Міністерство освіти й науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

МЕТОДОЛОГІЯ НАУКОВИХ ДОСЛІДЖЕНЬ В ІТ-ГАЛУЗІ

Конспект лекцій

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Одеса-2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач кафедри «Кібербезпека та захист інформації»

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»

(Протокол від «06» жовтня 2025 р. №2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП

(Протокол від «14» жовтня 2025 р. №2)

ЗМІСТ

Тема 1. ВСТУП ДО МЕТОДОЛОГІЇ НАУКОВИХ ДОСЛІДЖЕНЬ В ІТ-ГАЛУЗІ

План

1. **Поняття методології. Особливості ІТ-досліджень**
2. **Предмет і сутність науки**
3. **Парадигми наукового знання: від класичної до постнекласичної науки.**
4. **Різниця між академічними та прикладними дослідженнями в ІТ.**
5. **Етика досліджень і академічна доброчесність.**

1. Поняття методології. Особливості ІТ-досліджень

Методологія — це система теоретичних принципів, практичних методів, прийомів і засобів, які застосовуються для отримання науково обґрунтованих результатів.

В ІТ-галузі методологія враховує специфіку цифрових технологій, програмного забезпечення та обчислювальних процесів.

Можна уявити, що загальна методологія — це фундамент. Вона формує універсальні принципи: науковість, обґрунтованість, системність, відтворюваність. Методологія в ІТ-галузі — це адаптація цих принципів до специфіки цифрових технологій, програмного забезпечення й обчислювальних процесів, дуже швидкої динаміки розвитку.

Побудова будь-якої методології передбачає проведення певних досліджень.

Особливості ІТ-досліджень

1. ***Динамічність*** — технології швидко змінюються, дослідження повинні бути актуальними. Як приклад розглянемо галузь кібербезпеки: методи захисту, актуальні 5 років тому (наприклад, підхід з простим firewall), сьогодні вже недостатні через розвиток Zero Trust Architecture та хмарних середовищ. Дослідження старих загроз (наприклад, вірусів, що видаляють інформацію) мають історичну цінність, але практично не застосовуються в сучасній безпеці. Розглянемо, враховуючу сучасність і актуальність, основні ідеї ***Zero Trust Architecture*** - сучасної концепції кібербезпеки, яка базується на принципі «нікому не довіряй, завжди перевіряй», руйнуючи традиційні підходи безпеки, коли вважалося, що всередині корпоративної мережі всі користувачі «свої», головне завдання — побудувати периметр і захистити його. При такому підході якщо зловмисник зможе прорватися всередину, він отримує широкий доступ. Zero Trust руйнує цю логіку: немає поняття «безпечної внутрішньої мережі», кожен доступ повинен підтверджуватись і контролюватися — незалежно від того, звідки він походить (зовні чи зсередини). Міжнародний досвід останніх років демонструє перспективність цього підходу до вирішення проблем кібербезпеки. Цей підхід є особливо актуальним для державних мереж, де критично важливо забезпечити безперервний контроль доступу до чутливої інформації та критичних систем.
2. ***Віртуальність експерименту*** — більшість досліджень проводиться в комп’ютерних середовищах, симуляторах, на моделях.

3. ***Алгоритмічність*** — процес дослідження часто описується у вигляді алгоритму. І хоча алгоритмізація дослідження притаманна будь-якій науці, зокрема ІТ, в ІТ-галузі алгоритмічність має додатково унікальність в тому сенсі, що тут часто алгоритм є об'єктом і продуктом дослідження: розробка нових алгоритмів (наприклад, шифрування, організації прихованого (стеганографічного) каналу в галузі інформаційної безпеки), оптимізація пошукових алгоритмів, удосконалення, підвищення ефективності існуючих алгоритмів. Таким чином, алгоритмічність в ІТ-галузі – це не лише «логіка кроків дослідника», а й, можливо, сутність того, що досліджується. Крім того, в ІТ-дослідженнях можна не тільки описати їх етапи, а й закодувати алгоритм дослідження у вигляді комп'ютерної програми чи сценарію.
4. ***Міждисциплінарність***. ІТ-галузь має власні фундаментальні дослідницькі напрями, які розвиваються незалежно від зовнішніх сфер, наприклад, теорія алгоритмів (проблема NP-повноти, обчислювальної складності), штучний інтелект і машинне навчання (нові архітектури, методи навчання), кібербезпека (криптографія, Zero Trust, постквантові алгоритми, стеганографія), комп'ютерні мережі (протоколи, оптимізація 5G/6G, IoT), програмна інженерія (методології розробки, формальні верифікації), обчислювальні системи (паралельні та розподілені обчислення, квантові комп'ютери). Тут ІТ виступає повноцінною дослідницькою галуззю, яка виробляє нові знання, теорії, методи. Але окрім власних фундаментальних досліджень, ІТ ще й створює моделі й алгоритми для інших наук (біоінформатика, соціальні науки тощо), стає провідником інновацій у медицині, економіці, освіті. Тут ІТ надає інстументи, що дозволяють вирішувати завдання інших сфер. Наприклад, генетичні алгоритми, що були розроблені для оптимізації в інформатиці, використовуються в інженерії (оптимізація конструкцій), економіці (моделювання ринків), робототехніці (еволюційний дизайн). Таким чином, ІТ-дослідження мають дві сторони: самостійна наука з власними теоретичними і прикладними проблемами, а також інструментальна наука, що підтримує інші дисципліни. Ця подвійність також вносить унікальність в ІТ-галузь: вона генерує нові знання сама по собі і прискорює розвиток інших наук.
5. ***Автоматизація та відтворюваність***.
   Автоматизація в ІТ-дослідженнях означає, що деякі (багато) етапи дослідження можна запускати автоматично після попереднього кодування. Це зменшує вплив людського фактору, економить час, підвищує точність, при цьому підвищення точності відбувається завдяки знов-таки зменшенню впливу людського фактору, а також завдяки забезпеченню однаковості умов експерименту, можливості працювати з великими даними без втрат, усуненню суб'єктивизму, полегшенню масштабування та перевірки результатів. Наприклад, в кібербезпеці застосовується автоматизоване виявлення загроз з використанням SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), при цьому SIEM-система автоматично збирає журнали (логи) з серверів, мережевих пристроїв, програм, аналізує їх у режимі реального часу, використовуючи правила й алгоритми для виявлення підозрілої активності (наприклад, багаторазові спроби входу з різних IP). Якщо SIEM виявляє

загрозу, SOAR запускає автоматичну реакцію, наприклад, блокує підозрілу IP-адресу у firewall; відключає скомпрометований акаунт; сповіщає адміністратора. Завдяки цьому процеси, які раніше займали години чи дні, виконуються за секунди.

Відтворюваність в IT-дослідженнях означає, що результати дослідження можна відтворити іншими дослідниками за тих самих умов. І хоча це фундаментальний принцип науковості, в IT він має свої унікальні інструменти. А саме:

- Системи контролю версій (Git, GitHub, GitLab, Bitbucket) дозволяють фіксувати всі зміни коду, експериментів і навіть наукових статей. Інший дослідник може завантажити потрібну версію й отримати ідентичне середовище. Системи контролю версій фіксують код і дозволяють відновити стан проєкту.
- Контейнеризація та віртуалізація (Docker, Kubernetes, VirtualBox) дозволяють «упакувати» програму з усіма залежностями (бібліотеками, середовищем) у контейнер, що гарантує, що експеримент запуститься однаково на будь-якому комп'ютері.
- Open Data та Open Code - відкриті набори даних (Kaggle, UCI ML Repository, OpenML). Публікація коду разом із науковими статтями, що дозволяє іншим дослідникам завантажити ті самі дані й перевірити результати.
- Jupyter Notebook та інші інтерактивні середовища дають змогу об'єднати код, дані, пояснення та візуалізації в одному документі. Інший дослідник запускає «ноутбук» і крок за кроком відтворює експеримент.

Таким чином, унікальність IT полягає в тому, що відтворюваність тут технічно забезпечується спеціальними інструментами. Це робить IT-дослідження одними з найбільш «прозорих» і таких, що найкраще відповідають ідеалам сучасної науки.

Автоматизація та відтворюваність йдуть поряд: автоматизація робить дослідження швидкими та масштабованими, відтворюваність робить їх науково достовірними та придатними для перевірки. Разом вони формують новий стандарт наукової роботи в IT: дослідження мають бути описані, автоматизовані й відтворювані іншими.

2. Предмет і сутність науки

Наука – сфера діяльності людини, спрямована на одержання (вироблення і систематизацію у вигляді теорій, гіпотез, законів природи чи суспільства, методів тощо) нових знань про навколишній світ.

За Кантом, наука є сукупністю знань, впорядкованих згідно з певними принципами, реальним зв'язком правдивих суджень, передбачень і проблем дійсності та окремих її сфер чи аспектів.

"Наука" – явище складне, багатогранне і тому має декілька основних значень (рис. 1.1) [Зацерковний]

Рис.1.1. Компоненти науки

Наука - специфічна сфера людської діяльності, яка спрямована на вироблення і систематизацію нових знань

Специфічність науки полягає в її наступних рисах:

- Цілеспрямованість: головна мета науки полягає в тому, щоб не просто накопичувати факти, а пояснювати закономірності й відкривати нове;
- Методологічність: наука має власні методи - аналіз, синтез, експеримент, моделювання тощо.
- Відтворюваність: будь-який науковий результат має бути перевірений і підтверджений іншими дослідниками.
- Обґрунтованість: наукові знання базуються не на віруваннях чи інтуїції, а на доказах, аргументах, логіці.

Спрямованість науки на вироблення знань означає, що наука не просто користується вже готовими знаннями, а створює нові, при цьому нове знання може бути теоретичним (закони, моделі, концепції), практичним (технології, методи, алгоритми).

Спрямованість науки на систематизацію знань: знання не існує хаотично, воно структурується у вигляді теорій, гіпотез, концепцій, класифікацій, наукових дисциплін. Саме системність відрізняє науку від буденного досвіду чи народної мудрості.

Наука як система одержаних наукових знань, що є основою наукового розуміння світу. Знання в науці організовані у вигляді понять, категорій, законів, гіпотез, теорій, вони представляють не хаотичні факти, а впорядковану структура, при цьому кожне нове відкриття не є «ізольованою вершиною», а інтегрується в цілісну систему. Системність забезпечує пояснювальну силу науки: вона не лише описує явища, а й пояснює їх, відкриває причинно-наслідкові зв'язки. Розглянемо приклад системності знань у науці на прикладі кібербезпеки. Ітак, ми маємо **факти** (емпіричний рівень):

- Кібератака на енергосистему України (грудень 2015 р.), в результаті якої сотні тисяч людей залишилися без електроенергії. Це перший задокументований випадок успішного застосування кіберзброї проти енергосистеми держави;

- Кібератака BlackEnergy (2016 р.) - використовувалося шкідливе ПЗ BlackEnergy для виведення з ладу об’єктів критичної інфраструктури. Було порушено роботу енергомереж, що призвело до масштабних відключень;
- Вірус NotPetya (2017 р.) - масштабна атака, що почалася саме з України. Вірус швидко поширився по світу, вразивши банки, аеропорти, транспортні компанії. Збитки оцінювалися у мільярди доларів;
- Кібератаки перед початком вторгнення РФ у лютому 2022 р. - були здійснені масові DDoS-атаки на сайти урядових установ і банків (ПриватБанк, Ощадбанк, Міноборони, Кабмін), було застосовано шкідливе ПЗ, яке спотворювало дані на комп’ютерах державних і приватних організацій;
- Кібератака на телекомунікації та ЗМІ (2022–2023 рр.) - атаки на провайдера «Київстар» (грудень 2023 року) призвели до відключення мобільного зв’язку та інтернету в багатьох регіонах України. Це був один із найбільших кіберінцидентів у телекомунікаціях країни.

Щоб узагальнити факти, вводяться ***ключові поняття***: вразливість – слабке місце системи; загроза – потенційна небезпека; атака – реалізована загроза; фішинг, вірус, хробак, троян – різновиди шкідливого ПЗ. Завдяки поняттям факти отримують наукове пояснення. Звісно, що наведені ключові поняття виникли не на основі запропонованих вище сучасних фактів, а набагато раніше. А от останні факти можна розглядати як основу для розширення системи ключових понять - формування нових понять (кібервійна, кіберзброя, критична інфраструктура), а згодом і для категорій, закономірностей і теорій у науці про кібербезпеку.

Далі факти й поняття групуються у **категорії.** Для нашого прикладу можливі:

- Типи атак (мережеві, соціальна інженерія, експлуатація вразливостей;
- Методи захисту (криптографія, контроль доступу тощо);
- Принципи безпеки (конфіденційність, цілісність, доступність).

У кібербезпеці вже сформульовано певні стійкі **закономірності**, наприклад:

- Складність атаки зростає зі складністю інфраструктури, а вразливостей стає більше;
- Без регулярного оновлення ПЗ рівень захисту системи невпинно знижується тощо. Це універсальні знання, перевірені часом.

У сучасних дослідженнях формулюють нові припущення, що потребують часу для перевірки:

- Моделі машинного навчання виявляють аномалії у трафіку краще за класичні системи правил;
- Zero Trust Architecture знижує ризик внутрішніх атак на корпоративні мережі тощо.

Ці гіпотези перевіряються і можуть перейти в розряд нових закономірностей і теорій.

На найвищому рівні формуються **цілісні наукові системи,** наприклад:

- Теорія криптографії – базується на теорії чисел;

- Zero Trust Architecture – сучасна концепція безпеки, що відмовляється від «довіри всередині периметра».

Тут знання інтегровані у цілісні системи, що пояснюють і прогнозують розвиток подій.

Таким чином, у кібербезпеці можна побачити ***системність наукових знань***: факти → поняття → категорії → закономірності (правила, що діють завжди) → гіпотези (нові ідеї для перевірки) → теорії (узагальнені моделі, які формують наукову картину безпеки).

Наука формує ***сучасну наукову картину світу*** (наприклад, еволюційна теорія в біології, теорія відносності у фізиці, клітинна теорія в біології). Ця картина замінює міфологічні чи релігійні уявлення, роблячи розуміння світу об'єктивним. Наукові знання застосовуються в різних сферах: від пояснення природних явищ до створення технологій, прогнозування майбутнього. Саме наука дає суспільству орієнтири: як розвивати економіку, які технології впроваджувати, як захищати довкілля, захищати інформацію. На прикладі галузі кібербезпеки: моделі розвитку загроз дозволяють передбачати появу нових видів атак (наприклад, з використанням штучного інтелекту чи квантових комп'ютерів); аналітика загроз прогнозує ймовірність атак на державні установи та критичну інфраструктуру; моделювання поширення вірусів у мережах допомагає оцінити масштаб потенційних інцидентів. Тут знання дозволяють бачити наперед і готуватися до майбутніх ризиків.

Наука як система взаємозв'язків між науковими організаціями та членами наукової спільноти. Наука функціонує не ізольовано, а як мережа взаємодій: організації створюють умови, науковці продукують знання, а зв'язки забезпечують перевірку, обмін і розвиток (див.табл.1.1).

Таблиця 1.1. Наука як система взаємозв'язків

Елемент	Приклади	Функції у науці
Наукові організації	Академії наук (НАН України), університети, лабораторії, фонди	Забезпечують ресурси, інфраструктуру, фінансування, задають напрями досліджень
Члени спільноти	Студенти, аспіранти, дослідники, рецензенти, викладачі, наукові менеджери	Генерують знання, перевіряють результати, поширюють і впроваджують їх
Взаємозв'язки між організаціями	Спільні дослідницькі проєкти, міжнародні програми, конференції, публікації у журналах	Обмін знаннями, колективне вирішення глобальних проблем, стандартизація науки
Взаємозв'язки між людьми	Наукове керівництво, наставництво, співпраця в групах, рецензування статей, критика результатів	Підвищення якості досліджень, формування наукових шкіл, розвиток молодих науковців
Приклад з кібербезпеки	CERT-UA ↔ ENISA,	Забезпечення

	українські університети ↔ міжнародні дослідження, спільний аналіз вірусів (NotPetya)	кіберзахисту, формування глобальних стандартів безпеки, колективне реагування на загрози

Наука як продуктивна сила і наука як соціальний інститут:

Наука як продуктивна сила суспільства

- Наука безпосередньо впливає на виробництво: у сучасному світі розвиток технологій напряму визначає економічну потужність держав. Приклади: ІТ, штучний інтелект, біотехнології, нанотехнології — це вже не «знання для знання», а фактори конкурентоспроможності економіки.
- Наука сприяла заміні праці людини технікою: завдяки науці створюються нові машини, автоматизовані системи, робототехніка. Наука перетворюється на безпосередню продуктивну силу, бо її результати у вигляді знань «втілюються» в засоби виробництва. І це є дуже значною і затребованою характеристикою науки (захист дисертації потребує актів впровадження тощо).
- Інновації як двигун прогресу: суспільства з високим рівнем науки і технологій (наприклад, США, Японія, Південна Корея) показують приклад, як наукові знання визначають економічне зростання.

Наука як соціальний інститут

- Організація наукової діяльності: наука має свої структури - університети, академії, дослідницькі інститути, лабораторії; є власні норми (етика публікацій, рецензування, авторське право).
- Система соціальних ролей: вчені, дослідники, викладачі — це професійна спільнота, яка функціонує за певними правилами; формуються ієрархії: студент → аспірант → науковець. Система соціальних ролей у науці — це механізм функціонування науки як спільноти, де кожна роль важлива і взаємопов’язана з іншими.
- Взаємодія з іншими інститутами: наука тісно пов’язана з державою (державне фінансування), бізнесом (інноваційні стартапи), освітою (підготовка кадрів); вона стає механізмом передачі знань і технологій у суспільство.

Таким чином, наука відіграє економічну роль у виробництві, створенні технологій, інноваціях, при цьому має соціальну організацію та культурне значення: правила, норми, структури, які забезпечують функціонування науки. Тобто наука — не лише джерело ідей, а центральний фактор розвитку цивілізації, який визначає як матеріальний, так і духовний прогрес суспільства.

3. Парадигми наукового знання: від класичної до постнекласичної науки

1. Класична наука (XVII – XIX ст.). Характерними рисами класичної науки були: орієнтація на об’єктивність і детермінізм (світ розглядався як машина, що працює за законами Ньютона); суб’єкт і об’єкт чітко розділені; основні використовувані методи - експеримент, спостереження, математичне

моделювання. Представниками класичної науки є**:** класична механіка Ньютона, електродинаміка Максвелла.

2. Некласична наука (кінець XIX – XX ст.). Відкриття закону відносності Ейнштейном, квантової механіки, термодинаміки зруйнували уявлення про «механістичний світ»; суб'єкт і об'єкт вже не повністю розділені: умови експерименту впливають на результат (принцип невизначеності Гейзенберга); розуміння того, що світ не є повністю детермінований, з'являються ймовірнісні моделі; наука усвідомлює власні межі та відносність істини. Представниками некласичної науки є квантова фізика, теорія відносності.

3. Постнекласична наука (друга половина XX ст. – сьогодення). Дослідження складних, відкритих, самоорганізованих систем (біологічних, соціальних, технічних, систем захисту інформації); наука усвідомлює свою вбудованість у суспільство й культуру; важливою рисою є міждисциплінарність; вивчення хаосу, нестабільності, нелінійності. Наука мислиться як відкрита система, де знання постійно уточнюються й переглядаються. Прикладами постнекласичних теорій є теорія складних систем, штучний інтелект, біоінформатика.

Еволюція науки від класичної до постнекласичної парадигми показує, що наукове знання — це не застигла система істин, а динамічний процес, який змінюється разом із розвитком цивілізації. Так класична наука прагнула пояснити природу, сформувала фундамент для промислової революції, технічних відкриттів та становлення сучасної науки як провідного способу пізнання світу; некласична наука показала, що світ набагато складніший, сам дослідник і методи дослідження впливають на результат; постнекласична наука відображає нову реальність: ми живемо у світі глобальних системних викликів. Тут наука не лише «вивчає природу», а й усвідомлює власну відповідальність перед суспільством, прагне керувати взаємодією людини, суспільства й технологій у глобальному масштабі.

IT-галузь зобов'язана к**ласичній парадигмі** створенню перших обчислювальних машин за законами логіки та математики; н**екласичній -** розвитку теорії інформації, ймовірнісних алгоритмів, штучного інтелекту; п**остнекласичній -** дослідженню складних систем (штучний інтелект + суспільство + етика), кібербезпеці як глобальній проблемі.

4. Різниця між академічними та прикладними дослідженнями в IT

У науці прийнято розрізняти **академічні** (фундаментальні) та **прикладні** дослідження. Це два взаємопов'язані, але різні за спрямованістю типи наукової діяльності (табл.1.2).

Метою **фундаментальних** досліджень є отримання нових знань про закономірності світу без прямої орієнтації на практичний результат. Характер таких досліджень є теоретичним, пояснювальним, спрямованим на розширення наукової картини світу, вони дають «фундамент», на якому будуються майбутні технології. Прикладом фундаментальних досліджень у кібербезпеці можуть бути дослідження в теоретичній криптографії (дослідження математичних задач, що лежать в основі шифрування, наприклад, факторизація великих чисел); теоретичній стеганографії (отримання достатніх умов стійкості стеганосистеми до атак проти вбудованого повідомлення).

Метою **прикладних** досліджень є використання наукових знань для вирішення практичних завдань, вони орієнтовані на розробку технологій, продуктів, методів, алгоритмів, сервісів. Наприклад, створення антивірусного програмного забезпечення.

Таблиця 1.2. Порівняння академічних та прикладних досліджень

Ознака	Академічні дослідження	Прикладні дослідження
Мета	Пошук істини, нових знань	Практичне застосування знань
Характер	Теоретичні, фундаментальні	Емпіричні, орієнтовані на результат
Результат	Закони, теорії, моделі	Технології, методи, продукти
Часовий горизонт	Довгостроковий (результат може проявитися через десятки років)	Коротко- або середньостроковий (швидке впровадження)
Приклад із ІТ	Дослідження квантових технологій	Створення захищеного месенджера з квантовим шифруванням

Відмінність між «фундаментальним і прикладним» у науці загалом універсальна: теорія - практика, але в ІТ вона має свою специфіку: коротший шлях від ідеї до технології, більша алгоритмічність і швидше старіння результатів. У ІТ навіть фундаментальні результати часто мають форму математичної моделі, яку можна реалізувати програмно, на відміну від, наприклад, фізики чи біології, де теорія може бути абстрактною. В ІТ вона вже «напівприкладна» (модель - це майже готовий «рецепт»). У класичних науках проходять десятки років, перш ніж фундаментальне відкриття стає технологією (квантова механіка → комп'ютери). В ІТ цей розрив часто дуже короткий. Наприклад, Zero Trust Architecture була сформульована дослідниками у 2010–2011 рр., а практичне застосування уже через 5–7 років (великі компанії (Google, Microsoft, уряд США) почали масово впроваджувати Zero Trust у свою інфраструктуру). У кібербезпеці фундаментальні дослідження дуже швидко переходять у практику, бо дуже швидко еволюціонують загрози, бізнес і держава мають високий попит на захист, тому різниця між «фундаментальним відкриттям» і «технологією» в кібербезпеці (взагалі в ІТ) може становити лише кілька років (а може й місяців), а не десятиліття, як у класичних науках (див.табл.1.3).

У класичних науках межа між фундаментальними і прикладними дослідженнями більш чітка, ніж в ІТ (дослідження в стеганографії може бути і теоретичним (достатні умови стійкості стеганоалгоритму), і прикладним (достатні умови визначають конкретний спосіб вбудови додаткової інформації). У фізиці чи хімії фундаментальні теорії залишаються на десятиліття, в ІТ навіть фундаментальні моделі швидко змінюються.

Таблиця 1.3. Фундаментальні та прикладні дослідження в кібербезпеці

Критерій	Фундаментальні дослідження	Прикладні дослідження
Мета	Зрозуміти основи безпеки, сформулювати закони та моделі	Розробити практичні рішення для захисту систем
Характер	Теоретичні, пояснювальні	Емпіричні, інженерні
Приклади	- Теоретична криптографія (RSA, еліптичні криві як математика) - Постквантова криптографія (решіткові задачі) - Теорія обчислювальної складності (P vs NP) - Моделі інформаційної безпеки (CIA, Белла-Лападули, Біба) - Формальна верифікація протоколів	- Створення системи багатофакторної автентифікації - Розробка антивірусів чи IDS/IPS - Впровадження Zero Trust Architecture в компанії - Автоматизація виявлення DDoS-атак - Розробка захищених месенджерів
Результат	Теорії, моделі, доведення, математичні основи	Програмні продукти, інфраструктурні рішення, практичні методики
Часовий горизонт	Порівняно довгостроковий	Коротко-/середньостроковий (використання тут і зараз)
Цінність	Закладають фундамент усієї кібербезпеки, незалежно від технологій	Дають захист у реальних умовах, протистоять конкретним загрозам

Таким чином, академічні дослідження формують теоретичну основу науки в будь-якій галузі, прикладні дослідження перетворюють ці знання на практичні рішення, а разом вони утворюють повний цикл розвитку науки та технологій: від ідеї до практики.

5.Етика досліджень та академічна доброчесність

Етика досліджень - це система моральних принципів і норм, які регулюють діяльність ученого. Основними вимогами тут можна назвати наступні:

- Не шкодити (наприклад, у сфері кібербезпеки експерименти з атаками мають проводитися в ізольованих середовищах, без ризику для суспільства);

- Дотримання прав людини: конфіденційність даних, інформована згода на участь у дослідженні.
- Прозорість і чесність: недопустимість маніпуляцій результатами.
- Відповідальність за наслідки впровадження технологій (наприклад, етичність використання AI).

Академічна доброчесність - це сукупність принципів і правил у науці та освіті, що забезпечують довіру до результатів. Основними принципами тут є: оригінальність (недопустимість плагіату); коректне цитування (посилання на джерела); верифікованість (можливість перевірки поданих результатів іншими); відсутність фабрикацій та фальсифікацій (неможливість використання вигаданих даних та результатів); об'єктивність (неможливість підганяти результати під бажаний висновок); повага авторства (співавтори повинні бути зазначені чесно, без «гостьових»).

Етика досліджень та академічна доброчесність мають велике значення, оскільки формують довіру до науки й університетів, захищають суспільство від небезпечних експериментів, стимулюють якісні дослідження, а не «гонитву за кількістю публікацій». В IT і кібербезпеці етика досліджень та академічна доброчесність є критично важливими, бо помилка чи недоброчесність тут може коштувати національної безпеки (табл.1.4).

Таблиця 1.4. Академічна доброчесність у дослідженнях з IT та кібербезпеки

Принцип	Суть	Приклад в IT / кібербезпеці
Оригінальність	Уникати плагіату, створювати власні результати	Написання унікального коду чи алгоритму без копіювання з чужих проєктів без вказівки авторства
Коректне цитування	Давати посилання на джерела, визнавати авторів	У науковій статті навести бібліографію до використаних алгоритмів (наприклад, AES чи RSA)
Верифікованість	Результати мають бути перевірені іншими дослідниками	Викласти код експерименту на GitHub із відкритим доступом до даних
Відсутність фальсифікацій	Заборона вигадування чи підтасовки даних	Не можна симулювати «успішний захист від DDoS» на вигаданих логах
Об'єктивність	Не підганяти результати під бажані висновки	Якщо тест системи ШІ показав низьку точність, дослідник чесно публікує ці результати
Поважання авторства	Вказувати реальних	У публікації з

	співавторів, уникати «гостьових» імен	кібербезпеки зазначати всіх членів команди, які зробили внесок у дослідження
Відповідальність за наслідки	Усвідомлювати вплив на суспільство	Проводити пентести лише в тестових середовищах, не атакуючи «живі» системи користувачів

Питання

1. Особливості ІТ-досліджень: динамічність, віртуальність експерименту, алгоритмічність, міждисциплінарність, автоматизація та відтворюваність.
2. В чому полягає специфічність науки?
3. Наука - система взаємозв’язків між науковими організаціями та членами наукової спільноти. Пояснити.
4. Фундаментальні та прикладні наукові дослідження: цілі, характер, приклади.
5. Специфіка відмінності між фундаментальними і прикладними дослідженнями в ІТ-галузі.
6. Етика досліджень та академічна доброчесність.

Тема 2. ПОСТАНОВКА ТА ДИЗАЙН ДОСЛІДЖЕННЯ

План

1. **Наукова проблема, мета та задачі дослідження**
2. **Об'єкт і предмет дослідження**
3. **Висновки наукового дослідження**
4. **Дослідницький дизайн: експериментальний, кореляційний, якісний, змішаний**

1. Наукова проблема, мета та задачі дослідження

Наукове дослідження завжди починається з усвідомлення проблеми. Саме проблема є тим «стрижнем», навколо якого вибудовується все інше: мета, завдання, методологія, результати. У науці, як правило, не працюють з темами «заради теми». **Дослідження починаються, коли виявляється суперечність між потребами практики і можливостями наявних рішень**, прогалина в знаннях, яку ще ніхто не закрив, новий виклик, на який існуючі методи не дають адекватної відповіді. **Наприклад**, сучасна стеганографія використовує зараз на практиці приховані канали з незначною пропускною спроможністю, що вносить вкрай незначні зміни в контейнер, а існуючі стеганоаналітичні методи поки не розраховані повною мірою на такі умови. Ще один приклад: виявлення фальсифікацій цифрових контентів, де область фальсифікації дуже незначних розмірів. Саме з цього моменту народжується наукова проблема.

Таким чином, перед тим як писати статтю, дослідник має поставити собі ключове запитання: «Що в науці або практиці ще не вирішено, і який внесок можу зробити я?». І вже після усвідомлення проблеми ми можемо переходити до формулювання мети і завдань дослідження.

Таким чином, **наукова проблема** — це суперечність або невирішене питання в науці, яке потребує пояснення чи нового рішення. Тому проблемі притаманні: **актуальність** (вона має значення для науки чи практики саме зараз), для неї існує можливість зазначити, що вона не є повністю вирішеною або існуючі рішення мають обмеження.

Бажаною є **конкретність** проблеми – вона повинна бути не занадто загальною, хоча це не завжди може бути наявним. Дійсно, для нових галузей знань на старті проблема може бути описана загально (наприклад, «як навчаються нейронні мережі?»), і лише згодом уточнюється у конкретніші питання («які архітектури підвищують стійкість до шуму?»). Крім того, у складних система, зокрема у кібербезпеці, проблема часто багатошарова, її не можна «звузити» одразу, бо вона охоплює і технічні, і соціальні, і правові аспекти (наприклад, при побудові математичної моделі СЗІ кожна з її складових повинна мати деякий кількісний вираз, але ці складові дуже різні (організаційні, нормативно-правові, криптографічні, технічні тощо), тому складно надати їм кількісний вираз. Тому спробували звузити цю проблему, розглядаючи лише технічні засоби захисту інформації. На сьогодні вже існують можливі рішення загальної проблеми. Говорячи про конкретність проблеми, треба пам'ятати і те, що безперервно відбувається еволюція знань, разом з якою формулювання проблеми може змінюватися у процесі дослідження.

Як правило, проблема формулюється як суперечність або нестача знань, наприклад: «Існують методи …, але вони неефективні для …», «Дотепер не досліджено …, не запропоновано способів розв'язку….». У статті наукова проблема зазвичай подається у вступі.

Усвідомивши проблему, дослідник формулює **мету** свого дослідження. Мета - це своєрідна відповідь на проблему, вона формується в «світлі проблеми», спрямована на розв'язок проблеми, конкретизує й звужує проблему для даного дослідження. Зазвичай наукова проблема є ширшою, вона може містити цілий спектр питань, аспектів, нерозв'язаних суперечностей, а досягнення мети конкретного дослідження не вирішує проблему цілком. Мета дослідження обирає з цієї проблеми конкретний сегмент, з яким дослідник працює на даному етапі, а результати її досягнення є підмножиною результатів, необхідних для вирішення проблеми.

Розглянемо наступний **приклад**: *Проблема*: Сучасні методи виявлення кіберзагроз не забезпечують достатньої точності й швидкодії при зростанні обсягів мережевого трафіку та ускладненні атак. *Мета*: Підвищити ефективність виявлення DDoS-атак у високонавантажених мережах за допомогою алгоритмів машинного навчання. Тут проблема охоплює всю сферу кіберзагроз, а мета зосереджується лише на одному їхньому класі (DDoS).

Таким чином:

Мета наукового дослідження - це узагальнене уявлення про кінцевий результат, якого прагне досягти дослідник у процесі роботи, сформульоване як відповідь на поставлену наукову проблему.

Метою обов'язково повинно бути «покращення», «підвищення ефективності», «забезпечення…(того, що раніше не забезпечувалося)». В висновках роботи обов'язково повинно бути зазначено: «на скільки покращено», «на скільки підвищено ефективність», «що і як забезпечено», інакше мета роботи буде вважатися недосягненою.

Таким чином, мета повинна бути сформульована як кінцевий результат дослідження, а не процес («розробка/створення/моделювання» само по собі; розробка, створення, моделювання - це шляхи досягнення мети, а не сама мета); вона повинна бути конкретною і спрямованою на розв'язання (частки) проблеми; вона повинна бути **одна** для всього дослідження (а не кілька «цілей»).

Таким чином, загальною формулою для правильного формулювання мети дослідження можна вважати: «Мета дослідження полягає у [кінцевий результат/ефект] шляхом [шлях / спосіб / метод].

<u>Варіанти конструкцій:</u>

- Мета дослідження полягає у підвищенні [якісного показника] шляхом [метод/алгоритм/підхід], наприклад, мета дослідження полягає у підвищенні точності виявлення аномалій у мережевому трафіку шляхом застосування алгоритмів машинного навчання.
- Мета дослідження полягає у забезпеченні [умови/властивості] шляхом [інструменту], наприклад, мета дослідження полягає у забезпеченні стійкості до постквантових атак шляхом розробки певного криптографічного алгоритму.

- Мета дослідження полягає в удосконаленні [процесу/системи] через [новий підхід], наприклад, мета дослідження полягає в удосконаленні системи управління базами даних шляхом впровадження оптимізованого механізму індексації.
- Мета дослідження полягає у створенні умов для [результат] шляхом [засіб], наприклад, мета дослідження полягає у створенні умов для безпечного зберігання великих обсягів даних шляхом використання технологій блокчейну.
- Мета дослідження полягає у зменшенні [ризику/недоліку] завдяки [рішення], наприклад, мета дослідження полягає у зменшенні ризику успішних фішингових атак завдяки побудові інтелектуальної системи аналізу електронних листів.

Перейдемо до завдань дослідження, саме вони конкретизують, як саме дослідник досягне мети.

Завдання дослідження — це конкретні кроки, які необхідно виконати для досягнення мети. Вони показують шлях від «широкої цілі» до конкретних результатів. Завдання має бути логічним етапом досягнення мети, повинно бути реалістичним і перевірюваним.

Розглянемо приклад **. Мета: підвищити точність виявлення фішингових атак у банківських системах шляхом розробки методу, що враховує сучасні техніки соціальної інженерії. Для досягнення цієї мети необхідно вирішити наступні завдання:

- Проаналізувати існуючі методи виявлення фішингових атак; виявити їхні обмеження щодо виявлення сучасних технік соціальної інженерії;
- Розробити новий метод виявлення фішингових атак у банківських системах, що враховує сучасні техніки соціальної інженерії;
- Реалізувати експериментальну перевірку методу на тестових наборах даних;
- Оцінити ефективність розробленого методу порівняно з існуючими підходами.

Завдання дослідження завжди мають звучати як чіткі наукові дії, які ведуть до досягнення мети. Кожне завдання повинно бути сформульоване дієсловом, що означає активну дію: проаналізувати, систематизувати, узагальнити, визначити, виявити, класифікувати, обґрунтувати, довести, оцінити, виокремити, розробити, запропонувати, побудувати, удосконалити, порівняти, оцінити ефективність, визначити перспективи.

2. Об’єкт і предмет дослідження

Плутанина в розумінні того, що таке об’єкт і предмет дослідження, може призвести до недостовірності висновків і до підміни результатів дослідження припущеннями щодо істин, які встановлені раніше і не підлягають оспорюванню.

Об’єкт дослідження - це процес, явище або система, що існує у дійсності й породжує наукову проблему, на яку спрямована пізнавальна діяльність дослідника. Об’єкт є реальним, він існує незалежно від дослідника, саме в

ньому виникає суперечність чи «біле місце» знань; об’єкт є ширшим за предмет, він охоплює всю сферу, у якій розташована дослідницька проблема.

Для ІТ-галузі, зокрема кібербезпеки, для об’єкта дослідження можна виділити характерні риси:

- Значна швидкість змін: в ІТ цикл життя технологій іноді становить 2–3 роки, тоді як у фізиці чи біології - десятиліття. Це робить об’єкт дослідження в ІТ особливо нестабільним;
- Багато об’єктів існують лише у вигляді коду чи симуляцій (стеганосистема), на відміну від, наприклад, хімії чи біології, де об’єкт завжди має матеріальну основу, навіть якщо досліджується через моделі;
- У кібербезпеці об’єкт «живе» в умовах постійної протидії атакам (процес виявлення несанкціонованих змін інформації): захист - напад. При цьому, наприклад, у медицині також є «загрози» (віруси), але вони не змінюються так швидко і не мають «свідомого супротивника»;
- Глобальна масштабованість: кіберзагроза одразу може мати планетарний масштаб (вірус поширюється по світу за години), в той час у традиційних науках вплив часто повільніший (наприклад, епідемія — місяці/роки, а не хвилини), що звісно впливає на поведінку та характеристики об’єкту.

Предмет дослідження — це конкретні властивості, відносини, механізми або аспекти об’єкта, які безпосередньо вивчаються в даній науковій роботі. Предмет завжди вужчий, ніж об’єкт, він визначає фокус дослідження, описує саме те, що дослідник аналізує, моделює чи змінює в межах об’єкта.

Таким чином, можна собі уявити, що об’єкт - це поле, де існує проблема, а предмет - конкретна «точка» в цьому полі, яку ми досліджуємо.

Предмет у дослідженні більш конкретний, ніж об’єкт, і тому в ньому ще більше, ніж в об’єкті, проявляється специфіка ІТ та кібербезпеки.

Унікальні риси предмета дослідження в ІТ-галузі:

- Алгоритмічність: предмет часто є алгоритмом, моделлю або методом обробки даних, тобто у класичних науках предметом є природні явища, а в ІТ - штучні, створені людиною алгоритмічні структури.
- Програмна реалізованість: предмет практично завжди можна (і потрібно) втілити у вигляді коду, прототипу чи системи, в той час, як, наприклад, у фізиці чи соціології предмет не завжди підлягає прямій реалізації.
- Відтворюваність через цифрове середовище: інші дослідники достатньо легко можуть відтворити предмет дослідження (алгоритм, модель) у точності, якщо отримають код і дані, в той час, як, наприклад, у біології чи медицині відтворюваність залежить від складних зовнішніх факторів.
- Тісний зв’язок із практикою: предмет майже завжди орієнтований на розв’язання прикладної задачі (оптимізація пошуку, безпечна автентифікація, стиснення даних), тоді як у фундаментальних науках предмет може залишатися суто теоретичним.

Навіть в межах ІТ-галузі предмет дослідження в кібербезпеці має свої унікальності:

- Двоїстий характер: предмет охоплює і методи захисту, і способи атак (бо щоб захиститися від атак, нейтралізувати їх, треба на них розумітися). Тут дослідник працює з подвійною природою предмета.

- Динамічність загроз: предмет дослідження постійно змінюється разом із появою нових технік атак, наприклад, учора предметом було виявлення SQL-ін’єкцій, сьогодні — adversarial-атаки на ШІ.
- Етична й правова складова: предмет дослідження завжди пов’язаний з етикою (що дозволено/не дозволено тестувати) та правом (законність експериментів), що нехарактерно для більшості класичних предметів природничих наук.
- Взаємодія із супротивником: предмет не лише вивчає систему, а й передбачає дії «розумного опонента», відповідно, він завжди рухається у «гонці озброєнь».

Розглянемо декілька прикладів об’єкта і предмета дослідження в кібербезпеці:

- Тема: Методи виявлення фішингових атак у банківських системах.
  Об’єкт: процес забезпечення інформаційної безпеки в комп’ютерних мережах банківських систем.
  Предмет: методи виявлення фішингових атак, що базуються на аналізі вмісту електронних листів та поведінкових характеристик користувачів.
- Тема: Використання машинного навчання для виявлення DDoS-атак.
  Об’єкт: процес захисту комп’ютерних мереж від мережевих атак.
  Предмет: алгоритми машинного навчання для виявлення та класифікації DDoS-атак у реальному часі.
- Тема: Системи автентифікації користувачів у хмарних сервісах.
  Об’єкт: інформаційна безпека хмарних обчислювальних середовищ.
  Предмет: методи та протоколи багатофакторної автентифікації користувачів у хмарних сервісах

У кібербезпеці об’єкт майже завжди стосується «забезпечення інформаційної безпеки», а предмет - конкретних методів, алгоритмів, протоколів.

3. Висновки наукового дослідження

Висновки - це узагальнені результати дослідження, які логічно випливають із мети, завдань і отриманих даних, та відображають наукову новизну й практичне значення роботи.

Характерні риси висновків:

- кожне завдання повинно мати відображення у висновках;
- висновки не повторюють експериментальні дані, а підсумовують їх;
- вказують, що нового внесено у науку;
- показують, як результати можуть бути використані;
- як правило, формулюються стисло, але змістовно.

Повернемося до прикладу **. Висновки для нього можуть мати наступний вміст:

- Виконано аналіз існуючих методів виявлення фішингових атак та визначено їхні слабкі сторони: незадовільна адаптація до нових загроз, пов’язаних з застосуванням технік соціальної інженерії;
- Запропоновано метод виявлення атак, який поєднує контент-аналіз електронних листів із поведінковим аналізом користувачів.
- Експериментально перевірено, що метод підвищує точність виявлення атак на 15% у порівнянні з класичними підходами.

- Практичне значення полягає у можливості інтеграції запропонованого методу в банківські системи для зменшення кількості успішних атак.
- Подальші дослідження варто спрямувати на інтеграцію розробленого методу з моделями машинного навчання для його адаптивності до нових технік соціальної інженерії.

4. Дослідницький дизайн: експериментальний, кореляційний, якісний, змішаний

Дослідницький дизайн - це загальний план дослідження, логіка його організації: як саме ми збираємо дані, як їх аналізуємо і як відповідаємо на дослідницькі питання.

Розрізняють такі основні типи дослідницького дизайну: ***експериментальний, кореляційний, якісний, змішаний***.

- ***Експериментальний*** дизайн: дослідник активно втручається в умови, створює ситуацію і спостерігає за результатами. В ході проведення дослідження є змінні, які змінює дослідник (незалежні), і залежні, яка вимірюється. Експериментальний дизайн дає змогу встановити причинно-наслідкові зв'язки. Наприклад, тестування впливу різних алгоритмів шифрування (AES, RSA, ECC) на швидкість передачі даних у мережі.
- ***Кореляційний*** дизайн: дослідник не втручається, а спостерігає та аналізує взаємозв'язки між змінними, що дозволяє виявити, чи пов'язані змінні між собою, але не доводить причинність. Наприклад, дослідження залежності між кількістю фішингових листів і часом реакції системи безпеки на їх блокування.
- ***Якісний*** дизайн: орієнтований на глибоке розуміння явищ, а не на статистичну перевірку, використовує методи інтерв'ю, аналіз контенту, спостереження, результатом чого є опис, інтерпретація, розкриття смислів. Наприклад, інтерв'ю з фахівцями з кібербезпеки щодо практичних труднощів у впровадженні Zero Trust Architecture.
- ***Змішаний*** дизайн: поєднує кількісні (експеримент, кореляція) та якісні (інтерв'ю, кейси) методи, дає повнішу картину, бо кількісні дані показують закономірності, а якісні — пояснюють «чому так». Наприклад, кількісний етап - експерименти з продуктивністю нових алгоритмів детектування атак; якісний етап - опитування фахівців безпеки щодо зручності інтеграції цих алгоритмів у робочі процеси.

Вибір дизайну дає можливість впорядкувати свої дослідження, оскільки дослідницький дизайн забезпечує:

- Структурованість і прозорість: дизайн робить план явним і формалізованим, щоб будь-хто інший міг зрозуміти логіку того, як збиралися дані, чому саме так, як аналізувались;
- Відтворюваність: оскільки наука базується на тому, що інші можуть повторити дослідження і перевірити результат, то дослідницький дизайн тут дуже важливий, оскільки дає «рецепт» для повторення;
- Вибір правильних підходів: є різниця, чи ми хочемо довести причинність чи просто показати зв'язок. Без чіткого дизайну можна вибрати неправильний підхід і зробити сумнівні висновки.

- Легітимність і науковість: дизайн демонструє, що дослідження відповідає науковим стандартам, а не є хаотичною діяльністю. У магістерських і кандидатських роботах це особливо важливо: екзаменаційна комісія, наукова рада хоче бачити, що дослідження зроблено не «як доведеться», а за чіткою схемою;
- Економія ресурсів: добре спланований дизайн допомагає уникнути зайвих кроків. Наприклад, якщо досить кореляційного аналізу, то не потрібно організовувати складний експеримент.

Таким чином, дизайн потрібен не для «паперової бюрократії», а для того, щоб процес виконання роботи був науково обґрунтованим, результат можна було перевірити, дослідження мало довіру й цінність.

Постановка та дизайн дослідження — це основа наукової діяльності, адже вони визначають логіку руху від ідеї до результату. Дослідження починається з усвідомлення проблеми (суперечності між потребами практики й можливостями наявних рішень) та її актуальності для науки і суспільства. Далі формулюються мета і завдання, які уточнюють, що саме дослідник прагне довести чи створити. Важливими є також об’єкт і предмет, які окреслюють сферу та фокус дослідження.

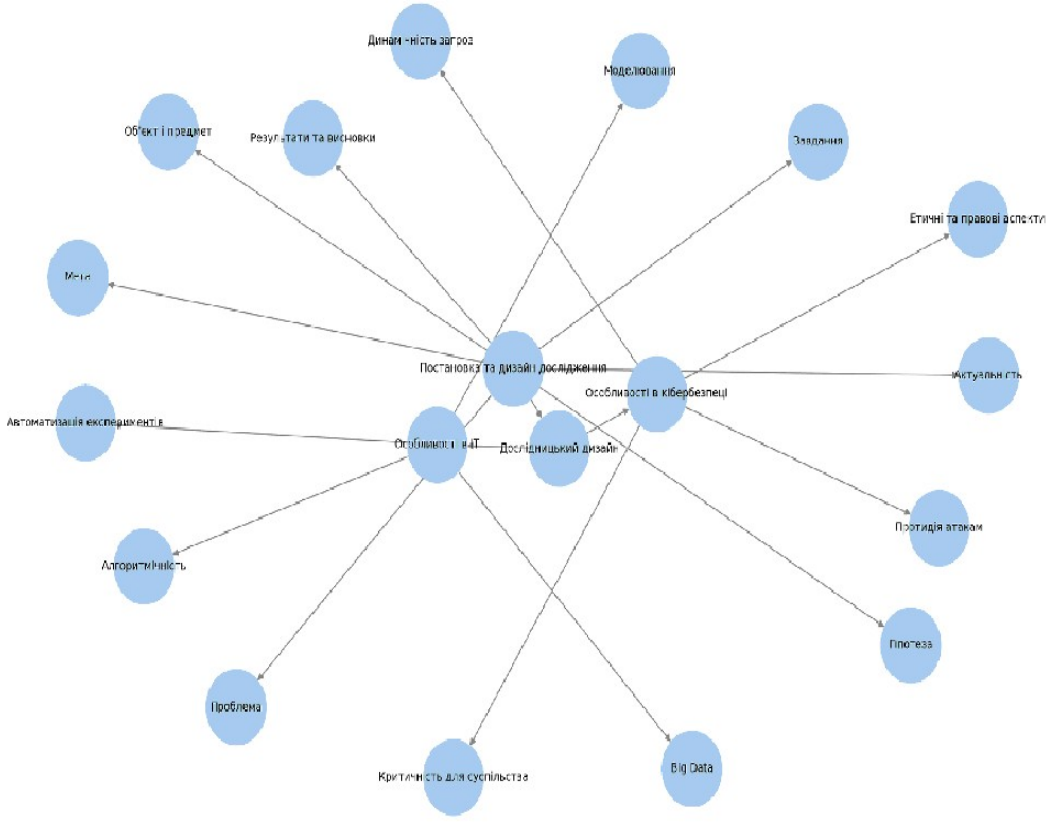

Рис.2.1. Постановка та дизайн дослідження (ІТ-галузь)

Дослідницький дизайн задає структуру дослідження, визначає типи даних, способи їх збору та аналізу. У класичній науці це може бути експериментальний, кореляційний, якісний чи змішаний підхід. В ІТ-галузі дизайн має унікальні риси: алгоритмічність, моделювання у віртуальних середовищах, автоматизація експериментів, робота з великими даними. У

кібербезпеці додаються ще й специфічні виміри: постійна протидія атакам, динамічність загроз, етичні й правові обмеження, критичність результатів для суспільства.

Отже, постановка та дизайн дослідження — це не формальність, а каркас наукової роботи, який гарантує її цілісність, логічність і відтворюваність (рис.2.1). Для ІТ та кібербезпеки вони мають особливе значення, адже саме тут швидкість змін, глобальний масштаб і наявність «активного супротивника» роблять правильне формулювання проблеми, мети та вибір дизайну не лише академічним завданням, а й фактором реальної безпеки суспільства.

Питання

1. Пояснити, що таке наукова проблема, навести приклади.
2. Пояснити, як визначається мета наукового дослідження. Як мета пов’язана з проблемою? Навести приклади.
3. Пояснити, що таке завдання дослідження? Як завдання пов’язані з метою? Навести приклади.
4. Об’єкт і предмет дослідження, їх зв'язок. Навести приклади.
5. Характерні риси для об’єкта і предмета дослідження в ІТ-галузі.
6. Унікальні риси предмета дослідження в кібербезпеці.
7. Пояснити, що таке висновки наукового дослідження. Характерні риси висновків.
8. Дослідницький дизайн: експериментальний, кореляційний, якісний, змішаний. Що забезпечує дослідницький дизайн?

Тема 3. МЕТОДИ ЗБОРУ ДАНИХ В ІТ-ДОСЛІДЖЕННЯХ

План

1. **Класифікація методів збору даних**
2. **Конфіденційність – фундаментальний принцип наукового дослідження**
3. **Загальний регламент про захист даних**
4. **Статистичний зсув**
5. **Помилкова класифікація**
6. **Методи збору даних в ІТ-дослідженнях у воєнний час**

1. Класифікація методів збору даних

Традиційні соціальні методи використовуються тоді, коли об'єктом дослідження є користувачі, їхня поведінка, досвід:

- Анкетування - масовий збір структурованої інформації від великої кількості користувачів, наприклад, опитування щодо безпечної поведінки в інтернеті;
- Інтерв'ю - глибоке розуміння мотивацій, бар'єрів, досвіду, наприклад, інтерв'ю з фахівцями SOC про практики реагування на інциденти;
- Фокус-групи - дискусії невеликих груп користувачів для виявлення ставлення до нових технологій, наприклад, оцінка сприйняття багатофакторної автентифікації серед працівників компанії

Технічні методи збору даних

- Логи систем - автоматичні записи подій (вхід у систему, мережеві з'єднання, спроби атаки). Використовуються для аналізу інцидентів та аномалій.
- Телеметрія - дані про роботу пристроїв/ПЗ, що передаються у реальному часі, наприклад, телеметрія від антивірусного програмного забезпечення.
- Метрики програмного забезпечення - час відгуку, кількість помилок, використання пам'яті тощо, наприклад: аналіз продуктивності веб-додатків під час навантаження.

Методи аналізу великих даних

- Інтелектуальний аналіз даних (Data Mining) - виявлення закономірностей у великих наборах даних. Наприклад, знаходження патернів у поведінці користувачів, що передує внутрішнім загрозам.
- Аналіз соціальних мереж - дослідження поширення інформації, виявлення ботів, інформаційних атак, наприклад, моніторинг Twitter для виявлення кампаній дезінформації.
- A/B тестування - експериментальний метод: порівняння двох варіантів системи для визначення ефективнішого, наприклад, тестування різних механізмів попередження користувачів про фішинг.

Зауважимо, що навіть маючи справу з ІТ-галуззю, зокрема кібербезпекою, нехтувати традиційними соціальними методами не можна. Дійсно, саме людина є найслабшою ланкою безпеки: 80% інцидентів у кібербезпеці пов'язані з людським фактором, наприклад, клік по фішинговому лінку, слабкий пароль, ігнорування політик. Звісно, технічні логи покажуть, що сталося, але тільки інтерв'ю чи анкета пояснить, чому так сталося. Наприклад: після атаки

з’ясовують, чому співробітники відкрили шкідливий файл. Виявляється, що попередження системи вони сприймають як «надокучливі» і ігнорують. Навіть найкраща система захисту буде марною, якщо користувачі не зможуть чи не захочуть нею користуватися. Соціальні методи дозволяють оцінити зручність, зрозумілість, доцільність прийняття нових рішень. Наприклад, тестування показує, що користувачі масово обходять складні політики паролів. З цього можна зробити висновок: потрібні альтернативи (MFA (багатофакторна автентифікація), біометрія). Анкетування та опитування допомагають оцінити рівень обізнаності працівників і сформувати навчальні програми. Наприклад, опитування показало, що 60% працівників не відрізняють фішинговий лист від справжнього. З цього приймається рішення про необхідність проведення тренінгу. Крім цього, інформаційні атаки, дезінформація, маніпуляції у соцмережах - це вже не лише технічні, а й соціальні явища, без соціальних методів неможливо зрозуміти, як вони впливають на людей, які наслідки матимуть.

Таким чином, традиційні соціальні методи в IT і зокрема кібербезпеці **потрібні** для вивчення людського фактора, оцінки зручності та прийнятності технологій, формування культури безпеки, аналізу соціальних інформаційних загроз. Тобто вони доповнюють технічні методи й показують, чому люди діють так, а не інакше.

Таким чином маємо, що не всі методи специфічні саме для IT. Унікальність IT у тому, що ця галузь має власні джерела даних (логи, телеметрія, метрики), які не існують у класичних галузях, а сила IT-досліджень полягає саме у поєднанні людського фактору (універсальні методи) та технічні (специфіка IT).

2. Конфіденційність – фундаментальний принцип наукового дослідження

Одним із ключових викликів сучасних IT-досліджень є питання ***конфіденційності*** даних. У науці загалом воно завжди мало значення, адже стосувалося етики поводження з інформацією про людей. Проте в IT і, особливо, у кібербезпеці, ця проблема набуває особливої гостроти.

Справа в тому, що більшість сучасних методів збору даних у цій сфері мають автоматизований характер. Системи генерують гігабайти логів, телеметрії, статистики про дії користувачів і пристроїв. І навіть коли дослідник збирає лише технічну інформацію, наприклад, IP-адреси чи журнали подій у мережі, у цих даних усе одно може бути прихована персональна або «чутлива» інформація.

Візьмемо простий приклад. При аналізі логів корпоративної мережі ми можемо дізнатися не тільки про підозрілу активність чи спроби атаки, а й про те, які сайти відвідували співробітники, з яких пристроїв вони заходили, у який час підключалися до системи. Якщо ці дані випадково потраплять у відкритий доступ, це вже буде серйозне порушення права на приватність.

У світі існують чіткі стандарти, які регулюють це питання. Найвідомішим є GDPR - Загальний регламент захисту даних у Європейському Союзі, що встановлює суворі правила зберігання й обробки персональної інформації. В Україні діє власний закон «Про захист персональних даних», адаптований до

європейських вимог. Для дослідника це означає одне: з даними треба працювати так, щоб жодним чином не нашкодити людині, чиї дані були зібрані.

Сучасна наука виробила кілька технік того, як це робити на практиці. Великим помічником тут є ***анонімізація,*** яка означає видалення будь-яких прямих ідентифікаторів: імен, адрес, номерів. ***Псевдонімізація*** замінює їх умовними позначеннями на кшталт «Користувач_123». Більш складні методи - це ***диференційна приватність***, коли в дані навмисно додають «шум», щоб неможливо було відновити інформацію про конкретну особу, та ***федеративне навчання***, коли алгоритми навчаються безпосередньо на пристроях користувачів, і «сирі» дані ніколи не залишають їхнього середовища. Ще одною важливою технікою тут є ***контроль доступу*** — дослідники отримують лише ті дані, які їм потрібні для конкретної задачі

Але головний виклик полягає в ***балансі***. Чим більше даних ми збираємо, тим точнішими можуть бути результати дослідження. Та водночас зростає ризик втручання в приватне життя. Саме тому завдання дослідника — не лише вміти збирати дані, а й розуміти, які з них дійсно потрібні, а які краще не торкати взагалі.

Таким чином, конфіденційність у методах збору даних в IT - це не другорядна деталь, а фундаментальний принцип, який визначає і етичність, і легальність наукового дослідження. І хоча не всі IT-дослідження пов’язані з приватною інформацією, є велика кількість завдань, де конфіденційність взагалі не є проблемою (аналіз алгоритмів (дослідження їхньої швидкодії, складності); тестування мережевих протоколів (моделювання віртуальних мереж у лабораторних умовах); вимірювання продуктивності програмного забезпечення, наприклад, як зміна алгоритму впливає на споживання пам’яті чи швидкість обчислень; робота з відкритими наборами даних тощо), конфіденційність все одно в IT-дослідженнях вважають фундаментальним принципом. Дійсно, не завжди можна наперед знати, які дані виявляться чутливими, лог може містити лише технічну інформацію, але при перехресному аналізі вона може «деанонімізувати» людину (наприклад, IP-адреса + час входу = конкретний співробітник); дослідження часто переходять у сферу взаємодії з людьми, наприклад, UX у кібербезпеці (User Experience in Cybersecurity - напрям, який вивчає зручність, зрозумілість і сприйняття користувачами систем захисту) чи аналіз соцмереж неминуче пов’язані з приватними даними. І нарешті - це питання довіри: навіть якщо дані не персональні, але дослідник нехтує конфіденційністю, суспільство й колеги можуть сумніватися у доброчесності його роботи.

3. Загальний регламент про захист даних

GDPR (General Data Protection Regulation) - це Загальний регламент про захист даних, який набув чинності в ЄС у 2018 році. Його головна ідея: кожна людина має право контролювати свої персональні дані: хто їх збирає, як їх обробляють, скільки зберігають і кому передають.

GDPR діє не тільки в межах ЄС: якщо компанія чи дослідник працює з даними громадян ЄС, він також підпадає під регламент, незалежно від країни.

GDPR викликом як для наукових дослідників, так і для бізнесу.

Так у наукових проєктах в ІТ та кібербезпеці часто використовуються дані користувачів: логи систем, телеметрія, поведінкові патерни. GDPR вимагає отримати згоду користувача на збір даних; мінімізувати обсяг зібраного (брати тільки те, що потрібно); забезпечити право на забуття (користувач може вимагати видалення своїх даних). Це звісно ускладнює проведення експериментів і збір інформації. Наприклад, якщо дослідник хоче проаналізувати трафік у корпоративній мережі, він повинен показати, що збирає лише ті дані, які дійсно потрібні для наукової мети, і що вони захищені. Якщо команда з України чи США працює з даними європейських користувачів, вона також зобов'язана дотримуватися GDPR. Це знову створює додаткові правові й організаційні бар'єри: від отримання дозволів до технічної адаптації інфраструктури.

Якщо розглянемо бізнес, то тут GDPR зобов'язує компанії прозоро пояснювати, які дані вони збирають і як використовують. За порушення передбачені величезні штрафи — до 20 млн євро або 4% річного обороту компанії. Для досліджень у великих ІТ-компаніях це означає додаткові витрати на аудит, анонімізацію даних, юридичний супровід.

Таким чином, GDPR - це виклик насамперед для дослідників і компаній в ІТ/кібербезпеці, які працюють із даними користувачів (табл.3.1): дані не можна збирати «про всяк випадок»; потрібні додаткові процедури захисту та анонімізації; є ризик серйозних юридичних наслідків у разі порушення. Тобто, з одного боку, GDPR захищає права людини; з іншого - ускладнює проведення досліджень і змушує розробляти нові методи збору даних.

Таблиця 3.1. Вимоги GDPR і наслідки для ІТ-досліджень

Вимога GDPR	Що це означає для ІТ-дослідника
Прозорість – користувач має знати, які дані збираються і для чого	Потрібно чітко формулювати мету збору даних у дослідженні, пояснювати учасникам, які дані будуть використані
Згода користувача	Не можна збирати дані без явної згоди; потрібні форми інформованої згоди або повідомлення
Мінімізація даних – збирати тільки те, що дійсно потрібно	Дослідник має визначити мінімальний набір даних для аналізу (наприклад, лог подій без імен користувачів)
Право на доступ і виправлення	Якщо учасник дослідження просить, дослідник має надати копію його даних або виправити помилки
Право на забуття (видалення)	Учасник може вимагати видалення своїх даних із дослідження чи бази
Захист даних	Необхідно використовувати шифрування, анонімізацію, контроль доступу
Повідомлення про витік	Якщо дані були скомпрометовані, дослідник чи організація повинні

	повідомити про це у встановлений термін
Передача даних за межі ЄС	Потрібні додаткові юридичні гарантії, якщо дані обробляються в Україні чи США, але стосуються громадян ЄС

GDPR — це не лише «бюрократія», а й стимул для дослідників розробляти нові, етичні та безпечні методи збору й обробки даних. Тому він і є викликом: одночасно обмеженням і поштовхом до інновацій.

Розглянемо приклад дослідження в кібербезпеці, яке довелося перебудувати через вимоги GDPR: дослідження логів у банку.

Група дослідників хотіла проаналізувати логи доступу до онлайн-банкінгу, щоб виявити аномалії поведінки: підозрілі входи з різних геолокацій, багаторазові спроби входу, нетипові години активності користувачів, метою чого було створити модель виявлення шахрайства. Під час роботи у них виникла проблема з GDPR: логи містили IP-адреси, геолокаційні дані, ідентифікатори клієнтів, час операцій, але ж все це - персональні дані. Згідно з GDPR, банк не міг просто передати їх дослідникам. З приводу цього дослідникам довелося: застосувати анонімізацію даних (замість реальних ідентифікаторів клієнтів кожному присвоїли псевдонім (User_001, User_002)); змінити масштаб геолокації (точні координати замінили на рівень «країна/регіон»); дослідники зобов'язалися видаляти дані користувача, якщо він цього вимагав; працювати з логами могли тільки окремі співробітники, які підписали угоди про конфіденційність.

В результаті, не дивлячись на додаткові труднощі, дослідникам вдалося побудувати модель аномалій навіть на знеособлених даних, хоча при цьому довелося витратити більше часу на юридичну та технічну підготовку. Як результат, дослідження стало етично і юридично безпечним та могло бути опубліковане у міжнародному журналі. Тобто GDPR - це не «гальмо для науки», а рамка, яка змушує шукати нові методи: працювати з анонімними даними, будувати синтетичні набори, використовувати федеративне навчання.

4. Статистичний зсув

Ще одним серйозним викликом для будь-яких досліджень у сфері IT і особливо в кібербезпеці є статистичний зсув (statistical shift, data shift, dataset shift).

Статистичний зсув — це ситуація, коли дані, на яких ми тренували або тестували систему, не збігаються з тими, що зустрічаються у реальному середовищі. У результаті метод чи модель працює добре в лабораторії, але погано в реальних умовах.

Прикладами статистичних зсувів можуть бути:

- Виявлення атак. Модель машинного навчання тренувалася на даних про фішингові листи 2022 року, а у 2025 з'явилися нові типи атак (наприклад, згенеровані штучним інтелектом). Модель не впізнає їх, бо «не бачила» таких прикладів;
- A/B тестування. Університет тестує інтерфейс MFA на молодих

студентах, а потім його впроваджують у держсекторі серед людей 50+. Результати зовсім інші, бо аудиторія має інші звички, навички, досвід роботи тощо;

- Кібербезпека банків України: банк тренував модель для виявлення шахрайських транзакцій на даних 2020–2021 років, але там були поширені класичні сценарії: крадіжка карткових даних, підроблені SMS тощо. У 2022–2023 роках різко зросла кількість атак із використанням DeepFake-дзвінків та шкідливих застосунків у Google Play, пов'язаних із війною (наприклад, «додатки для благодійності», які виявлялися шахрайськими). Модель, натренована на «старих» даних, майже не виявляла ці нові загрози.
- Виявлення фішингу в умовах війни. До 2022 року системи антифішингу в Україні були орієнтовані здебільшого на «банківський» фішинг (псевдосайти банків, Приват24), але під час повномасштабного вторгнення поширився новий тип атак: фішингові сайти, замасковані під державні портали (Дія, Пенсійний фонд, волонтерські ініціативи). Стара модель «не бачила» їх, бо у тренувальних наборах таких прикладів просто не було.
- Системи моніторингу кібератак у військовий час. До війни українські CERT-структури тренували системи виявлення на «типових» інцидентах: банківські трояни, DDoS-атаки. З 2022 року почали масово застосовуватися цільові атаки на енергетичну та урядову інфраструктуру. Алгоритми, які добре працювали на «мирних» даних, виявилися майже безсилими проти нових військово-орієнтованих загроз.

Статистичний зсув - це розрив між лабораторними даними й реальною практикою. У кібербезпеці він особливо небезпечний, оскільки система може створювати ілюзію захисту, але насправді пропускати нові типи атак. Тому сучасні дослідження спрямовані на те, щоб розробляти методи, стійкі до змін даних (наприклад, адаптивне навчання, регулярні оновлення датасетів).

Причини статистичного зсуву можна розбити на 2 групи:

1. Зовнішні (динаміка IT-середовища): дані змінюються з часом, виникають нові атаки, нові технології, інша поведінка користувачів. Модель, побудована «вчора», уже не підходить «сьогодні».
2. Внутрішні (помилки дослідника): дослідник використовує обмежену вибірку, наприклад, тренує алгоритм виявлення вторгнень лише на даних із Windows-систем, а потім застосовує його у середовищі з Linux. Вибірка була нерепрезентативною. У такому разі проблема не в швидкій динаміці IT, а в помилці планування експерименту.

Тому під час планування експерименту треба пам'ятати, що якість і репрезентативність вибірки - це основа наукової доброчесності й надійності результатів.

5. Помилкова класифікація

Одним із серйозних викликів під час збору й аналізу даних у сфері IT та кібербезпеки є помилкова класифікація. Це ситуація, коли система неправильно відносить об'єкт до певної категорії. Інакше кажучи, вона або бачить загрозу там, де її немає, або, навпаки, не помічає справжньої атаки.

У науковій літературі це поділяють на два типи: хибнопозитивні спрацьовування (False Positive) та хибнонегативні спрацьовування (False Negative) (табл.3.2). У першому випадку ми отримуємо «фальшиву тривогу», яка насправді виявляється нормальним явищем. У другому - пропускаємо подію, яка є реальною загрозою.

Розглянемо приклади. Антивірусна система може визначити звичайний додаток як шкідливий і заблокувати його. Це хибнопозитивна класифікація, яка шкодить довірі користувачів. З іншого боку, система виявлення вторгнень (IDS) може пропустити атаку, бо вона не схожа на ті, що система бачила раніше. Це хибнонегативна класифікація, яка створює ризик компрометації мережі. Аналогічна ситуація виникає і з фільтрами електронної пошти: легітимний лист від клієнта потрапляє у «спам», а фішинговий лист може пройти у «вхідні».

Чому це є викликом для дослідника? По-перше, у реальних даних завжди є шум і неоднозначність. Деякі приклади важко класифікувати навіть людині, не кажучи вже про алгоритм. По-друге, завжди існує компроміс між кількістю хибнопозитивних і хибнонегативних результатів. Якщо ми зробимо систему занадто чутливою, вона буде «кричати» надто часто, генеруючи сотні фальшивих тривог. Якщо ж зробимо її поблажливою, вона стане «сліпою» до реальних атак.

Завдання дослідника полягає у пошуку оптимального балансу. Це означає не тільки зібрати й обробити дані, а й правильно налаштувати чутливість алгоритму, обрати відповідні метрики оцінки (наприклад, precision, recall, F1-score) і вміти інтерпретувати помилки. І найголовніше: пам’ятати, що йдеться не лише про технічні характеристики, а й про довіру користувачів до всієї системи безпеки.

Отже, помилкова класифікація - це виклик, який змушує науковця мислити ширше. Це не тільки проблема алгоритму, а й питання методології: які дані ми зібрали, як ми їх позначили, чи достатньо вони репрезентативні. У сфері кібербезпеки правильне розуміння та мінімізація помилкової класифікації визначають не лише успіх дослідження, а й безпеку інформаційних систем загалом.

Таблиця 3.2. Наслідки FP і FN у класифікації

Тип помилки	Що це означає	Приклад у кібербезпеці	Можливі наслідки
False Positive (хибнопозитивне спрацювання)	Система бачить «загрозу» там, де її немає	Антивірус блокує легальну програму; фільтр спаму відправляє діловий лист у «спам»	- Втрата довіри до системи - Даремні витрати часу на перевірку - Зниження продуктивності роботи
False Negative (хибнонегативне спрацювання)	Система не бачить реальної загрози	IDS не помічає атаку; антифішингова система пропускає шкідливий лист	- Пропуск реальної атаки - Компрометація системи - Фінансові та

			репутаційні втрати

Таким чином, методи збору даних у IT-дослідженнях охоплюють як традиційні підходи (анкетування, інтерв'ю, фокус-групи), так і специфічні інструменти цифрової епохи - журнали подій, телеметрію, метрики програмного забезпечення, аналіз соціальних мереж. Саме комбінація цих методів дозволяє отримати глибше й точніше розуміння досліджуваних процесів. Разом із цим, IT-дослідники стикаються з низкою викликів: питання конфіденційності та необхідність дотримання нормативів на кшталт GDPR; ризик статистичного зсуву, коли дані тренування не відповідають реальним умовам; проблема помилкової класифікації, яка впливає на довіру до систем; складність у забезпеченні репрезентативності вибірки.

Унікальність IT-досліджень полягає в тому, що тут збір даних майже завжди автоматизований, а результати можуть бути відтворені іншими дослідниками завдяки логам, скриптам і відкритим наборам даних. Це робить IT однією з найдинамічніших і найточніших сфер наукової діяльності, але одночасно накладає високі вимоги до етики, якості даних та правильного експериментального дизайну.

6. Методи збору даних в IT-дослідженнях у воєнний час

Війна суттєво змінила характер IT-досліджень в Україні, і це особливо відчутно у сфері збору даних. Якщо раніше акценти робилися переважно на класичних кіберзагрозах — фішинг, банківське шахрайство, DDoS-атаки, то тепер у центрі уваги опинилися реальні кібератаки на критичну інфраструктуру: енергетичні об'єкти, державні органи, військові системи. Збір даних дедалі більше базується на аналізі кіберінцидентів, які фіксують національні та корпоративні центри реагування, а також волонтерські спільноти на кшталт «IT-армії».

Дослідники почали значно активніше використовувати відкриті джерела - соціальні мережі, телеграм-канали, форуми даркнету. Такі дані допомагають відстежувати поширення дезінформації, виявляти фішингові кампанії чи навіть механізми вербування «кібервійськ». Це новий пласт джерел, який раніше рідше розглядався в академічних дослідженнях. Тут може виникнути сумнів: соціальні мережі, телеграм-канали чи даркнет-форуми - це радше поле діяльності журналістів-розслідувачів чи спецслужб, а не науковців. Але ці джерела мають безпосереднє відношення до наукових досліджень в IT, особливо в умовах війни та кіберзагроз. У соціальних мережах і месенджерах зосереджені масиви даних, які можна аналізувати автоматизованими методами: від збору повідомлень і статистики поширення до виявлення ботів та інформаційних операцій. Для дослідника це унікальне «живе середовище» для застосування алгоритмів машинного навчання, NLP (обробка природної мови), графового аналізу. Форуми даркнету - джерело інформації про нові шкідливі програми, способи атак, продаж баз даних. Telegram-канали - місце, де можуть координуватися фішингові кампанії чи DDoS-атаки. Для науковця це означає можливість збирати унікальні датасети й аналізувати нові типи загроз, які ще не

описані в літературі чи стандартних базах. Кібербезпека і цифрова трансформація давно перестали бути «чисто технічними». Тут важливий людський фактор: як користувачі реагують на дезінформацію, як відбувається вербування в кібервійська, як формуються спільноти хакерів. Це вже сфера міждисциплінарних досліджень на перетині ІТ, соціології та психології. Наукові результати таких досліджень – це побудова моделей поширення дезінформації; створення алгоритмів для виявлення бот-мереж; аналіз ефективності захисних повідомлень у соцмережах; розробка нових методів OSINT-аналізу. Це не просто «розслідування», а саме систематизація та генералізація знань у вигляді моделей, алгоритмів і рекомендацій, які потім можна перевіряти, відтворювати та впроваджувати.

Таким чином, використання соціальних мереж, телеграм-каналів і даркнет-форумів у наукових ІТ-дослідженнях — це не сенсаційне «полювання на факти», а спосіб отримати нові емпіричні дані, на основі яких створюються алгоритми, системи аналізу й наукові узагальнення. Це особливо важливо для України сьогодні, де кіберпростір став ще одним фронтом війни.

Паралельно зросло значення етики. У воєнний час будь-яке ненавмисне розкриття приватної інформації може становити реальну загрозу для людини чи організації. Саме тому на перший план вийшли методи анонімізації та синтетичні набори даних, які дають змогу досліджувати безпеку, не ризикуючи конкретними людьми.

Змінилося й географічне походження даних. Українські дослідники отримали значно ширший доступ до глобальних баз зразків шкідливого коду та індикаторів атак, які надають міжнародні партнери з ЄС і НАТО. Це дозволяє аналізувати не лише локальні загрози, а й бачити їх у глобальному контексті.

З’явилися й нові технічні інструменти. Зокрема, активніше застосовуються honeypots — спеціальні системи-пастки, які імітують уразливі сервери й дають змогу збирати зразки реальних атак у «дикій природі». Використовується й телеметрія з мобільних застосунків, у тому числі тих, що безпосередньо пов’язані з війною та волонтерством.

Яскравим прикладом є дослідження фішингу. Якщо до війни воно зосереджувалося переважно на підроблених банківських сайтах, то тепер головним об’єктом аналізу стали фейкові версії державних сервісів — «Дії», порталу Пенсійного фонду, а також шахрайські сайти з нібито благодійними зборами. Це означає, що дослідники вимушені застосовувати нові методи збору даних: моніторинг фейкових доменів, відстеження телеграм-ботів, аналіз даркнет-форумів.

Отже, методи збору даних в українських ІТ-дослідженнях у воєнний час стали більш орієнтованими на реальні атаки, більш розосередженими за джерелами, значно чутливішими до питань етики й безпеки, а також більш міжнародними завдяки партнерству. Це зробило їх не лише прикладними, а й стратегічно важливими для національної безпеки та кіберстійкості держави.

Питання

1. Конфіденційність як фундаментальний принцип наукового дослідження. Анонімізація, псевдонімізація, диференційна приватність, федеративне

навчання, контроль доступу.
2. Загальний регламент про захист даних.
3. Поняття статистичного зсуву. Причини та приклади статистичного зсуву.
4. Поняття помилкової класифікації.
5. Специфіка методів збору даних в ІТ-дослідженнях у воєнний час.

Тема 4. МІЖДИСЦИПЛІНАРНІСТЬ ЯК МЕТОДОЛОГІЧНИЙ ВИКЛИК В ІТ-ДОСЛІДЖЕННЯХ

План

1. **Міждисциплінарність в ІТ як умова наукової валідності сучасних досліджень**
2. **Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: розширення об'єкта ІТ-досліджень**
3. **Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: проблема різних стандартів доказовості**
4. **Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: новизна на стику**
5. **Проблема даних різної природи**

1. Міждисциплінарність в ІТ як умова наукової валідності сучасних досліджень

Сучасні наукові дослідження в ІТ давно вийшли за межі «чистої інформатики». Якщо ще кілька десятиліть тому ІТ розглядалися переважно як сфера алгоритмів, обчислень і програмування, то сьогодні вони стали універсальним інструментом науки, який проникає в біологію, медицину, економіку, психологію, соціологію і навіть гуманітарні науки.

Але таке розширення породжує нові методологічні виклики.

Дослідник в ІТ уже не може обмежитися тільки кодом, експериментом чи симуляцією. Йому доводиться працювати з різними типами даних (числовими, текстовими, поведінковими), комбінувати різні методи (машинне навчання, соціологічні опитування, когнітивні експерименти), співставляти різні стандарти доказовості (наприклад, точність алгоритму та статистичну значущість у соціальних науках).

Тут виникає ключове методологічне питання: ***як поєднати різні підходи так, щоб отримати не хаотичний набір фактів, а справжнє наукове знання? Як комбінувати різні типи знань і методів у межах одного дослідження?***

Міждисциплінарність в ІТ — це не просто модний тренд. Це умова наукової валідності сучасних досліджень, адже більшість реальних проблем — кібербезпека, захист даних, медицина майбутнього, цифрова економіка — знаходяться на стику кількох наук. Саме тому ми сьогодні розглянемо міждисциплінарність не як абстракцію, а як методологічний інструмент і виклик для ІТ-дослідників.

2. Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: розширення об'єкта ІТ-досліджень

ІТ сьогодні - це не ізольована сфера, а універсальний інструмент для інших наук. Але тоді виникає питання: як це впливає на методологію дослідження?

Щоб відповісти, ми розглянемо кілька ситуацій, у яких чисто ІТ-підходи виявляються недостатніми.

У кожному випадку ми подивимося:

- Проблема - що не спрацьовує, якщо брати тільки технічні методи;
- Приклад - реальна ситуація з кібербезпеки чи іншої ІТ-сфери;
- Методологічний висновок - які підходи потрібно додати, як узгодити різні дисципліни, що це означає для дослідника.

Ситуація 1. Антифішинг

Проблема: алгоритми машинного навчання здатні з високою точністю виявляти фішингові листи та підроблені сайти. Проте на практиці атаки все одно успішні. Чому? Тому що користувач не завжди поводиться раціонально: клікає на підозріле посилання, вводить пароль у сумнівній формі, ігнорує попередження системи. Отже, чисто технічні рішення тут не гарантують безпеки, якщо не врахувати поведінковий фактор.

Приклад: в Україні під час війни з'явилися десятки фішингових сайтів, які маскувалися під державний портал «Дія» або під волонтерські ініціативи. Алгоритмічні системи досить швидко навчились їх виявляти. Але користувачі все одно залишали свої дані, тому що довіряли бренду «Дія», не перевіряли URL або поспішали зробити «благодійний внесок». Технічна система вчасно сигналізувала, але людський фактор зруйнував захист.

Методологічний висновок: це показує, що в дослідженнях кібербезпеки ***об'єкт*** не обмежується лише процесом виявлення. Він включає і поведінку користувачів, а методологія досліджень тут має бути міждисциплінарною: технічні методи аналізу даних + психологічні методи вивчення довіри, когнітивних упереджень і сприйняття ризику. Тільки поєднання цих підходів дає валідні результати та справді ефективні системи захисту.

Ситуація 2. Медична інформатика (ІТ + медицина).

Проблема: у медицині накопичуються величезні обсяги даних - результати аналізів, зображення МРТ, історії хвороб. Лікар не може самостійно швидко опрацювати такий обсяг інформації. Алгоритми ШІ допомагають автоматизувати діагностику, але медична сфера має свої особливості: будь-яке рішення повинно бути клінічно обґрунтованим і підкріпленим доказовою медициною. Чисто «математична точність» алгоритму недостатня.

Приклад: система штучного інтелекту для діагностики раку легенів може показати 95% точності на тестових даних, але для реального використання цього замало - потрібно врахувати, як лікар буде інтерпретувати результати, чи не буде «хибнопозитивних» діагнозів, як пацієнт сприйме рекомендацію машини. Тобто тут перетинаються не лише ІТ та медицина, а й психологія пацієнта.

Методологічний висновок: дослідник в ІТ не може обмежитись метриками точності. Методологія має включати й медичні стандарти валідації (клінічні випробування, контрольні групи), і етичні аспекти. Це типова міждисциплінарність: технічні методи обчислень + методологія доказової медицини + етика.

Ситуація 3. Дезінформація в соцмережах (ІТ + соціологія)

Проблема: системи автоматичного аналізу текстів добре знаходять фейки чи маніпулятивні повідомлення, але цього замало: дослідникам потрібно зрозуміти як і чому ці повідомлення поширюються, чому вони впливають на людей. Алгоритми бачать контент, але не пояснюють соціальну поведінку.

Приклад: під час війни в Україні масово поширювалися фейки через Telegram-канали («Київ оточений», «система ППО не працює»). Технічно можна було виявити схожі формулювання та джерела, але чому частина користувачів миттєво повірила й поширила ці повідомлення? Це пояснюють закони соціальної психології: довіра до «своїх», поширення паніки, ефект «інформаційного вакууму».

Методологічний висновок: аналіз дезінформації неможливий лише з ІТ-позицій. Потрібна методологія соціальних наук: теорія масових комунікацій, аналіз довіри в суспільстві, дослідження поведінки у кризових ситуаціях. Це означає, що наукова новизна тут народжується на стику ІТ-алгоритмів (NLP, класифікація) і соціологічних моделей.

Таким чином, очевидним стає висновок, що методологія в ІТ-дослідженнях повинна передбачати комбінування дисциплін.

Міждисциплінарність в ІТ-дослідженнях — це не данина моді і не красиве слово, а методологічна необхідність. Сучасні наукові проблеми занадто складні, щоб їх можна було вирішити лише алгоритмами чи експериментами з даними.

Ми побачили на прикладах: у кібербезпеці технічні антифішинг-системи неефективні без розуміння психології користувача. У медичній інформатиці алгоритмічна точність недостатня без клінічних стандартів та етичної оцінки. У боротьбі з дезінформацією автоматичний аналіз текстів дає лише частину відповіді, решту пояснює соціологія та психологія масової поведінки.

Ці приклади показують: **об'єкт ІТ-досліджень розширюється** - він включає технічні системи, людей, суспільство, а іноді навіть біологічні процеси. Відповідно, і методологія має змінюватися: замість ізольованих підходів ми комбінуємо методи з різних наук, узгоджуємо різні стандарти доказовості й шукаємо новизну саме на стику.

3. Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: проблема різних стандартів доказовості

У різних науках «наукова достовірність» означає різні речі.

Так в ІТ достатньо показати, що алгоритм дає, скажімо, 95% точності на стандартному датасеті, і інший дослідник отримав такий самий результат на тих самих даних.

У психології чи соціології одного експерименту недостатньо. Треба мати вибірку респондентів, статистично значущі результати, контрольні та експериментальні групи, врахування культурних, когнітивних і соціальних чинників.

У медицині взагалі золотим стандартом є клінічні випробування на кількох етапах, де бере участь сотні чи тисячі пацієнтів.

І коли ІТ-дослідник заходить у міждисциплінарну сферу, виникає методологічний конфлікт: результат, який в ІТ вважається «достатньо доказовим», для іншої науки може виглядати як «сирий експеримент».

Приклад: уявімо, що ви створили систему для виявлення фішингових листів. В ІТ-дослідженні достатньо показати метрики (precision, recall, F1-score) на датасеті. Але якщо ви хочете опублікувати цю роботу в журналі з поведінкової психології, редактор спитає: «А як користувачі реагували на повідомлення?», «Чи є контрольна група, яка бачила інші варіанти?», «Який

розмір вибірки? Чи можна узагальнити ці результати на ширшу популяцію?». І тоді ІТ-шнику доведеться додати експеримент з людьми, зібрати статистику, підтвердити значущість.

Методологічний висновок: у міждисциплінарних ІТ-дослідженнях не можна обмежуватися лише «своїми» стандартами доказовості. Тут методологічно правильно буде наступне: враховувати стандарти суміжної науки (психології, медицини, соціології тощо), поєднувати різні типи валідації: технічні метрики (точність, швидкодія), емпірична перевірка на людях, статистична значущість.

Отже, головний виклик тут - узгодження «різних мов» науки. Для ІТ-шника цифри precision/recall - переконливий аргумент. Для психолога чи лікаря цього недостатньо: потрібні контрольні групи, етика, статистика. А на стику дисциплін треба навчитися «перекладати» свої результати мовою іншої науки.

Розглянемо ще декілька прикладів, де різні стандарти доказовості зіткнулися безпосередньо.

Ситуація 1. Фішинг та поведінкова психологія

ІТ-результат: система машинного навчання показала 97% точності на датасеті з фішингових листів.

Проблема: на практиці користувачі продовжували відкривати небезпечні листи.

Стандарти доказовості психології: потрібні були експерименти з реальними людьми: як вони реагують на повідомлення різних типів, які когнітивні упередження впливають (довіра до бренду, поспіх, емоційний стан).

Методологічний висновок: метрики алгоритму потрібно доповнити експериментальними даними про поведінку користувачів, щоб дослідження було науково коректним і практично цінним.

Ситуація 2. Паролі та когнітивні науки

ІТ-результат: аналітики довели, що складніші політики паролів (довгі, з символами) зменшують ймовірність зламу brute-force.

Проблема: користувачі почали масово записувати паролі на стікерах чи повторно використовувати ті самі комбінації.

Стандарти доказовості когнітивних наук: потрібні експерименти з пам’яттю, навантаженням на когнітивні ресурси, usability-тести.

Методологічний висновок: ефективність паролів потрібно оцінювати не лише за стійкістю алгоритмів, а й за здатністю користувача їх реально запам’ятати та використовувати.

Ситуація 3. A/B тестування в безпеці

ІТ-результат: впроваджено нове попередження у браузері, яке зменшило кількість кліків на небезпечні сайти на 20%.

Проблема: результати залежали від країни та вікової групи користувачів.

Стандарти доказовості соціальних наук: потрібно врахувати культурні відмінності, сегментацію аудиторії, статистичну значущість ефекту.

Методологічний висновок: навіть при високій ефективності «в середньому» дослідник має довести, що ефект стійкий для різних груп користувачів, або чітко обмежити межі застосовності.

У всіх цих випадках - одна закономірність: ІТ-метрики важливі, але недостатні. Щоб дослідження було справді науковим і мало практичну цінність, потрібно додавати стандарти суміжних наук - психології, соціології, медицини.

Таким чином, у традиційних ІТ-дослідженнях доказовість часто зводиться до точності алгоритму чи продуктивності системи на тестових даних, але в міждисциплінарних сферах цього замало. **Якщо в центрі дослідження з'являється людина, суспільство чи біологічний процес, потрібно враховувати стандарти суміжних наук:** статистичну значущість у психології, репрезентативність вибірки у соціології, клінічні випробування в медицині. Це створює методологічний виклик: як поєднати різні критерії достовірності так, щоб результат визнавали і в ІТ-спільноті, і в суміжних науках? Відповідь полягає у подвійній перевірці: технічні метрики гарантують коректність алгоритму, стандарти інших дисциплін - валідність для реального світу. Таким чином, міждисциплінарність в ІТ-дослідженнях - це не лише питання новизни, а й питання доказової культури. Справжній науковий результат з'являється лише тоді, коли ми здатні говорити мовою кількох наук одночасно, узгоджуючи їхні вимоги до достовірності.

4. Міждисциплінарність в ІТ-дослідженнях як методологічна необхідність: новизна на стику

Міждисциплінарні дослідження завжди стикаються з підозрою, що там «нічого нового нема», а просто одна наука запозичила ідею в іншої. У класичному ІТ-дослідженні новизна зрозуміла: новий метод, нова архітектура, нова метрика, але якщо ми поєднуємо ІТ з психологією, медициною чи соціологією, виникає питання: це справжня новизна, чи просто застосування відомого методу з однієї сфери до іншої? Розглянемо приклад.

Приклад. Кібербезпека + когнітивні науки

Дослідження соціальної інженерії спершу зводилися до опису прийомів шахраїв. Коли сюди додали когнітивну психологію (ефект авторитету, поспіху, інформаційного перевантаження), почали будуватися моделі «людської вразливості». А це вже не просто «застосування психології», а створення нової рамки аналізу кіберзагроз.

Методологічний критерій новизни. Щоб показати, що результат є новим науковим внеском, а не лише «запозиченням», дослідник повинен:

- Показати, що поєднання дисциплін дало якісно новий метод чи модель, яких раніше не існувало, наприклад, не просто «алгоритм у медицині», а алгоритм, який змінює підхід до діагностики;
- Вказати, яку наукову проблему вдалося вирішити, яка була невирішуваною в межах лише однієї дисципліни, наприклад, ІТ не могли пояснити, чому користувач клікає на фішинг, а психологія не могла моделювати атаки. Разом це стало можливим;
- Окреслити внесок кожної дисципліни й показати «надлишок» - що виникло на стику, чого не дала б жодна окремо.

Таким чином, тут методологічно важливо розуміти: новизна на стику наук з'являється тоді, коли комбінація дає нову якість - новий метод, нову модель, нову теорію, нове розуміння. Не достатньо просто «застосувати ІТ до іншої

сфери». Справжня наука починається тоді, коли це застосування змінює сам спосіб постановки проблеми і відкриває новий простір для досліджень.

5. Проблема даних різної природи

У «чистому» ІТ-дослідженні об’єкт зазвичай однорідний: це алгоритм, програмна система, набір логів або даних з певного домену. У міждисциплінарних дослідженнях з’являється кілька типів даних одночасно: технічні (логи, трафік, телеметрія), соціальні (поведінка користувачів, повідомлення в соцмережах), когнітивні (результати тестів, реакції, час відгуку), біологічні чи медичні (біосигнали, результати аналізів). Що це означає методологічно? Маємо декілька складових:

- Розширення об’єкта дослідження: дослідник фактично визнає, що об’єкт уже не обмежується «системою» чи «алгоритмом», про що говорилося вище;
- Проблема інтеграції даних: як поєднати числа з логів, текстові повідомлення й поведінкові спостереження? Кожен тип даних вимагає різних інструментів аналізу (статистика, NLP, когнітивні тести);
- Проблема валідності: дані з різних джерел можуть мати різний рівень надійності. Логи з системи - точні, а відповіді в анкеті можуть бути суб’єктивними. Методологічно дослідник має пояснити, чому поєднання цих даних дає валідний результат.

Таким чином, проблема «даних різної природи» - це і про розширення об’єкта дослідження (він виходить за межі чисто технічного), і про методологію обробки та валідації. Ключове завдання дослідника тут - показати, що різнорідні дані не просто «зібрані в одну купу», а узгоджені між собою так, щоб дати науково обґрунтований результат.

Приклад: дослідження кампаній фішингу під час війни в Україні

Об’єкт дослідження: не лише «алгоритм виявлення листів», а комплекс взаємодії технічних систем, користувачів і середовища поширення атак.

Дані різної природи:

- Технічні дані (логи поштових серверів (IP-адреси відправників, домени, кількість підозрілих листів)), аналіз вкладень (шкідливий код, посилання);
- Соціальні дані (пости й повідомлення у соцмережах, де зловмисники поширювали ті ж посилання, що й у листах); Telegram-канали з закликами «заповнити форму для допомоги переселенцям»;
- Поведінкові дані (експерименти з користувачами: як вони реагують на листи з «правдоподібними» назвами («Допомога від Міноборони», «Волонтерський фонд»)); опитування про довіру до різних джерел інформації.

Методологічний виклик: об’єднати «жорсткі» технічні дані (логи, код) із «м’якими» соціальними й поведінковими. Як уникнути того, що суб’єктивні опитування «розмиють» надійність результатів?

Вирішення

Поєднання відбулося через багаторівневу модель аналізу атаки:

- Технічний рівень: логи показали вектори розсилки (звідки надходять

листи, які домени використовуються).

- Соціальний рівень: ті ж самі домени виявилися присутніми у Telegram-каналах, що дозволило з'єднати «поштові атаки» і «соціальне поширення» в одну кампанію.
- Поведінковий рівень: експерименти підтвердили, що користувачі натискають на ті домени/посилання, які вже зустрічали у соцмережах (фактор довіри й впізнаваності).

Отже, поєднання даних різної природи дозволило побудувати ***єдину картину***: технічні атаки не були ізольовані, вони підкріплювалися соціальними механізмами, а вразливість користувачів пояснювалася когнітивними чинниками.

Отримані результати мають значення як для наукового дослідження: можна показати, що фішинг - це не лише технічна проблема, а багаторівневий феномен, який вимагає інтегрованої моделі, так і для практики: результати підказують, що протидія має включати не лише фільтри листів, а й інформаційні кампанії в соцмережах та навчання користувачів.

Таким чином, міждисциплінарність в ІТ-дослідженнях - це не просто «модно» чи «ширше бачення». Це методологічна необхідність, бо сучасні проблеми кібербезпеки, медицини, соціальних систем не можна вирішити лише технічними засобами. Для ІТ-дослідника це означає: навчитися працювати з даними різної природи, комбінувати методи, обґрунтовувати новизну саме на стику наук, інакше формулювати предмет та гіпотези дослідження.

Питання

1. Розширення об'єкта ІТ-досліджень внаслідок їх міждисциплінарності.
2. Проблема різних стандартів доказовості в ІТ-дослідженнях.
3. Наукова новизна в міждисциплінарних дослідженнях. Методологічний критерій новизни.
4. Проблема даних різної природи в міждисциплінарних дослідженнях.

Тема 5. НАУКОВА КОМУНІКАЦІЯ ТА КУЛЬТУРА ПУБЛІКАЦІЙ

План

1. **Комунікація як невід'ємна частина наукового процесу**
2. **Наука як діалог і як колективна діяльність**
3. **Форми наукової комунікації**
4. **Культура публікацій**
5. **Виклики для наукової комунікації та культури публікацій**

1. Комунікація як невід'ємна частина наукового процесу

Наукове дослідження ніколи не існує у вакуумі. Його сенс полягає не лише у відкритті нового знання, а й у передачі цього знання іншим - колегам, науковій спільноті, суспільству. Наука за своєю суттю є колективною діяльністю, а отже, комунікація є такою ж фундаментальною частиною дослідження, як і експеримент чи аналіз даних.

Без комунікації відкриття залишилося б лише у межах робочого зошита чи коду на комп'ютері, не вплинуло б на розвиток науки й не стало б підґрунтям для нових ідей. Саме тому ще з часів перших академічних журналів у XVII столітті науковці зрозуміли: результат має бути опублікований і обговорений.

У сучасному світі роль комунікації лише зростає. Нові відкриття в IT і кібербезпеці з'являються щотижня, і якщо вони не донесені до спільноти через статті, конференції чи відкриті репозиторії, вони швидко втрачають актуальність.

Наукова комунікація забезпечує:

- перевірку результатів,
- накопичення знань у базах даних і журналах,
- створення наукових шкіл і спільнот,
- практичне впровадження ідей у технологіях.

Таким чином, комунікація - це не «додаткова опція», а умова самого існування науки. Якщо результат не був переданий іншим, він не став частиною наукового знання.

Розглянемо дуже яскравий приклад, що підтверджує вищенаведене. У 2017 році світ сколихнула атака вірусу-здирника WannaCry, яка вразила сотні тисяч комп'ютерів у більш ніж 150 країнах. Технічні деталі уразливості, яку використав вірус (експлойт EternalBlue), були відомі дослідникам задовго до цього. Але вони залишалися у вузькому колі спеціалістів, без широкої публікації та обговорення у відкритій науковій і професійній спільноті. Причина цього лежать у площині культури наукової та професійної комунікації:

- Закритість розвідданих: EternalBlue був інструментом, який розробило Агентство національної безпеки США (NSA). Такі експлойти належать до категорії «cyber weapons» — кібервійськової зброї. За своєю природою вони не публікуються, а зберігаються у таємниці для використання у розвідці й операціях.
- Відсутність прозорої комунікації між спецслужбами та науковою

спільнотою: університети та незалежні дослідники часто дізнаються про такі уразливості вже «заднім числом», після витоків чи атак. Тут бракує наукової комунікації: дані були відомі, але не передані ні в якому (хоча б дуже обмеженому вигляді) для аналізу й обговорення.

- Ризики публікації: навіть якщо дослідник поза спецслужбами знаходить подібну уразливість, виникає дилема - опублікувати й дати шанс на виправлення (але тоді хакери одразу скористаються знанням) або утримати від публікації (але тоді суспільство залишається вразливим).
- Хижацький сценарій витоку: EternalBlue зрештою став відомим через витік групи Shadow Brokers. Це означає, що знання, яке зберігалося у «закритій науковій і розвідувальній екосистемі», раптово потрапило у відкрите (але неконтрольоване) середовище.

Лише після масового зараження почали з'являтися десятки статей, блогів, конференційних доповідей, де в деталях пояснювали механізм атаки й шляхи захисту. Саме завдяки такій науковій та професійній комунікації з'явилися оновлення безпеки, аналітика поведінки вірусу, а в результаті - колективне розуміння загрози.

Цей приклад добре показує: навіть найкраще технічне знання залишається «мертвим капіталом», якщо воно не комунікується. Тільки через публікації, конференції та обговорення в спільноті наукова ідея стає дієвою, перевіряється іншими й трансформується в реальний захист.

Цей приклад показує, що недостатність або затримка наукової комунікації може мати катастрофічні наслідки. Знання, яке залишається у «вузькому колі», не дає можливості підготуватися, випустити оновлення й захистити системи.

Але цей приклад ще демонструє дуже значну сучасну проблему: як знайти баланс між відкритістю (щоб виправити проблему) і обмеженням інформації (щоб її не використали зловмисники)? Не існує і не може існувати повної відкритості у сфері кібербезпеки. Якщо б усі «кіберзброї» одразу публікувалися, це створювало б загрози для мільйонів користувачів. Тому частина знань закономірно залишається секретною. Саме тут і з'являється методологічний і етичний виклик для науки та індустрії:

1. Чи може наука бути повністю закритою?

Якщо знання існує лише у «закритому колі спецслужб», воно не виконує повною мірою функцій наукового знання - перевіреність, відтворюваність, використовуваність. Воно перетворюється на «секретний інструмент».

2. ***Безпека не передбачає повної відкритості***.

Публікація уразливості без патчів і контрзаходів зробить світ більш вразливим. Саме це сталося з EternalBlue після витоку: хакери отримали готовий експлойт, і світ побачив WannaCry.

3. Між ними — практика «координованого розкриття» (responsible disclosure), що вже використовується в кібербезпеці:

- дослідник повідомляє про уразливість виробника;
- виробник випускає оновлення/патч;
- після цього публікується наукова стаття або технічний звіт.

Таким чином, наукова комунікація можлива і необхідна, але у контрольованій формі. Вона не розкриває «сирі експлойти», але пояснює механізми атаки, моделі захисту, методологію аналізу.

Таким чином, у сфері кібербезпеки існують речі, які не можна комунікувати прямо. Але це не означає, що наука має мовчати. Навпаки: тут формується ***особлива культура комунікації***, де дослідник має балансувати між науковою відкритістю і практичною безпекою. Саме такий позитивний досвід (з використанням пункту 3 (responsible disclosure)) розглянемо далі: своєчасна комунікація в IT-дослідженнях врятувала від масштабних проблем.

У 2018 році команда дослідників з Google Project Zero виявила критичні уразливості процесорів Meltdown і Spectre, які дозволяли зловмисникам отримати доступ до даних із пам'яті комп'ютера. Замість негайної публікації, яка могла б призвести до масових атак, було організовано координоване розкриття вразливостей: дослідники, як і передбачено responsible disclosure повідомили виробників процесорів і розробників ОС, разом із ними підготували оновлення безпеки та патчі і лише після цього опублікували статті та технічні звіти, пояснивши принцип атаки. Завдяки такій грамотній комунікації вдалося уникнути катастрофи: користувачі отримали захист ще до того, як зловмисники почали активно експлуатувати уразливість.

Цей випадок показує, що якість і форма комунікації у науці та кібербезпеці можуть прямо впливати на глобальну безпеку. Тут наукова публікація стала не лише формальним звітом, а й інструментом захисту мільйонів користувачів.

2. Наука як діалог і як колективна діяльність

Наука від самого початку формувалася не як справа одинаків, а як простір колективного пошуку істини. Жодне відкриття не виникає на порожньому місці: воно завжди пов'язане з попередніми дослідженнями, перебуває в дискусії із сучасними підходами і водночас створює ґрунт для майбутніх пошуків. Тому можна сказати, що наука існує у формі діалогу. Це діалог із минулим, коли ми спираємося на накопичені знання і враховуємо зроблені помилки. Це діалог із сучасниками, який відбувається у публікаціях, рецензіях, наукових конференціях, де відбувається обмін думками, уточнення результатів і навіть критика, яка допомагає підвищити якість роботи. І це діалог із майбутнім, адже будь-яке дослідження залишає за собою поле відкритих питань, які стимулюють продовження пошуку.

В IT цей діалог набуває сучасних форм: викладення коду у відкриті репозиторії, публікація препринтів, створення спільнот навколо окремих проблем. Коли дослідник розміщує свій алгоритм на GitHub, він фактично звертається до колег: «Ось моє рішення, хто готовий його покращити?». Це і є науковий діалог у цифрову добу.

Поряд із діалогом наука завжди була колективною діяльністю. У великих проєктах неможливо обійтися без розподілу ролей: одні займаються теорією, інші будують експериментальні установки, ще інші аналізують дані чи створюють інструменти. Саме завдяки такій взаємодії виникає ефект мережі: чим більше дослідників працює над проблемою, тим швидше рухається наука. Сьогодні це проявляється у міжнародних колабораціях, зокрема у сфері кібербезпеки. Жодна окрема команда не може відстежити всі глобальні загрози,

але спільні бази даних дозволяють об’єднати зусилля тисяч фахівців і створити більш надійний захист.

Таким чином, наука як діалог і колективна діяльність - це джерело її сили. Вона постійно самокоригується, розвивається завдяки обговоренню і взаємодії. Для дослідників у сфері ІТ це означає, що справжня цінність їхньої роботи починається лише тоді, коли вона стає частиною спільного наукового процесу, відкрита для дискусії, перевірки й продовження іншими.

Розглянемо приклад, який добре ілюструє колективний характер науки у сфері кібербезпеки. У 2020 році відбулася одна з найбільших кібератак сучасності (кампанія SolarWinds), коли через оновлення популярного програмного забезпечення зловмисники отримали доступ до сотень урядових та корпоративних мереж у всьому світі. Жодна окрема організація не могла б самотужки виявити та повністю зрозуміти масштаби атаки. Лише завдяки тому, що різні учасники - приватні компанії з кібербезпеки, державні структури, академічні дослідники та міжнародні CERT-групи - почали обмінюватися зразками шкідливого коду, логами та технічними звітами, вдалося поступово скласти «мозаїку» атаки. Кожна сторона бачила лише фрагмент, але об’єднання даних і спільні публікації дозволили реконструювати повний сценарій: від першого зараження до механізмів lateral movement у мережах жертв.

Ця атака стала своєрідним методологічним уроком: SolarWinds показав, що жодна організація не може самостійно протистояти атакам такого масштабу. Вирішальним фактором стала кооперація науковців, приватних компаній і державних структур. Комунікація, як у закритих, так і у відкритих каналах, була ключем до швидкого поширення інформації та створення захисту.

Таким чином, наука існує лише тоді, коли знання стає предметом обговорення та співпраці. Кожне дослідження є частиною великої розмови — з минулими поколіннями науковців, із сучасниками та з тими, хто продовжить роботу в майбутньому. У сучасних умовах ІТ та кібербезпеки цей діалог відбувається у формі відкритих публікацій, спільних баз даних, репозиторіїв коду та міжнародних колаборацій.

Колективний характер науки виявляється особливо яскраво у протидії глобальним загрозам: від атак на критичні інфраструктури до масових кампаній кіберзлочинців. Жодна команда чи організація не здатна впоратися з цим самостійно. Лише об’єднання знань, обмін інформацією та спільна інтерпретація результатів дають можливість адекватно реагувати на виклики.

Таким чином, наука як діалог і колективна діяльність - це не лише теоретичний принцип, а практична умова її існування. Вона забезпечує перевірку, розвиток і застосування знань, а в ІТ-дослідженнях і кібербезпеці стає ключем до виживання в умовах швидко мінливого світу загроз.

3. Форми наукової комунікації

Наукова комунікація має багато проявів, і вони змінювалися разом із розвитком науки та технологій. У класичному розумінні під цим маються на увазі журнальні публікації, монографії, конференції. Проте сьогодні, особливо в ІТ-галузі, спектр форм значно ширший.

Традиційні форми - це насамперед наукові журнали, які дають офіційний статус результатам і проходять процедуру рецензування, що забезпечує

перевірку якості. Монографії та колективні збірники дозволяють викласти результати великих досліджень у системному вигляді. Конференції виконують роль «гарячої лінії» науки: саме тут результати презентуються швидко, обговорюються і піддаються колективній критиці.

У ***сучасну*** добу виникли нові канали. Препринт-сервери (наприклад, arXiv) дають змогу опублікувати статтю ще до проходження рецензування, щоб швидко донести результати до спільноти. Відкриті рецензії дозволяють бачити коментарі експертів і прозорий процес оцінки. Наукові блоги і соціальні мережі стають простором популяризації й дискусій, де часто народжуються ідеї для майбутніх робіт. Так у 2020-2021 роках під час пандемії COVID-19 одним із найгарячіших напрямів стали дослідження моделей поширення вірусу. Хоча існували офіційні публікації в журналах, величезна кількість дискусій ідей відбувалася у Twitter та особистих блогах вчених. Саме там епідеміологи, математики та IT-спеціалісти в режимі реального часу обговорювали дані, ділилися графіками, перевіряли моделі одне одного. Багато з цих «попередніх» ідей потім переросли у формальні наукові статті. Таким чином, блоги й соцмережі можуть виконувати роль «інкубатора ідей». Це простір, де науковці швидко перевіряють гіпотези, отримують критику й запускають дискусію, яка згодом переходить у серйозні публікації.

Особливістю IT-галузі є власні, специфічні форми комунікації. Це white papers — технічні документи, які часто публікують компанії для опису нових технологій (наприклад, у сфері блокчейну). Це RFC-документи (Request for Comments), які з 1969 року є механізмом обговорення й стандартизації інтернет-протоколів. Це репозиторії коду (GitHub, GitLab), які стали не лише інструментом програмування, а й платформою для наукового обміну: тут дослідники викладають свої алгоритми, щоб інші могли перевіряти та вдосконалювати їх.

Таким чином, форми наукової комунікації можна уявити як безперервний спектр: від класичних академічних видань до динамічних цифрових платформ. Усі вони разом утворюють екосистему, яка дозволяє знанням циркулювати, перевірятися і розвиватися.

4. Культура публікацій

Коли ми говоримо про культуру публікацій, то найчастіше маємо на увазі академічну доброчесність: недопустимість плагіату, фальсифікацій результатів чи маніпуляцій з авторством (ці питання розглядалися в Темі 1). Але насправді культура публікацій значно ширша. Вона визначає, як дослідницькі результати стають частиною наукової спільноти, наскільки вони визнаються і який вплив мають на розвиток науки й практики.

Насамперед важливим є вибір майданчика для публікації. У сучасному світі існують як авторитетні журнали й конференції, так і так звані хижацькі видання, які беруть гроші за розміщення текстів без належного рецензування. Різниця принципова: у першому випадку стаття стає частиною перевіреної бази знань, у другому - перетворюється лише на формальність, яка може нашкодити репутації дослідника. Тому культура публікацій передбачає усвідомлений вибір: де саме розмістити результати, аби вони стали частиною серйозної наукової дискусії.

Загалом можна виділити наступні рівні публікацій: локальні, міжнародні, рейтинги Scopus/WoS. Не всі наукові публікації мають однакову вагу навіть тоді, коли вони публікуються в офіційних, «нехижацьких» наукових виданнях. Важливо розуміти, що існують різні рівні, які відображають як охоплення аудиторії, так і престиж видання. Для молодих дослідників, і особливо в IT-галузі, правильний вибір каналу публікації впливає не лише на кар'єру, а й на те, чи буде робота почута.

Локальні публікації - це журнали та конференції, орієнтовані на національну чи регіональну аудиторію. Їхня роль важлива: вони створюють простір для перших кроків у науці, дозволяють відпрацювати навички написання статей, дають можливість апробувати ідеї в колі колег. Але вплив таких публікацій обмежений: вони рідко цитуються за межами країни і не завжди входять у міжнародні бази.

Міжнародні публікації - це журнали та конференції, які мають глобальне охоплення. Вони індексуються у наукометричних базах Scopus та Web of Science (WoS), що робить результати доступними для науковців з усього світу. У сфері IT і кібербезпеки до таких належать конференції IEEE, ACM, Usenix Security, Black Hat чи журнали типу IEEE Transactions on Information Forensics and Security. Саме тут відбувається «велика розмова» науки, і саме ці публікації формують світовий порядок денний.

Щоб оцінити якість журналів, використовуються рейтинги. У Scopus та WoS видання поділяються на квартилі: від Q1 (найпрестижніші, з найвищим рівнем цитування та суворим відбором статей) до Q4 (журнали нижчого рівня, але все ж визнані міжнародною базою). Публікація в журналі Q1 чи Q2 значно підвищує видимість роботи та репутацію дослідника, тоді як Q3–Q4 частіше використовуються для апробації ідей чи для спеціалізованих тем із вузьким колом читачів. Для IT-досліджень ця ієрархія особливо важлива, бо швидкість розвитку галузі велика. Публікація на локальній конференції може швидко застаріти й залишитися непоміченою, тоді як міжнародний журнал чи конференція забезпечує реальний вплив: робота буде процитована, перевірена, розвинена іншими.

Таким чином, культура публікацій передбачає усвідомлений вибір рівня: локальні видання потрібні для тренування і перших кроків, але справжня наукова дискусія й визнання відбуваються на міжнародному рівні. А орієнтир на Q1-Q2 - це не лише «престиж», а й гарантія того, що результати стануть частиною глобального наукового процесу.

Не менш важливим є розуміння форматів публікацій. У класичній науці це журнальні статті, тези конференцій та монографії, у IT та кібербезпеці - ще й технічні звіти, препринти, відкриті репозиторії коду. Кожен формат виконує свою роль: стаття у журналі надає академічний статус, white paper дозволяє швидко донести результати індустрії, а викладений на GitHub код робить дослідження відтворюваним і придатним для перевірки іншими. Культура публікацій полягає у тому, щоб не обмежуватися «паперовою статтею», а обирати форму, яка відповідає меті дослідження.

Однією з ключових ознак наукової публікації є процедура ***рецензування***. Це процес, коли незалежні експерти оцінюють якість статті перед її прийняттям до журналу чи конференції. Рецензування виконує роль «фільтру» наукової

спільноти: воно захищає від неякісних чи неперевірених результатів, виявляє слабкі місця, інколи підказує напрями вдосконалення. У сфері ІТ це особливо важливо, адже нові алгоритми чи системи без перевірки можуть виглядати багатообіцяюче, але на практиці виявитися непридатними.

Якість наукових видань і статей часто вимірюють за допомогою імпакт-фактору. Це показник, який відображає, скільки разів у середньому статті з даного журналу цитуються іншими дослідниками. Високий імпакт-фактор означає, що журнал має великий вплив і публікує роботи, які активно використовують у науковій спільноті. Для ІТ-досліджень це своєрідний орієнтир: якщо стаття опублікована в журналі з високим імпакт-фактором, імовірність її помітності й цитування значно зростає.

Ще один важливий індикатор - h-index. Це показник, який вимірює продуктивність і вплив конкретного науковця. Наприклад, h=10 означає, що у дослідника є щонайменше 10 статей, які процитовані щонайменше 10 разів кожна. У галузях, що швидко розвиваються, таких як ІТ чи кібербезпека, цей показник демонструє не лише кількість робіт, а й їх реальну вагу у спільноті.

Проте наука — це не тільки тексти. Важливою частиною комунікації є презентація результатів. Виступи на конференціях, семінарах, вебінарах, захистах магістерських чи дисертаційних робіт - це спосіб донести ідеї «живим голосом». У ІТ-дослідженнях часто саме презентація дозволяє показати роботу алгоритму, продемонструвати прототип чи живий приклад коду. Вдалий виступ може дати досліднику нові контакти, ідеї для співпраці й критичний зворотний зв’язок, який неможливо отримати з письмової рецензії.

Таким чином, рецензування, імпакт-фактор і h-index - це механізми, які забезпечують якість і вимірюють вплив наукової діяльності, тоді як презентація результатів - це мистецтво комунікації, що робить дослідження видимим і зрозумілим. Для магістрів важливо розуміти: ці елементи не є «формальністю», а частиною культури науки, яка визначає, чи стане ваша робота частиною великого наукового діалогу.

Окрема риса культури публікацій у сучасній науці - це відтворюваність і відкритість. Якщо раніше достатньо було опублікувати текст із формулами й таблицями, то сьогодні наукова спільнота очікує доступу до вихідних даних і до коду. Особливо це стосується ІТ-досліджень. Алгоритм, який неможливо відтворити, викликає сумніви, а стаття без відкритого репозиторію сприймається як неповна. Тому культура публікацій вимагає прозорості: ми не лише декларуємо результат, а й даємо іншим можливість його перевірити.

Ще одна складова культури публікацій - мова та стиль. Англійська фактично стала універсальною мовою науки. Це створює виклик для дослідників, адже потрібно не просто перекласти свої думки, а навчитися писати зрозуміло й чітко, уникати двозначності, дотримуватися наукового стилю. Для ІТ-галузі тут є додаткова специфіка: важливу роль відіграють не лише слова, а й графіки, таблиці, блоки коду, які повинні бути подані так, щоб інші могли їх використати.

І нарешті, культура публікацій охоплює питання рецензування та авторства. У спільній статті важливо правильно визначити, хто є автором, а хто зробив допоміжний внесок. У рецензуванні важлива взаємоповага: навіть

критика має бути конструктивною, а не принизливою. Це формує атмосферу довіри й підтримки в науковій спільноті, без якої розвиток науки неможливий.

Таким чином, культура публікацій - це не лише уникання помилок і порушень. Це система норм і практик, яка визначає, як знання входить у науковий обіг, наскільки воно стає визнаним і чи може його використати спільнота. Для ІТ-досліджень і кібербезпеки культура публікацій має особливе значення: темп змін у галузі дуже високий, і лише правильна комунікація результатів дозволяє дослідникам бути почутими, а їхнім ідеям знайти практичне застосування.

Розглянемо приклад, який добре показує, чому культура публікацій іноді має просто вирішальне значення. У 2019 році кілька дослідницьких груп заявили про створення «революційних» методів виявлення фішингових сайтів за допомогою машинного навчання. У статтях були наведені дуже високі показники точності - понад 98%. Але коли інші науковці спробували повторити результати, виявилося, що автори не опублікували ані вихідних даних, ані коду. Це зробило відтворення експериментів неможливим. Згодом незалежні групи, використавши власні датасети, змогли показати, що точність насправді набагато нижча, особливо на нових, «свіжих» фішингових зразках. Тобто первісні результати виявилися завищеними, а без доступу до вихідних матеріалів це можна було приховати. У підсумку такі статті втратили довіру в науковій спільноті, хоча формально вони були опубліковані в журналах.

Цей приклад показує, що публікація без відкритих даних і коду у сфері ІТ фактично знецінює дослідження. У швидкозмінному середовищі кібербезпеки результат, який неможливо перевірити та застосувати на практиці, не має наукової ваги. Саме тому культура публікацій передбачає прозорість: дослідник має дати іншим інструменти для перевірки, інакше його робота залишиться лише «красивою декларацією».

6. Виклики для наукової комунікації та культури публікацій

Виклики для наукової комунікації та культури публікацій - це проблеми, які сьогодні суттєво впливають на якість, прозорість і довіру до наукових результатів.

Першим викликом є «хижацькі» журнали та конференції. Вони маскуються під академічні видання, але фактично працюють за принципом «заплати - і твою статтю надрукують», без належного рецензування. Це загрожує тим, що у науковий обіг потрапляють слабкі чи навіть фальсифіковані роботи, а молоді дослідники можуть втратити репутацію. ***Приклад***: у 2017 році журналісти Science провели експеримент: відправили вигадану статтю з грубими помилками до десятків журналів, які позиціонували себе як міжнародні академічні. Більшість із них прийняли роботу «за гроші», без рецензування. У сфері ІТ молоді дослідники часто стикаються з подібними пастками — наприклад, конференції, що називають себе «глобальними», але насправді збирають кілька людей у готелі й видають сертифікати.

Другим викликом є перевантаження інформацією. Щороку виходять сотні тисяч статей, і знайти серед них справді якісні стає дедалі важче. У ІТ це особливо відчутно: нові алгоритми з’являються майже щодня, і науковцям складно відрізнити прорив від «шуму». ***Приклад***: у сфері машинного навчання

щороку публікуються десятки тисяч статей. Наприклад, лише на конференції NeurIPS подається понад 10 тисяч заявок. Це призводить до ситуації, коли навіть досвідченим дослідникам важко відслідковувати справді значущі роботи. У кібербезпеці це проявляється у «шумі» навколо нових вразливостей, коли десятки повідомлень від різних дослідників повторюють одне й те саме.

Третім викликом є баланс між швидкістю та якістю. Препринти й блоги дозволяють швидко донести результати, але без рецензування вони можуть містити помилки. У той самий час журнальні статті часто виходять із запізненням, що в ІТ робить результати, що тільки вийшли, менш актуальними. ***Приклад***: під час пандемії COVID-19 багато досліджень із моделювання поширення вірусу з'являлися у вигляді препринтів. Частина з них була якісною, але чимало містили грубі помилки. Їх активно цитували й використовували політики, хоча ці результати ще не пройшли рецензування. У ІТ схожа ситуація трапляється з дослідженнями нових алгоритмів: препринт може набрати популярність у спільноті GitHub чи Twitter, але згодом виявляється, що модель не відтворюється.

Четвертий виклик пов'язаний із відтворюваністю досліджень. У багатьох роботах, особливо в ІТ, бракує відкритих даних чи коду, що унеможливлює перевірку результатів. Це підриває довіру до науки. Яскравий ***приклад*** - скандал із роботами у сфері штучного інтелекту для медицини. Деякі групи заявляли про алгоритми, які перевершують лікарів у діагностиці, але не надавали даних чи коду. Коли незалежні команди намагалися відтворити результати, вони отримували зовсім інші показники. Це стало сигналом для руху «Reproducibility Crisis» у науці.

П'ятий виклик — мовний бар'єр та доступність. Наука сьогодні в ІТ-сфері переважно англомовна, що ускладнює участь для тих, хто не володіє мовою достатньо добре. Додатково існує проблема платного доступу до багатьох журналів, що обмежує обіг знань. ***Приклад***: у країнах, де англійська не є основною мовою, науковцям важко публікуватися у престижних журналах. Наприклад, українські дослідники часто змушені витрачати значні ресурси на професійний переклад і редактуру англійською. Додатково існує проблема платних журналів: публікація в Q1-виданні може коштувати кілька тисяч доларів, що є недоступним для багатьох університетів.

І нарешті, серйозним викликом є етика у науковій комунікації. Неправильне визначення авторства, упередженість у рецензуванні, фабрикація результатів чи плагіат підривають довіру до науки загалом. ***Приклад***: у 2020 році вибухнув скандал із рецензуванням у сфері штучного інтелекту: деякі дослідники виявили упередженість у відхиленні робіт на конференції NeurIPS, що викликало дискусії про прозорість процесу. А ще частими є конфлікти навколо авторства: у великих ІТ-проєктах, де працюють десятки людей, не завжди зрозуміло, хто справді заслуговує бути співавтором статті

Таким чином, основні виклики для наукової комунікації та культури публікацій можна сформулювати як питання довіри, прозорості й якості у світі, де кількість результатів зростає швидше, ніж можливості їхньої перевірки.

Говорячи про наукову комунікацію, можна стверджувати, що це та частина фундаменту, без якого сама наука не існує. Результати досліджень набувають

цінності лише тоді, коли вони стають частиною спільного обміну знаннями. Класичні форми публікацій, як-от журнали та конференції, і сучасні цифрові інструменти - препринти, відкриті дані, репозиторії коду, блоги та соціальні мережі - разом створюють складну екосистему, яка забезпечує рух науки вперед.

Культура публікацій визначає якість цього процесу. Вона вимагає чесності, прозорості, відтворюваності й поваги до спільноти. Для ІТ-досліджень і кібербезпеки це має особливе значення: результати тут швидко старіють, і лише правильна комунікація дозволяє зробити їх корисними, вчасними та застосовними.

Разом із тим наукова комунікація стикається з викликами: хижацькі журнали, інформаційне перевантаження, баланс між швидкістю та якістю, проблеми відтворюваності, мовні бар'єри й етичні дилеми. Уміння орієнтуватися в цих викликах є не менш важливою навичкою для молодого дослідника, ніж знання методів чи інструментів аналізу.

Таким чином, культура публікацій - це не лише технічний аспект академічної роботи. Це цілісна система норм і практик, яка формує довіру, репутацію й вплив науковця. Для магістрів у сфері ІТ та кібербезпеки це означає одне: ваша робота буде визнана наукою лише тоді, коли вона стане частиною відкритого діалогу і буде доступною для перевірки, критики й розвитку іншими.

Питання

1. Що забезпечує наукова комунікація?
2. Баланс між відкритістю і обмеженням інформації.
3. Особлива культура комунікації в кібербезпеці.
4. Наука як діалог і як колективна діяльність. Знання як предмет обговорення та співпраці.
5. Пояснити, в чому полягають виклики для наукової комунікації та культури публікацій. Навести приклади.

Тема 6. СУЧАСНІ ТРЕНДИ В ІТ-ДОСЛІДЖЕННЯХ

План

1. **Штучний інтелект нового покоління**
2. **Zero Trust Architecture**
3. **Квантові обчислення і криптографія**
4. **Конфіденційні та розподілені обчислення**
5. **Соціотехнічні аспекти та людиноцентрична безпека**

Наука в ІТ-галузі має особливу динаміку: нові результати дуже швидко переходять у практику, а іноді навіть індустрія випереджає академічну науку і стає джерелом трендів. Причин цьому достатньо. По-перше, для перевірки гіпотез, проведення експериментів в ІТ-галузі часто достатньо ноутбука, хмарних ресурсів або відкритих датасетів, тоді як, наприклад, в біології чи фізиці для цього потрібні дорогі лабораторії. По-друге, результати ІТ-досліджень часто одразу можуть інтегруватися у продукти (новий алгоритм → новий сервіс), що стимулює індустрію фінансувати дослідження, при цьому великі компанії (Google, Microsoft, Amazon) мають власні наукові підрозділи, публікації яких на топ-конференціях часто випереджають по значущості університетські. По-третє, це відкритість і глобальність досліджень в ІТ-галузі: публікація коду й датасетів на GitHub, HuggingFace чи Kaggle робить дослідження відтворюваним і швидко масштабованим.

ТОП-5 трендів ІТ-досліджень 2025: штучний інтелект нового покоління, Zero Trust Architecture, квантові обчислення і криптографія, конфіденційні та розподілені обчислення, соціотехнічні аспекти та людиноцентрична безпека.

1. Штучний інтелект нового покоління

Тренди:

- *великі мовні моделі* (Large Language Model) (LLM): працює з текстами, мають дуже багато параметрів (штучних «нейронних з'єднань»), наприклад, GPT-3 мала 175 мільярдів параметрів, при цьому чим більше параметрів, тим модель точніше «розуміє» контекст і мову. LLM навчилася прогнозувати наступне слово у реченні, тому може відповідати на запитання, писати тексти, генерувати код, перекладати, навіть імітувати діалог. Прикладами застосування в ІТ є: автоматичне написання коду, виявлення підозрілих листів (антифішинг), автоматичне пояснення логів чи подій безпеки, створення «розумних» чат-ботів для користувачів.

  Але все не так безхмарно: LLM можуть помилятися або «вигадувати» факти (це називають галюцинаціями), є ризики з конфіденційністю даних (якщо їх тренувати на приватних текстах), моделі можна використати і для зловмисних цілей (генерація фішингових повідомлень).

  Не дивлячись на це, сьогодні серед програмістів (найбільш яскравих представників ІТ-сфери) наявне велике занепокоєння, що дуже скоро вони просто стануть непотрібними. Але це **хибна тривога**, принаймні, назараз. Великі мовні моделі (LLM), як-от GPT-4 чи GPT-5, справді здатні генерувати код, пропонувати виправлення, пояснювати алгоритми і

навіть створювати робочі прототипи програм. Але це не означає повну заміну програмістів. Розглянемо докладно, чому LLM не можуть замінити програмістів повністю. По-перше, модель не розуміє реальних бізнес-процесів чи стратегічних цілей компанії. Вона може написати код, але не визначає, який саме продукт потрібен. При цьому згенерований код може містити помилки, вразливості або працювати не так, як очікує користувач. Людина повинна його перевірити, протестувати й інтегрувати. Дуже важливим є питання безпеки та відповідальності (особливо в галузі кібербезпеки). Дійсно, некоректно згенероване рішення у сфері кібербезпеки може призвести до критично серйозних ризиків. Машина не несе відповідальності, на відміну від програміста. Для програміста одним з ключових моментів є питання оптимізації коду, а також питання креативності. LLM же здатна комбінувати відомі патерни, але пошук принципово нових підходів, нестандартна оптимізація чи робота в умовах неповних даних лишається за людиною.

Таким чином, LLM у програмуванні - це інструмент підсилення (як калькулятор для математика). Вони допомагають з рутинними завданнями: написати шаблон, знайти синтаксичну помилку, пояснити бібліотеку, прискорюють прототипування й знижують поріг входу у програмування для новачків. Але стратегічні рішення, дизайн архітектури, тестування, забезпечення якості й відповідальність залишаються за фахівцями-програмістами. LLM - це потужний інструмент, який може автоматизувати частину роботи, але не замінити професіонала. Швидше за все, майбутній програміст буде працювати «поруч із моделлю», використовуючи її як асистента, а не конкурента.

- *генеративний AI* - система, яка не тільки аналізує дані, а й створює новий контент: текст, зображення, музику, відео, код. Прикладами застосування в IT-дослідженнях можуть бути: генерація тестових даних для перевірки алгоритмів, створення синтетичних датасетів, якщо реальні обмежені. Безпосередньо в кібербезпеці: генерація фішингових листів, створення «сценаріїв атак» у тестових середовищах, одночасно - виявлення та протидія цим же загрозам у реальному часі. Таким чином, генеративний AI - це такий «творчий штучний інтелект», який не тільки розпізнає інформацію, а й створює нову. І хоча це дає величезні можливості, але і створює нові загрози: AI може «вигадувати» і видавати помилки, зловмисники можуть використати для створення ще більш реалістичних атак (deepfake, фішинг).

  Треба розрізняти LLM і AI (табл.6.1).

Таблиця 6.1. LLM та генеративний AI

Ознака	LLM (Large Language Model)	Генеративний AI (загалом)
Сфера	Робота з текстами (природна мова, код, діалоги, переклади)	Будь-які типи даних: текст, зображення, аудіо, відео, 3D-об’єкти
Приклади	GPT-4/5, Claude, LLaMA	Stable Diffusion, DALL·E,

		MidJourney, Sora, VALL-E
Завдання	Генерація тексту, відповідей, коду, резюме, чат-боти	Генерація картинок, музики, відео, віртуальних середовищ
Обмеження	Працює лише з текстовими даними	Може поєднувати кілька модальностей (текст + зображення + аудіо)
Відношення	LLM = підвид генеративного AI	Генеративний AI = ширша парасолька, що включає LLM

Таким чином, кожна LLM - це генеративний AI, але не кожен генеративний AI є LLM.

І хоча генеративний AI є більш потужною системою, ніж LLM, але й він не зможе повністю замінити програміста по тим самим причинам, що були перераховані вище. Генеративний AI не «замість», а «разом» з програмістами. Він змінює характер роботи: від ручного кодування до управління інтелектуальними інструментами й побудови складних рішень. Програмісти стають більше архітекторами й керівниками процесу, ніж «чистими кодерами». Важливішими будуть навички перевірки, інтеграції, тестування, безпекового аудиту. В майбутньому зросте попит на тих, хто вміє ефективно співпрацювати з AI (prompt engineering, code review для ШІ-згенерованого коду).

- *автономні агенти* - це система на базі ШІ, яка може ставити підзадачі, шукати інформацію, писати код, тестувати його, виправляти помилки й повторювати цикл без прямої участі людини, може планувати дії, змінювати стратегію, якщо умови змінилися, вчитися на досвіді, тобто це вже не просто «скрипт», а щось ближче до «цифрового співробітника». В ІТ-дослідженнях автономні агенти застосовуються для автоматичного тестування програмного забезпечення, оптимізації використання хмарних ресурсів; безпосередньо в кібербезпеці для автоматичного аналізу логів й відслідкування аномалії, симуляції кібератак для тестування захисту, автономні SOC - мінімізують участь людини в рутинних завданнях. Але і тут виникають питання: як гарантувати, що агент не вийде з-під контролю? Хто винен, якщо автономний агент завдав шкоди? Крім того, зловмисники теж можуть створювати автономних агентів-«хакерів». Таким чином, у кібербезпеці це означає і нові можливості захисту, і нові ризики від автоматизованих атак.

  Автономні агенти — це новий крок у розвитку штучного інтелекту. Вони здатні не лише виконувати окремі інструкції, а й самостійно ставити підзадачі, планувати кроки, генерувати код, тестувати його та виправляти помилки. На перший погляд може скластися враження, що такі агенти готові повністю замінити людину, зокрема програміста. Проте це не так.

  Насамперед агенти не володіють розумінням контексту. Вони можуть написати програму, але не здатні усвідомити, навіщо ця програма

потрібна бізнесу чи суспільству, які стратегічні цілі вона має реалізувати, які ризики чи наслідки може спричинити. Людина-програміст бере на себе саме цю ключову функцію — зв’язати технічне рішення з реальними потребами.

Другою проблемою є надійність. Сучасні агенти схильні до так званих «галюцинацій» — створення рішень, які виглядають правильними, але насправді є некоректними або небезпечними. У сфері кібербезпеки чи критичних інфраструктур така помилка може мати катастрофічні наслідки. Тому роль людини як контролера і перевіряючого тут є незамінною.

Ще одна межа — креативність. Агенти можуть комбінувати вже відомі патерни і будувати рішення на основі наявних даних, але створення принципово нових підходів, інноваційних алгоритмів чи архітектур — це поки що виключно сфера людської творчості.

Не менш важливо й те, що автономні агенти не несуть відповідальності. Якщо написаний ними код призведе до збою системи чи витоку даних, то відповідальність завжди буде на розробнику або компанії, яка застосувала цей інструмент. Людина тут виконує роль гаранта якості, безпеки і етичності продукту.

Таким чином, автономні агенти — це не заміна програмістів, а інструменти, що змінюють характер їхньої роботи. Вони знімають рутину, дозволяють швидше виконувати завдання, але ключові ролі — стратегічне бачення, контроль, креативність і відповідальність — залишаються за людиною.

Висновок

Автономні агенти роблять програмування швидшим і доступнішим, але вони не можуть повністю замінити людину. Вони не розуміють контексту, схильні до помилок, не здатні на справжню креативність і не несуть відповідальності. Тому майбутнє — це не «агенти замість програмістів», а програмісти, які ефективно керують агентами та використовують їх як інструменти підсилення.

2. Zero Trust Architecture

Тренд: відмова від класичних периметрів, перевірка «кожного і всюди».

Події останніх років демонструють якісно новий рівень кіберзагроз, де кібератаки стають невід’ємною частиною воєнних дій та геополітичних протистоянь. Державні мережі, які традиційно розглядаються як відносно захищені периметром системи, сьогодні стикаються з безпрецедентними за масштабом і складністю загрозами, що потребує фундаментального перегляду підходів до управління кібербезпекою.

Міжнародний досвід останніх років демонструє інтерес до архітектури «нульової довіри» (ZeroTrustArchitecture, ZTA) як до перспективного підходу до вирішення існуючих проблем. Концепція ZTA, що базується на принципі «ніколи не довіряй, завжди перевіряй», пропонує радикально інший підхід до управління кібербезпекою, де довіра не є статичним атрибутом, а динамічно оцінюється для кожного запиту на доступ до ресурсів. Цей підхід є особливо актуальним для державних мереж.

Для державних мереж України, що функціонують в умовах повномасштабної агресії, питання інтеграції ZTA-підходів у систему управління кібербезпекою набуває особливої актуальності. Необхідність забезпечення безперервності функціонування критичних державних сервісів за умов постійного кіберпротистояння потребує не тільки технологічної модернізації, але й адаптації управлінських процесів до реалій архітектури нульової довіри.

Впровадження ZTA у державних мережах України стикається з комплексом специфічних проблем, які потребують особливої уваги та адаптації міжнародних підходів до національних умов. Ці проблеми охоплюють нормативно-правову, технічну, економічну, організаційну та геополітичну сфери.

Для розуміння масштабу необхідних змін важливо порівняти переваги архітектури нульової довіри із традиційною периметровою моделлю, яка нині домінує в українських державних мережах. Таблиця 6.2 ілюструє ключові різницю між цими підходами.

Таблиця 6.2. Порівняння периметрової моделі і Zero Trust Architecture

Критерій	Периметрова модель	Zero Trust Architecture
Модель довіри	Довіра – всередині периметра, недовіра – ззовні	Нікому не довіряй, завжди перевіряй
Принцип безпеки	Захист периметра	Захист кожного ресурсу
Автентифікація	Одноразова при вході до мережі	Неперервна для кожного запиту
Авторизація	Широкі права доступу всередині периметра	Мінімальні привілеї для кожного ресурсу
Сегментація	Груба сегментація по підмережам	Мікросегментація на рівні застосунків
Моніторинг	Фокус на периметрі	Моніторинг всіх взаємодій
Масштабуємість	Обмежена віддаленим доступом	Висока для розподілених середовищ
Адаптивність до загроз	Повільна реакція на внутрішні загрози	Швидке виявлення і реагування
Складність управління	Відносна проста	Висока, потребує автоматизації
Вартість впровадження	Низька для існуючих систем	Висока на початковому етапі
Сумісність з хмарними рішеннями	Обмежена	Висока
Захист від інсайдерських загроз	Слабка	Сильна

Це порівняння демонструє, що перехід від периметрової моделі до ZTA вимагає фундаментального перегляду підходів до безпеки. Незважаючи на

очевидні переваги архітектури нульової довіри, цей перехід пов’язаний із значними викликами в українському контексті.

Нормативно-правові виклики є однією з найбільш серйозних проблем для впровадження ZTA. Чинний Закон України «Про захист інформації в інформаційно-комунікаційних системах» не містить спеціальних положень, які б регулювали принципи нульової довіри, що створює правову невизначеність при впровадженні відповідних технологій. Відсутність національних стандартів ZTA призводить до фрагментарного та несистемного підходу до впровадження цих технологій у різних державних організаціях.

Вимоги Державної служби спеціального зв’язку та захисту інформації України, розроблені для традиційних периметрових моделей безпеки, не повністю відповідають принципам ZTA. Це створює необхідність адаптації існуючих процедур атестації та сертифікації інформаційних систем. Виникає також потенційний конфлікт між вимогами відкритості державних даних, закріпленими у Законі «Про доступ до публічної інформації», та принципами обмеженого доступу, що лежать в основі архітектури нульової довіри.

Особливе занепокоєння викликають технічні обмеження, які є серйозною перешкодою для впровадження ZTA. Значна частина державних мереж побудована на застарілих технологіях, які не підтримують сучасні протоколи автентифікації та авторизації. Відсутність сучасних засобів моніторингу та аналітики у більшості державних організацій унеможливлює реалізацію принципу неперервної верифікації доступу. Обмежена пропускна спроможність каналів зв’язку, особливо у регіональних державних установах, створює додаткові труднощі застосування систем, які потребують інтенсивної мережевої взаємодії.

Кадрові проблеми посилюють технічну ситуацію. Гостра нестача фахівців з кібербезпеки у державному секторі призводить до того, що багато організацій не мають достатнього експертного потенціалу для планування та реалізації проектів впровадження ZTA. Недостатній рівень знань про сучасні технології безпеки серед існуючих IT-фахівців потребує значних інвестицій у навчання та перепідготовку. Висока плинність кадрів у IT-підрозділах державних організацій, обумовлена низьким рівнем оплати праці в порівнянні з приватним сектором, створює додаткові труднощі для накопичення експертизи в галузі ZTA.

Економічні чинники є критичним обмеженням для впровадження ZTA. Обмежене фінансування IT-проектів у державному секторі, особливо в умовах воєнного часу, робить проблематичним виділення коштів на масштабні проекти модернізації безпекової інфраструктури. Висока вартість сучасних безпекових рішень, включаючи ліцензії на програмне забезпечення, обладнання та послуги інтеграції, часто перевищує бюджетні можливості державних організацій. Необхідність значних інвестицій у навчання персоналу створює додаткове фінансове навантаження на і без того обмежені IT-бюджети.

Проблеми державних закупівель додають додаткових труднощів до економічних викликів. Існуючі процедури державних закупівель, орієнтовані на стандартні товари та послуги, погано адаптовані для придбання інноваційних рішень безпеки. Відсутність спеціалізованих технічних вимог для ZTA-рішень у типовій тендерній документації призводить до закупівлі неадекватних чи

неповних рішень. Обмежений вибір локальних постачальників, здатних надати комплексні ZTA-рішення, створює залежність від закордонних виробників, що є неприпустимим для державного сектору і критично важливої інфраструктури, та ускладнює процес закупівель.

Організаційні виклики включають культурні бар'єри та проблеми міжвідомчої взаємодії. Традиційний підхід до управління IT-безпекою, що базується на периметровій моделі, глибоко вкорінений в організаційній культурі державних установ. Опір змінам з боку персоналу, особливо серед керівного складу, що не має достатнього розуміння сучасних загроз кібербезпеці, уповільнює процес впровадження нових підходів. Недостатнє розуміння переваг ZTA на управлінському рівні призводить до низького пріоритету відповідних проектів у стратегічному плануванні організацій.

Складність міжвідомчої взаємодії створює додаткові перешкоди системного впровадження ZTA. Різні державні органи мають різний рівень готовності до впровадження нових технологій, що ускладнює координацію спільних проектів безпеки. Відсутність єдиного підходу до управління кібербезпекою на міжвідомчому рівні призводить до фрагментації зусиль та неефективного використання ресурсів.

Геополітичні чинники додають унікальні виклики для запровадження ZTA в умовах України. Військовий стан створює особливі вимоги до безпеки, які не завжди сумісні зі стандартними підходами до впровадження нових технологій. Необхідність забезпечення безперервності роботи критично важливих систем в умовах постійних загроз обмежує можливості масштабних змін інфраструктури. Постійні кібератаки на державну інфраструктуру вимагають фокусування ресурсів на оперативному реагуванні, що відволікає від довгострокових проектів модернізації.

Вимоги до імпортозаміщення в критично важливих системах створюють додаткові обмеження щодо вибору технологічних рішень. Необхідність використання вітчизняних чи союзних технологій може обмежувати доступ до найбільш передових ZTA-рішень, представлених на світовому ринку.

Таким чином, для успішного впровадження ZTA у державному секторі України необхідна розробка комплексного підходу, який би враховував специфіку національних умов та поетапну стратегію реалізації. Такий підхід має включати адаптацію міжнародних методологій до національного контексту, розробку відповідної нормативної бази, створення програм підготовки кадрів, оптимізацію процедур закупівлі та забезпечення міжвідомчої координації. Особливу увагу слід приділити забезпеченню сумісності з існуючими системами та поетапному переходу від традиційних периметрових моделей до архітектури нульової довіри.

Таким чином, аналіз сучасних кіберзагроз та вразливостей традиційних периметрових моделей безпеки демонструє критичну необхідність переходу українських державних організацій до архітектури нульової довіри. Традиційна модель «довіри всередині периметра» демонструє свою неефективність в умовах сучасних кібератак, особливо з огляду на специфіку геополітичної ситуації в Україні. Перехід до архітектури нульової довіри забезпечить державним структурам значні переваги: підвищення адаптивності до нових видів атак, покращення можливостей моніторингу та реагування на інциденти,

посилення захисту від інсайдерських загроз, а також підвищення загального рівня кібербезпеки критично важливої інфраструктури.

3. Квантові обчислення і криптографія

Тренд: розвиток квантових процесорів, що ставить під загрозу класичні криптографічні алгоритми.

Класичний комп'ютер працює з бітами (0 або 1). Квантовий - з к'юбітами, які можуть перебувати у стані суперпозиції (одночасно 0 і 1) та «переплутаності». Це дозволяє виконувати обчислення паралельно і вирішувати задачі, недосяжні для класичних машин. Більшість сучасних алгоритмів шифрування (RSA, ECC) базуються на задачах факторизації або дискретного логарифмування, які класичні комп'ютери вирішують дуже повільно. Але алгоритм Шора (1994) показав, що квантовий комп'ютер може розв'язати ці задачі швидко. Як наслідок, у майбутньому квантовий комп'ютер зможе зламати поширені криптосистеми за години чи дні. Щоб підготуватися до «квантового дня» (моменту, коли класична криптографія стане зламаною), науковці створюють нові алгоритми, стійкі до квантових атак (пост-квантова криптографія (PQC)).

У 2024 році NIST стандартизував перші алгоритми PQC: CRYSTALS-Kyber (ключовий обмін) і CRYSTALS-Dilithium (цифровий підпис), а 2025 рік став періодом переходу від експериментів до практичного впровадження у реальні системи. Але ми не знаємо, коли з'явиться потужний квантовий комп'ютер, сотні мільйонів пристроїв доведеться оновлювати під нову криптографію, нові алгоритми потребують більше пам'яті та обчислювальних потужностей, навіть PQC алгоритми ще мають пройти багаторічні випробування.

Таблиця 6.3. Класична криптографія та пост-квантова криптографія

Ознака	Класична криптографія (RSA, ECC)	Пост-квантова криптографія (PQC)
Математична основа	Факторизація великих чисел, дискретний логарифм	Ґраткові задачі, багатоваріантні рівняння, кодові конструкції
Стійкість до класичних комп'ютерів	Висока — розв'язання займає мільярди років	Висока
Стійкість до квантових комп'ютерів	Низька — алгоритм Шора може зламати за години/дні	Висока — задачі вважаються важкими навіть для квантових алгоритмів
Продуктивність	Швидка, перевірена десятиліттями	Часто «важча»: більше пам'яті, довші ключі, потреба в оптимізації
Статус	Масово використовується (TLS, VPN, цифрові підписи)	На етапі впровадження; стандарти від NIST (Kyber, Dilithium)

Ризики	Загроза «Q-дня»: коли квантовий комп’ютер зламає сучасні алгоритми	Недостатньо перевірені на всі можливі атаки; потрібні роки тестування

Таким чином, квантові обчислення - це не просто новий тип процесора, а технологія, здатна змінити саму основу кібербезпеки. Хоча ми ще не маємо квантового комп’ютера, здатного зламати сучасні шифри, наукова спільнота вже активно готує «пост-квантову» епоху. Для дослідників у сфері ІТ і кібербезпеки це означає одне: потрібно бути готовими до змін і вже сьогодні вивчати нові стандарти криптографії.

Українська наукова спільнота вже працює в напрямку пост-квантової криптографії. У 2023 році Україна разом із Нідерландами започаткувала проект ALPaQCa (Improved Algebraic Methods for Cryptanalysis of Post-Quantum Cryptosystems) під керівництвом професора Андрія Олійника зі Київського національного університету імені Тараса Шевченка. Цей проект зосереджений на криптоаналізі постквантових криптосистем, тобто досліджує, наскільки стійкими є нові алгоритми шифрування проти потенційних атак, зокрема, тих, що можуть бути здійснені майбутніми квантовими комп’ютерами. Дослідники аналізують алгебраїчні властивості цих систем, шукають слабкі місця, моделюють атаки на нові конструкції. Така робота важлива саме для України, бо в умовах війни цифрова інфраструктура, державні та військові комунікації стають потенційними цілями. Попередньо, критична інформація, заснована на класичній криптографії, може стати вразливою до майбутніх квантових атак, тому підготовка до ери квантової криптографії вже зараз має бути одним із пріоритетів.

Ще одним яскравим прикладом українського науковця, який активно працює в темі криптографії й постквантових систем, є Горбенко І.Д. - доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій у Харківському національному університеті імені В. Н. Каразіна. У його доробку є праці, присвячені методам перспективних криптографічних перетворень, обґрунтуванню вибору стандартів електронного підпису для національного рівня, аналізу стійкості до квантових атак.

Таким чином, українські науковці не просто спостерігають за тенденціями в галузі, а вже входять у передову лінію досліджень, поєднуючи теоретичні підходи та практичні виклики безпеки держави.

4. Конфіденційні та розподілені обчислення

Тренд: зростає попит на захист даних у хмарі та під час обробки.

Сучасні ІТ-системи працюють у світі, де дані постійно передаються, копіюються й аналізуються. Це створює величезні можливості, але й значні ризики: витік персональних даних, корпоративна шпигунія, атаки на хмарні сервіси. Тому одним із ключових трендів ІТ-досліджень є конфіденційні та розподілені обчислення - підхід, що дозволяє аналізувати дані, не розкриваючи їхнього змісту, та виконувати обчислення у децентралізованому середовищі.

Конфіденційні обчислення - це технології, які дозволяють обробляти дані у захищеному середовищі так, щоб навіть власник інфраструктури не міг отримати доступ до «чистої» інформації.

Розподілені обчислення - це обробка інформації одночасно на багатьох пристроях чи вузлах мережі, що дозволяє використовувати ресурси різних організацій без централізації; створювати системи з підвищеною відмовостійкістю; знижувати ризик компрометації, бо дані зберігаються не в одному місці. Прикладами тут можуть слугувати блокчейн, federated learning (федеративне навчання), peer-to-peer мережі.

Таким чином, лікарні можуть спільно аналізувати медичні дані пацієнтів для виявлення закономірностей, не передаючи реальні бази між собою; компанії можуть обмінюватися інформацією про нові атаки у зашифрованому вигляді, зберігаючи конфіденційність своїх мереж; банки спільно борються з шахрайством, використовуючи конфіденційні обчислення для аналізу транзакцій.

Таким чином, конфіденційні та розподілені обчислення стають одним із головних трендів IT-досліджень 2025 року, бо вони поєднують дві потреби: захист даних і ефективну співпрацю. Для кібербезпеки ці технології відкривають нову еру, коли аналіз загроз, тренування моделей і обмін знаннями стають можливими навіть у середовищах з високим рівнем недовіри.

5. Соціотехнічні аспекти та людиноцентрична безпека

Тренд: кіберзахист більше не тільки технічна проблема, а й соціальна.

Коли ми говоримо про кібербезпеку, уявляємо собі складні алгоритми шифрування, міжмережеві екрани чи системи виявлення атак. Проте практика показує: найслабшою ланкою залишається не технологія, а людина. Саме соціотехнічні аспекти та людиноцентричний підхід сьогодні формують окремий напрям у дослідженнях IT і кібербезпеки. Вони враховують, що будь-яка система - це поєднання машинних і людських компонентів, і безпека залежить від взаємодії між ними.

Більшість успішних атак реалізуються не шляхом ламання шифрів, а через маніпуляції з людьми. Приклади включають фішинг, соціальну інженерію, виманювання даних через месенджери чи телефонні дзвінки. Це означає, що наукові дослідження мають враховувати психологічні, культурні та соціальні чинники.

IT-системи не існують у вакуумі. Вони вбудовані у соціальні практики: корпоративні культури, робочі процеси, правила доступу, звички користувачів. Наприклад, навіть найсучасніший захист не буде ефективним, якщо працівники зберігають паролі на папірцях чи нехтують оновленнями. Дослідження у цьому напрямі включають аналіз поведінкових моделей, факторів довіри до систем і бар'єрів прийняття нових технологій.

Традиційний підхід у кібербезпеці полягав у створенні максимально «жорстких» правил: довгі паролі, складні процедури аутентифікації, суворі політики доступу. Але на практиці це часто призводило до протилежного ефекту - користувачі починали обходити системи, щоб зменшити власне навантаження. Людиноцентрична безпека пропонує інший підхід: будувати захист навколо потреб і можливостей користувачів. Це означає створювати

рішення, якими реально зручно користуватися, які інтегруються в повсякденну діяльність і не провокують саботажу з боку людей.

Як приклади такого дослідження можна навести наступні: у сфері автентифікації вже помітний перехід від складних паролів до біометрії та багатофакторних методів; у корпоративній культурі все більше уваги приділяється не лише технічному тренінгу, а й психології (наприклад, як формувати культуру «не звинувачення», щоб співробітники не приховували інциденти).

Людиноцентрична безпека стикається з кількома викликами. По-перше, це баланс між зручністю та захищеністю: надто «м'які» системи будуть уразливими, надто «жорсткі» - не використовуватимуться. По-друге, різноманітність користувачів: рішення, які підходять для однієї культури чи вікової групи, можуть не працювати в іншій. По-третє, швидка еволюція загроз, які постійно знаходять нові способи впливати на людський фактор.

Таким чином, соціотехнічні аспекти та людиноцентрична безпека змінюють саму методологію досліджень у сфері ІТ. Вони показують, що кібербезпека - це не лише про коди і протоколи, а про розуміння людини. Це створює простір для міждисциплінарних досліджень на перетині ІТ, психології, соціології та когнітивних наук. У майбутньому успішними будуть ті рішення, які одночасно надійні технічно й дружні до користувачів.

Розглянемо декілька прикладів, які ілюструють впровадження людиноцентричного підходу у сфері кібербезпеки та комунікації саме в нашій країні.

Всеукраїнська інформаційна та освітня кампанія з кібергігієни. Це ініціатива під егідою РНБО України за підтримки уряду США, Міністерства освіти та науки, різних освітніх платформ. Кампанія має на меті підвищити обізнаність населення про кіберзагрози та базові правила кібергігієни. У межах кампанії випускаються навчальні матеріали, інфографіки, ролики, поради, які орієнтовані на різні групи - від дітей до дорослих. Це дозволяє «доступно мовою користувача» донести важливість безпеки в інтернеті.

Проєкт «Кібербезпека критично важливої інфраструктури України». Це великий міжнародний проєкт, у якому беруть участь університети, урядові органи, приватний сектор. Одним із аспектів є формування довіри, комунікація між приватним бізнесом, держструктурами та науковцями. У межах проєкту реалізують навчальні майданчики, симуляції, тренінги, де фахівці й локальні групи взаємодіють, обмінюються знаннями і практиками, враховуючи контекст користувачів систем.

Таким чином, в Україні вже реалізують проєкти, де людський фактор - не післямова, а ключовий компонент безпеки.

Питання

1. Сучасні тренди в ІТ-дослідженнях.
2. Участь України в сучасних ІТ-дослідженнях

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Мокін, Б. І. Методологія та організація наукових досліджень: підручник – вид.3-е, змін. та доп. [Електронний ресурс] / Б.І.Мокін, О.Б.Мокін, В.Б. Мокін. – Вінниця: ВНТУ, 2023. 230 с. https://press.vntu.edu.ua/index.php/vntu/catalog/view/805/1408/2677-1
2. Методологія наукових досліджень та приклади її використання [Електронний ресурс] : навчальний посібник / Самсонов В. В., Сільвестров А. М., Тачиніна О. М. – Київ : Національний університет харчових технологій, 2022. – 385 с. https://ela.kpi.ua/items/f5445ef1-700d-4ab6-a00d-391c5c6439b7
3. Зацерковний В. І. Методологія наукових досліджень : навч. посіб. / В. І. Зацерковний, І. В. Тішаєв, В. К. Демидов. – Ніжин: НДУ ім. М.Гоголя, 2017. – 236 с. https://dspace.ksaeu.kherson.ua/bitstream/handle/123456789/4642/%D0%9C%D0%95%D0%A2%D0%9E%D0%94%D0%9E%D0%9B%D0%9E%D0%93%D0%86%D0%AF%20%D0%9D%D0%90%D0%A3%D0%9A%D0%9E%D0%92%D0%98%D0%A5.pdf?sequence=1

Допоміжна

1. Трифонова О.М. Інформаційні технології в наукових дослідженнях / О.М.Трифонова, М.І.Садовий // Збірник наукових праць "Педагогічні науки" . 2022. № 98. С.27-33. https://ps.journal.kspu.edu/index.php/ps/article/view/4502

Інтернет ресурси

1. https://corewin.ua/blog/gdpr-compliance-guide/
2. https://www.researchgate.net/publication/376412417_Explainable_AI_is_Responsible_AI_How_Explainability_Creates_Trustworthy_and_Socially_Responsible_Artificial_Intelligence