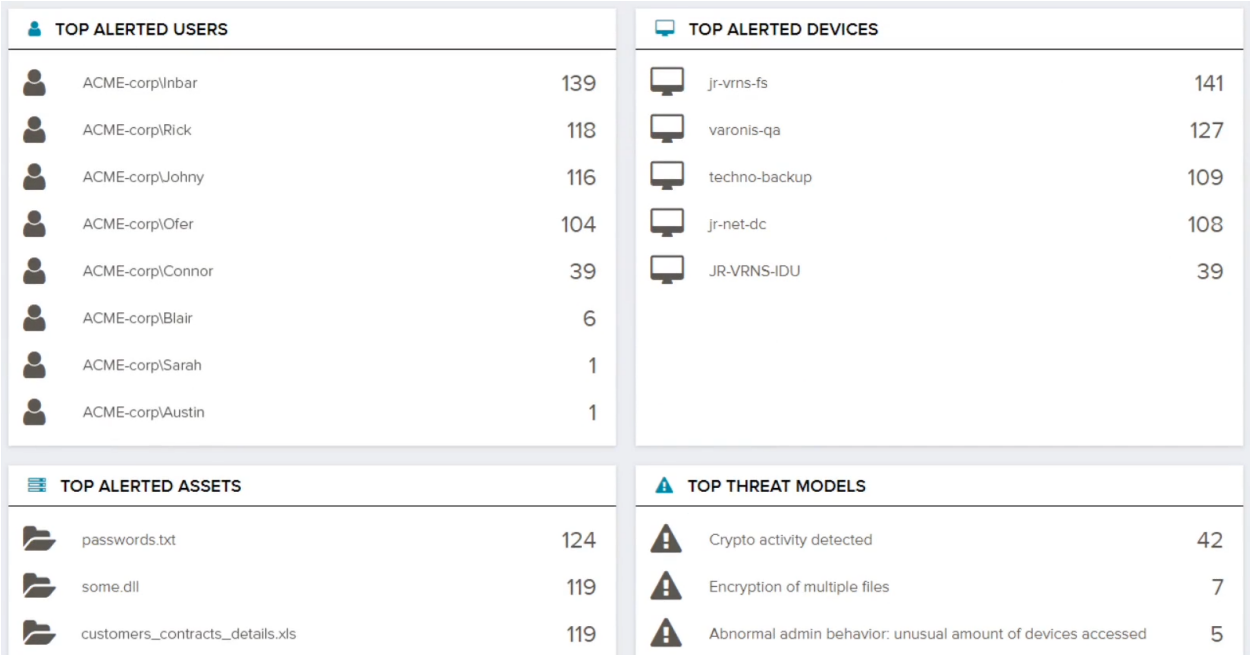

Рис. 3.23. Вигляд статистики сповіщень в консолі IBM Qradar при інтеграції з Varonis DatAdvantage

Також, додаткові модулі допоможуть прокласифікувати дані на джерелах та встановити де саме знаходиться конфіденційна інформація та захистити дані ресурси змінивши права доступу для неактивних або небажаних користувачів. Встановлення тегів підготує ресурси для використання DLP. Коли співробітник намагатиметься завантажити або змінити критичний файл з тегом PII, PCI DSS або GDPR то система Symantec DLP автоматично побачить що файл відповідає тегові та для нього застосовується певна дія. Агент автоматично застосує одне з правил та повідомить адміністратора або заборонить доступ для співробітника в залежності від налаштувань.

Змоделюємо ситуацію:

1. Адміністратор підключається по VPN всередину організації.
2. Змінює права доступу для папки що містить конфіденційну інформацію додаючи новоствореного користувача.
3. Перепідключається на файловий ресурс з новим користувачем та намагається завантажити файл на термінальний сервер де знаходиться поштовий клієнт.
4. Спроба вивантажити файл.

Дана атака може проходити не 1 день, а цілий місяць що в свою чергу ускладнює процес розслідування. Інформація яку отримає спеціаліст з кібербезпеки в кожній з систем:

- IBM Qradar – інформація про підключення до VPN організації та аналітика отримана з Varonis та Symantec.
- Varonis DatAdvantage - інформація про підключення до серверів та зміни в інфраструктурі в тому числі додавання користувача та зміна прав на папку.
- Symantec DLP – інформація про маніпуляції з файлом (перейменування, зміна формату та інше) та спроби вивантажити на сторонній ресурс.

Що стосується хмарних ресурсів та файлів на них, то співробітники зазвичай поширюють файли для своїх колег всередині організації але деякі з них можуть створити посилання на ззовні для анонімного доступу до них. В такому разі достовірно дізнатися звідки прийшло підключення практично не можливо. Запровадження політик поширення файлів та автоматичних дій при створені таких посилань можуть врятувати ситуацію.

Висновок до розділу 3

Захист організації від ІА є дуже важливий в теперішніх реаліях віддаленої роботи та COVID-19 пандемії. В розділі було рекомендовано будувати свій захист виходячи з вже наявної інфраструктури та переглядати всі шляхи захисту ресурсів компанії додатковими програмними засобами для зупинення витоку даних перш за все на фізичні носії.

Технологія протидії ІА виглядає поєднанням класу рішень Insider Risk Management Solutions разом з SIEM та DLP системами. Можлива інтеграція між ними за допомогою API допоможе адміністраторам швидко реагувати на інциденти та мінімізувати їх вплив. Людський фактор завжди буде наявний в кожній організації, тому для зменшення кількості подій ІЗ необхідно проводити тренінги для співробітників.

ВИСНОВКИ

В магістерській роботі було проаналізовано модель інсайдера та описані ефективні технології захисту від ІА. Також було проаналізовано програмні комплекси що можуть створити додатковий захист протидії інсайдерам.

З кожним роком втрати від ІА зростають та необхідно вдосконалювати та побудувати стійкий захист проти цих загроз. Необхідно провести аудит наявної інфраструктури та переглянути всі шляхи захисту ресурсів компанії на фізичному та програмному рівнях. Не варто забувати про навчання персоналу щоб попередити майбутні інциденти та мінімізувати вплив інсайдерів на співробітників. Найчастіше інсайдери впливають на файлові сервери та сервери баз даних. При цьому все ще залишається небезпека друку та винесення інформації на фізичних носіях через спеціальні або особисті пристрої.

Ключове питання для департаменту безпеки — це побудова захисту від ІА базуючись на вже наявних ресурсах чи обрати технологію що може перекрити ”дірки” за короткий термін. Перший варіант зручніший для малих організацій у звязку з мінімальним вкладенням коштів, але при цьому необхідно мати високий рівень навичок адміністраторів для створення цілісної політики безпеки. Другий варіант є універсальним «антидотом» та довгою мандрівкою в пошуках необхідної технології. Правильний та комплексний підхід до вирішення цієї проблеми допоможе вберегти організацію від розкриття конфіденційної інформації та зменшити ризики на майбутні роки.

Було виконано зазначену мету і вирішено наступні задачі:

1. Проведено аналіз виявлення інсайдерських атак та їх вплив на інформаційну систему організації;
2. Переглянуті методи та засоби протидії інсайдерських атак;
3. Запропоновано технологію протидії під час із.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CERT Definition of 'Insider Threat' – Updated [Електронний ресурс] – Режим доступу: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

2. Insider Threat Mitigation [Електронний ресурс] – Режим доступу: https://www.cisa.gov/insider-threat-mitigation

3. The CISO’s Guide to Managing Insider Threats [Електронний ресурс] – Режим доступу: https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/

4. What is an Insider Threat? Definition and Examples [Електронний ресурс] – Режим доступу: https://www.varonis.com/blog/insider-threats/

5. 2020 Cost of Insider Threats: Global Report [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/us/resources/threat-reports/2020-cost-of-insider-threats

6. How much does a data breach cost? [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/data-breach

7. Insider Threat Incidents: Assets Targeted by Malicious Insiders [Електронний ресурс] – Режим доступу: https://insights.sei.cmu.edu/blog/insider-threat-incidents-assets-targeted-by-malicious-insiders/

8. Insider Threat Incidents: Most Commonly Affected Devices [Електронний ресурс] – Режим доступу: https://insights.sei.cmu.edu/blog/insider-threat-incidents-most-commonly-affected-devices/

9. Insider-threat-report [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

10. Insider Threat and Physical Security of Organizations [Електронний ресурс] – Режим доступу: https://insights.sei.cmu.edu/blog/insider-threat-and-physical-security-of-organizations/

11. Insider Threats are Weakening Your Physical Security [Електронний ресурс] – Режим доступу: https://blog.techguard.com/insider-threats-are-weakening-your-physical-security

12. What does identity and access management mean? [Електронний ресурс] – Режим доступу: https://www.onelogin.com/learn/iam

13. Building A Holistic and Risk-Based Insider Threat Program [Електронний ресурс] – Режим доступу: https://www.securetechalliance.org/wp-content/ uploads/astrichc.pdf

14. Как выбрать лучшую DLP-систему? [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/practice/methods/how-to-choose-the-best-dlp-system

15. Enterprise Data Loss Prevention (DLP) Reviews and Ratings [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/enterprise-data-loss-prevention

16. Symantec Endpoint Data Loss Prevention [Електронний ресурс] – Режим доступу: https://docs.broadcom.com/doc/data-loss-prevention-for-endpoint-en

17. About the Gartner Magic Quadrants [Електронний ресурс] – Режим доступу: https://it-visibility.net/gartner-magic-quadrants-apm-npm-siem-iam/#1585000609120-f1f84dfd-f558

18. One Identity Named a Leader in the 2021 Gartner® Magic Quadrant™ for Privileged Access Management [Електронний ресурс] – Режим доступу: https://www.oneidentity.com/whitepapert/one-identity-safeguard-named-a-leader-in-its-2021-gartner-magic-quadra8150463/

19. One Identity Safeguard [Електронний ресурс] – Режим доступу: https://www.oneidentity.com/documents/one-identity-safeguard-datasheet-128512.pdf

20. Insider Threat Control: Using a SIEM signature to detect potential precursors to IT Sabotage [Електронний ресурс] – Режим доступу:

https://insights.sei.cmu.edu/blog/insider-threat-control-using-a-siem-signature-to-detect-potential-precursors-to-it-sabotage/

21. IBM QRadar and AWS Best Practices - AWS VPC, AWS IAM, and AWS Security Groups [Електронний ресурс] – Режим доступу: https://community.ibm.com/community/user/security/blogs/patrick-routh/2019/10/01/ibm-qradar-and-aws-best-practices-vpc-iam-security

22. Insider Risk Management Solutions Reviews and Ratings [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/insider-risk-management-solutions

23. Varonis Data Security Platform Reviews [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/insider-risk-management-solutions/vendor/varonis/product/varonis-data-security-platform

24. Varonis and QRadar [Електронний ресурс] – Режим доступу: https://www.youtube.com/watch?v=xkmMpWYrLQ4

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)