КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.175185
УДК 004.94:519.21

**Шевченко Світлана Миколаївна**
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9736-8623
*s.shevchenko@kubg.edu.ua*

**Жданова Юлія Дмитрівна**
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9277-4972
*y.zhdanova@kubg.edu.ua*

**Складанний Павло Миколайович**
кандидат технічних наук,
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7775-6039
*p.skladannyi@kubg.edu.ua*

**Бойко Софія Валеріївна**
студентка Факультету інформаціонних технологій та управління
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-8586-5964
*svboiko.fitu18@kubg.edu.ua*

# ІНСАЙДЕРИ ТА ІНСАЙДЕРСЬКА ІНФОРМАЦІЯ: СУТЬ, ЗАГРОЗИ, ДІЯЛЬНІСТЬ ТА ПРАВОВА ВІДПОВІДАЛЬНІСТЬ

**Анотація.** Постійний розвиток інформаційних технологій, зростаюча роль на сучасному етапі людського потенціалу створюють нові внутрішні загрози для інформаційної безпеки підприємств. У статті досліджено і проаналізовано проблеми інформаційної безпеки, пов'язані з внутрішніми порушниками компаній та їх інсайдерською діяльністю. Економічні звіти та аналітичні матеріали дозволили визначити актуальність і важливість даної роботи. Спираючись на наукову літературу, було здійснено огляд різних підходів до визначення поняття «інсайдер» та «інсайдерська інформація». Охарактеризовані основні ключові індикатори інсайдера та ознаки інсайдерської інформації. Представлена класифікація джерел даних для дослідження інсайдерських загроз, серед яких виділяють реальні дані системного журналу та дані із соціальних мереж; аналітична інформація з синтетичними аномаліями; змодельовані дані внаслідок формування стохастичних моделей; теоретико-ігровий підхід. Описані алгоритми виявлення інсайдерських загроз в залежності від намірів, поведінки, можливостей інсайдерів, від способів використання ресурсів, а також моделі, що включають декілька алгоритмів. Висвітлюються нормативні питання захисту інсайдерської інформації від несанкціонованого розголошення та правової відповідальності за неправомірне використання інсайдерської інформації в українському законодавстві.

**Ключові слова:** інформаційна безпека; внутрішні загрози; інсайдер; інсайдерська інформація; інсайдерська загроза; інсайдерська діяльність.

## ВСТУП

◦ **Постановка проблеми.** Розвиток сучасного суспільства стає все більш залежним від стрімкого впровадження інформаційних технологій у всі сфери нашого життя. Інформація та людський фактор стають тими системами, захист яких є найважливішим в інформаційній безпеці підприємства. Інформація може бути підроблена, втрачена, викрадена, пошкоджена, знищена не лише зовнішніми порушниками. Зловмисні, недбалі та скомпрометовані користувачі компаній становлять не менший ризик, який на сьогодні має тенденцію зростати. Як показує Глобальний звіт про витрати на внутрішні загрози за 2022 рік [1]:

- інциденти з інсайдерськими загрозами зросли на 44% за останні два роки;
- витрати на інцидент зросли більш ніж на третину до 15,38 мільйона доларів;
- вартість крадіжки облікових даних для організацій зросла на 65% з 2,79 мільйона доларів у 2020 році до 4,6 мільйона доларів на даний момент;
- час стримування інциденту з внутрішньою загрозою збільшився з 77 днів до 85 днів, що змусило організації витрачати найбільше на стримування;
- інциденти, які зайняли понад 90 днів, щоб стримати витрати організацій, у середньому становили 17,19 мільйонів доларів США на річній основі.

◦ Інша аналітична статистика «Insider Threats: 20 Alarming Facts and Figures» [2] підкреслює, що 25% співробітників використовують електронну пошту, щоб вилучити конфіденційні дані компанії; 34% глобальних компаній страждають від внутрішніх загроз; 50% організацій вважають, що вони вразливі до інсайдерських атак; 55 % організацій вважають привілейованих користувачів найбільшим ризиком внутрішньої загрози; 97% IT-лідерів вважають інсайдерські загрози серйозною проблемою безпеки.

◦ Атаки з боку інсайдерів, будь-то співробітники, постачальники чи інші компанії, законно підключені до комп'ютерної системи компанії, становлять більш згубну загрозу, ніж зовнішні атаки. Ці інсайдери мають знання про внутрішню роботу організації та повністю володіють усіма правами та привілеями, необхідними для здійснення атаки, яких не вистачає стороннім особам. Отже, інсайдери можуть зробити свої атаки звичайними операціями [1].

**Аналіз останніх досліджень і публікацій.** Аналіз попередніх досліджень та публікацій свідчить, що дана тема не є новою, певні дослідження висвітлені у працях [3] – [17]. Вважають, що початком обговорення на рівні наукових та правлячих організацій щодо внутрішніх загроз є проєкт «Інсайдерське дослідження загроз», який у 2002 році розпочали Програма CERT Інституту програмної інженерії Університету Карнегі-Меллона і Національний центр оцінки загроз (NTAC) Секретної служби США (USSS). Уперше був здійснений комплексний аналіз внутрішніх загроз на основі досвіду NTAC у поведінковій психології та технічного досвіду CERT з питань безпеки. Команда проєкту CERT акцентувала увагу на важливість використання реальних даних для створення моделі внутрішньої загрози — складних взаємодій, відносного ступеня ризику та непередбачених наслідків політики, практики, технологій, внутрішніх психологічних проблем та організаційної культури з часом. Таким чином було започатковано проєкт MERIT (Management and Education of the Risk of Insider Threat) – «Управління та навчання ризику внутрішньої загрози» [3].

Дослідники I.A. Gheyas і A.E. Abdallah [4] провели широкий огляд літератури з даної тематики з 1950 року до 2015 року та здійснили мета-аналіз для порівняння та ранжування існуючих внутрішніх загроз, алгоритмів виявлення та прогнозування внутрішніх загроз.

Результати цих наукових робіт показали, що отримати емпіричні дані щодо інсайдерських загроз для аналізу практично неможливо. Це є очевидним, оскільки зберігається тенденція матеріальної, службової, а також національної безпеки. Крім того, часто інсайдерські атаки навіть не фіксуються, оскільки зловмисник не залишає слідів.

Слід відзначити також, що на сучасному етапі розвитку юридичної науки все частіше піднімається питання про необхідність розвитку правового регулювання, спрямованого на забезпечення нормального функціонування інсайдерської діяльності та встановлення кримінальної й адміністративної відповідальності за незаконне використання інсайдерської інформації [5; 6; 7].

Постійний розвиток інформаційних технологій, зростаюча роль на сучасному етапі людського потенціалу створюють нові внутрішні загрози для інформаційної безпеки підприємств. Цим і підтверджується актуальність даного дослідження та визначає мету.

**Мета статті.** Метою статті є висвітлення питань, пов'язаних з інсайдерською інформацією та інсайдерськими загрозами для визначення рішень в управлінні внутрішніми загрозами на підприємстві.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

### Поняття та ознаки інсайдерської інформації

Поняття «інсайдерська інформація» в наукових колах розглядають з різних сторін правового поля, найчастіше на інтуїтивному рівні:

- істотна, публічно не розкрита інформація до певного часу;
- особливий різновид службової таємниці;
- особливий вид інформації з обмеженим доступом.

Інсайдерською може бути, наприклад, інформація щодо злиття чи розпаду компаній; фінансові звіти підприємства; інформація, яка може вплинути на бізнес-процеси компанії; істотні зміни у планах капіталовкладень товариства; операції зі значними активами емітента за неринковою ціною; знищення або пошкодження значної частини майна емітента внаслідок непередбачуваних подій тощо [6].

В Директиві Ради Європейських Співтовариств від 13 листопада 1989 року 89/592/ЄЕС інсайдерська інформація визначається як інформація, яка не була розголошена, має чітку форму і відноситься до одного чи декількох емітентів цінних паперів, що підлягають обігу або стосується одного чи декількох цінних паперів, що підлягають обігу, та розголошення якої вірогідно матиме суттєвий вплив на ціну відповідного цінного паперу чи паперів, що підлягають обігу [8].

В Україні вперше поняття «інсайдерської інформації» набуло юридичної сили у Законі "Про цінні папери та фондовий ринок" від 23.02.06 р. [5]: інсайдерська інформація – неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених цим Законом. Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією. Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону. Перелік відомостей, віднесених до інсайдерської інформації, визначається Державною комісією з цінних паперів та фондового ринку.

Інсайдерську інформацію слід відрізняти від комерційної таємниці. «Документи про неплатоспроможність підприємства (наприклад, за результатами проведеного аудиту), інформація про забруднення навколишнього природного середовища (за яке підприємство може бути покаране як штрафами, так і зобов'язанням відшкодувати заподіяні збитки) та інша інформація, яка не може бути комерційною таємницею, ймовірно може викликати падіння ринкової вартості цінних паперів відповідного емітента після її оприлюднення. А отже, до моменту оприлюднення вона може бути інсайдерською інформацією» [9, с. 181].

Підсумовуючи вище викладене, можна вважати, що основними ознаками інсайдерської інформації є істотність (комерційна цінність), непублічність, релевантність.

**Поняття та ключові характеристики інсайдера**

Аналіз наукових джерел дозволив зробити висновок, що точного визначення поняття «інсайдер» не існує, кожен дослідник розробляє власне тлумачення, яке є специфічним для його власного набору даних, ситуацій, упереджень і припущень. Зупинимося на деяких з них.

Банківська енциклопедія трактує поняття «інсайдер» (англ. insider [ɪnˈsʌɪdə]-всередині) – особа, яка завдяки своєму службовому становищу або спорідненим зв'язкам має доступ до конфіденційної інформації про діяльність банку, що недоступна широкій громадськості, та може використати її у власних цілях з метою збагачення, одержання неконкурентних переваг, привілеїв тощо [10]. Далі перераховуються належність фізичних і юридичних осіб до класу інсайдерів.

Автори дослідження [11] пропонують розширити це поняття, враховуючи питання кібер- та фізичної безпеки. Інсайдер може бути визначений щодо двох примітивних дій:

- порушення політики безпеки з використанням легітимного доступу;
- порушення політики контролю доступу шляхом отримання несанкціонованого доступу.

У першому випадку інсайдер використовує свій законний доступ для виконання певних дій, які суперечать політиці безпеки, наприклад, коли конфіденційні дані передаються третім особам або коли доступ до ресурсу надається чи блокується. У другому випадку інсайдер використовує свій доступ для розширення своїх привілеїв таким чином, що порушує політику контролю доступу та безпеки.

Близьке поняття зустрічаємо у науковій праці [12] : інсайдер – довірена особа, якій надано повноваження порушувати політику безпеки.

Як стверджує група науковців [13], інсайдерами можуть бути колишні чи незадоволені працівники чи будь-який діловий партнер, який має чи мав санкціонований доступ до інформації для будь-якої конкретної організації. Вони мають заходи контролю та безпеки.

У роботі [14] дотримуються наступного визначення: інсайдери — це авторизовані користувачі, які мають законний доступ до конфіденційної інформації і вони можуть знати уразливі місця розгорнутих систем і бізнес-процесів.

Сучасні інформаційні потоки ініціюють створення так званих «структурних інсайдерів». Як стверджується в [15], «структурні інсайдери» – високошвидкісні трейдери, які купують і продають цінні папери за мілі- та мікросекунди. Цьому має сприяти декілька умов: близьке розташування з серверами біржі; постійні інформаційні потоки між біржами і трейдерами; автоматична відповідь на нові інформаційні масиви. Все це вимагає швидкодійних алгоритмів для обробки великих масивів даних у режимі

реального часу (HFT – high-frequency trading). Таким чином, перевага «структурних інсайдерів» в тому, що вони першими отримують новітню інформацію та торгують нею, а сторонні особи змушені здійснювати операції із застарілими даними та старими цінами.

З метою створення «портрету інсайдера» узагальнимо його ключові характеристики:

- інсайдери мають легітимний доступ до конфіденційної інформації;
- знають уразливості інформаційних активів;
- мають добре сформовані навички для здобуття цінної інформації;
- інсайдери завжди мотивовані (матеріальна сторона або емоційне невдоволення та помста).

У науковій роботі [16] підкреслюється, що для здійснення інсайдерської атаки мають бути одночасно три елемента: мотив, здатність, можливість.

Визначення окреслених ознак «портрету інсайдера» дає можливість сформувати поняття «інсайдерська діяльність». Інсайдерська діяльність – спрямовані дії мотивованих суб'єктів, які мають легітимний доступ до інформаційних активів та навички для здобуття цінної інформації, знають уразливі місця інформаційних систем і бізнес-процесів, для завдання матеріальних збитків та/або репутаційних втрат організації.

**Інсайдерські загрози та алгоритми їх виявлення**

Інсайдерська загроза проявляється, коли поведінка людей відходить від усталеної політики, незалежно від того, чи є вони результатом злоби, ігнорування чи незнання [17]. Інсайдерська загроза – це сукупність факторів, які можуть становити причину небажаного інсайдерського інциденту.

Вчені неодноразово підкреслювали вагомість емпіричних даних для моделювання та розроблення алгоритмів виявлення внутрішніх загроз. Джерелами для таких даних можуть слугувати [4]:

- реальні дані системного журналу;
- дані соціальних мереж;
- змодельовані дані, отримані зі стохастичних моделей;
- реальні дані з синтетичними аномаліями;
- змодельовані дані, отримані зі стохастичних моделей, розроблених на основі реальних даних;
- теоретико-ігровий підхід.

Удосконалення апаратних та програмних засобів захисту інформації дозволяють виділити джерела даних внаслідок моніторингу на основі хоста та мережі, які мають відношення до виявлення внутрішньої загрози: записи реєстру, дозволи на файли, події системи виявлення вторгнень (IDS), доступ до облікового запису, журнали брандмауера, перехоплення вмісту електронної пошти, журнали сервера доменних імен (DNS)/доступ до Інтернет-сайтів, обмін миттєвими повідомленнями, відома сигнатура програмного забезпечення [17].

Разом з тим, перевіряючи здатність виявляти інтрузивну поведінку у внутрішньому середовищі, необхідно подбати про придушення частоти помилкових тривог. Вирішення даного питання пропонується у роботі [4] із застосуванням ймовірнісного підходу, який ілюструє частоту виникнення події у відсотках, при цьому враховуючи частоту помилкових тривог на прийнятному рівні.

Узагальнення наукового доробку засвідчило, що у науковій літературі сформувалось декілька підходів до діагностики виявлення та прогнозування внутрішніх

загроз. Так, у дослідженні [4] здійснено огляд алгоритмів виявлення та прогнозування внутрішніх загроз. Ці алгоритми поділяються на 6 категорій моделей, які представлені у таблиці 1.

*Таблиця 1.*

**Алгоритми виявлення та прогнозування внутрішніх загроз**

| Назва моделі | Опис |
|---|---|
| Модель намірів (IM) | Впровадження психосоціальних покажчиків на основі психологічних профілів інсайдерів |
| Модель поведінки особистості (IBM) | Внаслідок минулої інформації щодо діяльності інсайдера створюється його модель поведінки |
| Модель поведінки спільноти (CBM) | Внаслідок минулої інформації щодо цілої групи інсайдерів створюється модель поведінки |
| Модель використання ресурсів (RUM) | Внаслідок аналітичних даних щодо використання інсайдерами якогось інформаційного ресурсу будується відповідна модель |
| Модель можливостей (CM) | Внаслідок статистичних даних щодо використання інсайдером різних рівнів IT-ресурсів моделюється відповідна діяльність |
| Змішана система (MS) | Технологія включає декілька моделей |

Сучасний етап характеризується впровадженням саме змішаних систем і методик виявлення інсайдерських загроз. Науковці пробують об'єднати два підходи у цьому напрямі:

- психосоціальний підхід, підґрунтям якого є аналіз психічних та емоційних станів співробітників, і це можливо дозволить передбачити поведінку інсайдера;
- неперервний моніторинг у мережі.

Так, робота вчених [17] продемонструвала підхід прогнозного моделювання до пом'якшення внутрішньої загрози, який має на меті об'єднати різноманітний набір джерел даних не лише кібер-сферу, а також психологічні/мотиваційні фактори, які можуть лежати в основі зловмисних інсайдерських дій. Система CHAMPION (Columnar Hierarchical Autoassociative Memory Processing In Ontological Networks) містить ієрархічну структуру міркувань, організовану семантичним шаром, який забезпечує теоретико-графові методи розпізнавання образів. Ця комплексна система оцінки загроз автоматизує виявлення високоризикованих видів поведінки («попередників» або «тригерів»), на яких можна зосередити увагу та надати цей аналіз персоналу з кібербезпеки, які в іншому випадку повинні були б аналізувати та співвідносити величезну кількість даних.

Проте, як свідчить огляд представленої літератури, ще не розроблено жодних системних методів, комплексних технологій, які б забезпечували повний та ефективний підхід до запобігання витоку даних, саботажу, шпигунства та диверсій.

Узагальнена інформація пропонується на рис 1.

ISSN 2663 - 4023


*Рис.1. Інсайдер та Інсайдерська інформація: суть, загрози, діяльність*

**Відповідальність за інсайдерську діяльність**

23 лютого 2006 року Верховною Радою було ухвалено Закон України «Про цінні папери та фондовий ринок» № 3480-IV, де уперше в Україні передбачено заборону, зокрема, здійснення торгівлі цінними паперами з використанням інсайдерської інформації та внесено зміни до Кримінального кодексу України з метою встановлення кримінальної відповідальності за розголошення або використання неоприлюдненої інформації про емітента або його цінні папери. Зокрема, в статті 146 Заборона використання інсайдерської інформації визначається, що особі, яка володіє інсайдерською інформацією, забороняється:

1) вчиняти з використанням інсайдерської інформації на власну користь або на користь інших осіб правочини щодо фінансових інструментів, яких стосується інсайдерська інформація, до моменту оприлюднення такої інформації;

2) передавати інсайдерську інформацію або надавати доступ до неї іншим особам, крім розкриття інформації в межах виконання професійних, трудових або службових обов'язків та в інших випадках, передбачених законодавством;

3) надавати будь-якій особі рекомендації стосовно фінансових інструментів, щодо яких вона володіє інсайдерською інформацією, до моменту оприлюднення такої інформації.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Внутрішні порушники – інсайдери через законний доступ до інформації, систем і мереж своїх організацій становлять значний ризик для організацій різних рівнів і напрямів. Виявлення та прогнозування інсайдерської загрози можливо лише при наявності такої моделі, яка б комплексно та у взаємозв'язку описувала інформаційні активи та працівників компанії. Вектор наступних досліджень планується у напрямку визначення «моделі інсайдера», його психосоціальних характеристик.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 2022 Ponemon Cost of Insider Threats Global Report https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

2 Infographic: 20 Alarming Insider Threats Statistics. https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/

3 Moore, A. P., Cappelli, D. M., Trzeciak, R. F. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures. У *Insider Attack and Cyber Security* (с. 17–52). Springer US. https://doi.org/10.1007/978-0-387-77322-3_3

4 Gheyas, I. A., Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1). https://doi.org/10.1186/s41044-016-0006-0

5 Про цінні папери та фондовий ринок, Закон України № 3480-IV (2021) (Україна). https://zakon.rada.gov.ua/laws/show/3480-15#Text

6 Дудоров, О.О., Каменський, Д.В. (2019). Інсайдерська інформація та кримінальний закон: від американських реалій до європейських перспектив, Юридичний науковий електронний журнал, 3, 185–201. http://dspace.lduvs.edu.ua/jspui/handle/123456789/306

7 Нашинець-Наумова, А. (2016). Поняття та ознаки інсайдерської інформації як особливого виду інформації з обмеженим доступом. *Підприємництво, господарство і право*, (4 (242)).

8 Council Directive 89/592/EEC of 13 November 1989 coordinating regulations on insider dealing. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0592:EN:HTML

9 Саєнко, В. В. (2002). *Правове регулювання використання інсайдерської інформації на ринку цінних паперів* [Неопубл. автореф. дис. канд. юрид. наук]. КНУТШ.
10 Колектив авторів. (2011). *Банківська енциклопедія*. ЦНД НБУ «Знання». ISBN. 978-966-346-923-2.
11 Bishop, M., Gates, C. (2008). Defining the insider threat. У *the 4th annual workshop*. ACM Press. https://doi.org/10.1145/1413140.1413158
12 Udoeyop, A. W. (2010). *Cyber Profiling for Insider Threat Detection* [Text]. Trace: Tennessee Research and Creative Exchange. http://trace.tennessee.edu/utk_gradthes/756
13 Ambre, A., Shekokar, N. (2015). Insider Threat Detection Using Log Analysis and Event Correlation. *Procedia Computer Science*, *45*, 436–445. https://doi.org/10.1016/j.procs.2015.03.175
14 Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M. (2019). *Insight Into Insiders and IT*. A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. https://dl.acm.org/doi/10.1145/1413140.1413158
15 Yadav, Ye (2018). .Insider Information and the Limits of Insider Trading. *Washington University Journal of Law & Policy*, 56. https://openscholarship.wustl.edu/law_journal_law_policy/vol56/iss1/14
16 Kandias, M. (2017). Insider threat prediction: *Psychosocial characteristics extraction and security data science techniques on OSN OSINT*. Department of Informatics Athens University of Economics & Business Athens, Greece. https://www.infosec.aueb.gr/Publications/Miltiadis%20Kandias%20PhD%20Thesis%20Site.pdf
17 Greitzer, F. L., Hohimer, R. E. (2011). Modeling Human Behavior to Anticipate Insider Attacks. *Journal of Strategic Security*, *4*(2), 25–48. https://doi.org/10.5038/1944-0472.4.2.2

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

**Svitlana M. Shevchenko**
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

**Yuliia D. Zhdanova**
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

**Pavlo M. Skladannyi**
PhD,
Head of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

**Sofia V. Boiko**
Student of the Faculty of Information Technology and Management
Borys Grinchenko Kyiv University, Kyiv, Ukraine
svboiko.fitu18@kubg.edu.ua

# INSIDERS AND INSIDER INFORMATION: ESSENCE, THREATS, ACTIVITIES AND LEGAL RESPONSIBILITY

**Abstract.** The constant development of information technologies, the growing role at the present stage of human potential create new internal threats to the information security of enterprises. The article investigates and analyzes the problems of information security associated with internal violators of companies and their insider activity. Economic reports and analytical materials allowed to determine the relevance and importance of this work. Based on scientific literature, a review of various approaches to the definition of "insider" and "insider information" was carried out. The main key indicators of the insider and signs of insider information are described. The classification of data sources for the study of insider threats is presented, among which real data of the system journal and data from social networks are allocated; analytical information with synthetic anomalies; simulated data due to the formation of stochastic models; theoretical and gaming approach. Insider threat detection algorithms are described depending on intentions, behavior, capabilities of insiders, how resources are used, as well as models involving several algorithms. The normative issues of protection of insider information from unauthorized disclosure and legal responsibility for illegal use of insider information in Ukrainian legislation are covered.

**Keywords:** information security; internal threats; insider; insider information; insider threat; insider activity.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1 2022 Ponemon Cost of Insider Threats Global Report https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
2 Infographic: 20 Alarming Insider Threats Statistics. https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/
3 Moore, A. P., Cappelli, D. M., Trzeciak, R. F. (2008). The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures. У *Insider Attack and Cyber Security* (с. 17–52). Springer US. https://doi.org/10.1007/978-0-387-77322-3_3

4 Gheyas, I. A., Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1). https://doi.org/10.1186/s41044-016-0006-0

5 Pro tsinni papery ta fondovyy rynok, Zakon Ukrayiny № 3480-IV (2021) (Ukrayina). https://zakon.rada.gov.ua/laws/show/3480-15#Text

6 Dudorov, O.O., Kamens′kyy, D.V. (2019). Insayders′ka informatsiya ta kryminal′nyy zakon: vid amerykans′kykh realiy do yevropeys′kykh perspektyv, Yurydychnyy naukovyy elektronnyy zhurnal, 3, 185–201. http://dspace.lduvs.edu.ua/jspui/handle/123456789/306

7 Nashynets′-Naumova, A. (2016). Ponyattya ta oznaky insayders′koyi informatsiyi yak osoblyvoho vydu informatsiyi z obmezhenym dostupom. Pidpryyemnytstvo, hospodarstvo i pravo, (4 (242)).

8 Council Directive 89/592/EEC of 13 November 1989 coordinating regulations on insider dealing. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0592:EN:HTML

9 Sayenko, V. V. (2002). Pravove rehulyuvannya vykorystannya insayders′koyi informatsiyi na rynku tsinnykh paperiv [Neopubl. avtoref. dys. kand. yuryd. nauk]. KNUTSH.

10 Kolektyv avtoriv. (2011). Bankivs′ka entsyklopediya. TSND NBU «Znannya». ISBN. 978-966-346-923-2.

11 Bishop, M., Gates, C. (2008). Defining the insider threat. У *the 4th annual workshop*. ACM Press. https://doi.org/10.1145/1413140.1413158

12 Udoeyop, A. W. (2010). *Cyber Profiling for Insider Threat Detection* [Text]. Trace: Tennessee Research and Creative Exchange. http://trace.tennessee.edu/utk_gradthes/756

13 Ambre, A., Shekokar, N. (2015). Insider Threat Detection Using Log Analysis and Event Correlation. *Procedia Computer Science*, *45*, 436–445. https://doi.org/10.1016/j.procs.2015.03.175

14 Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M. (2019). *Insight Into Insiders and IT*. A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. https://dl.acm.org/doi/10.1145/1413140.1413158

15 Yadav, Ye (2018). .Insider Information and the Limits of Insider Trading. *Washington University Journal of Law & Policy*, 56. https://openscholarship.wustl.edu/law_journal_law_policy/vol56/iss1/14

16 Kandias, M. (2017). Insider threat prediction: *Psychosocial characteristics extraction and security data science techniques on OSN OSINT*. Department of Informatics Athens University of Economics & Business Athens, Greece. https://www.infosec.aueb.gr/Publications/Miltiadis%20Kandias%20PhD%20Thesis%20Site.pdf

17 Greitzer, F. L., Hohimer, R. E. (2011). Modeling Human Behavior to Anticipate Insider Attacks. *Journal of Strategic Security*, *4*(2), 25–48. https://doi.org/10.5038/1944-0472.4.2.2