Міністерство освіти й науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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. ЗАГАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ

План

1. **Визначення інформаційно-аналітичної роботи. Етапи процесу створення аналітичної інформації.**
2. **Організація ІАР на об'єкті**
3. **Інформація та джерела її отримання**
4. **Інформаційна розвідка**
5. **Зміст інформаційної та аналітичної роботи**
6. **Методи, закони та правила, що застосовуються в ІАР**

1. Визначення інформаційно-аналітичної роботи. Етапи процесу створення аналітичної інформації

Інформаційно-аналітична робота (ІАР) – це процес збору, обробки, аналізу та оцінки інформації з метою отримання важливих відомостей, формулювання висновків і їх розповсюдження, прийняття обґрунтованих рішень.

ІАР складається з декількох етапів:

1. Визначення необхідної інформації і напрямків її пошуку (встановлення цілей та обсягів необхідних даних);
2. Збір інформації (пошук і отримання потрібних відомостей із різних джерел);
3. Первісна обробка інформації (упорядкування, фільтрація та підготовка даних до аналізу);
4. Аналіз (тобто знаходження причинно-наслідкових та інших зв'язків між фактами, явищами та ін.);
5. Оцінка інформації та виробництво аналітичного продукту (відсіювання несуттєвих фактів, сортування та визначення достовірності фактів та подій, формулювання висновків);
6. Дозоване та виборче поширення інформації (підготовка та розповсюдження звітів та аналітичних матеріалів з урахуванням цілей та аудиторії).

1-й і 2-й етапи називаються інформаційною роботою. В результаті інформаційної роботи отримується необхідний для виконання розробки інформаційний масив, який представляє розрізнені відомості з питання, що цікавить. Наступні етапи – аналітична робота, в результаті якої інформаційний масив перетворюється в строго доказовий продукт діяльності аналітиків - висновок. Висновок має бути доказовим, перевіряємим, коротким, необхідним.

Проведення інформаційно-аналітичної роботи на прикладі аналізу ситуації щодо кіберзагроз для компанії:

1. Визначення необхідної інформації і напрямків пошуку: Вирішено з'ясувати рівень ризиків кіберзлочинності, пошук звітів про нові вектори атак та тенденції у кібербезпеці.

2. Збір інформації: Збираються дані з відкритих джерел (індустрійні звіти, аналітичні ресурси, новини), внутрішні логи компанії та інформація від служби безпеки.

3. Первісна обробка інформації: Упорядковують отримані дані, видаляють дублікати, структурують за типами атак, фільтрують за релевантністю.
4. Аналіз: Прослідковують нові способи атак, співставляють дані з внутрішніми логами, визначають найбільш ймовірні загрози для компанії, виявляють закономірності та причини появи нових векторів.
5. Оцінка інформації та виробництво аналітичного продукту: Відсіюють несуттєві факти, підтверджують достовірність даних, готують звіт із рекомендаціями щодо посилення захисту, роблять висновки щодо найбільш небезпечних ризиків
6. Дозоване та виборче поширення інформації: Підготовлений звіт передають керівництву, з фокусом на ключових висновках та рекомендаціях, інші матеріали поширюють вузькому колу зацікавлених осіб

Такий підхід забезпечує системне і цілеспрямоване опрацювання інформації для ухвалення рішень щодо кібербезпеки.

Функції та задачі ІАР в області захисту інформації:

1. збір запобіжної інформації для виявлення осіб та організацій, що спеціалізуються на посяганнях у сфері інтересів інформації, що охороняється;
2. відстеження оперативної обстановки, що виникає навколо об'єкта (інформації), що охороняється, тобто фіксація подій та осіб, що дозволяє виявити ознаки підготовки недружніх акцій;
3. приховані методи розслідування: виявлення осіб, які займаються передачею інформації противнику (конкуренту) серед співробітників об'єкта, що охороняється; відстеження каналів витоку конфіденційної інформації;
4. створення системи взаємовідносин і контрактів з офіційними особами і структурами, ЗМІ, що дозволяють отримувати попереджувальну інформацію про акції, що готуються;
5. аналіз відкритих та конфіденційних джерел щодо встановлення витоку інформації, забезпечення охорони інтересів об'єкта, встановлення та запобігання спробам отримати несанкціонований доступ до конфіденційної інформації.

В ІАР доводиться багаторазово повертатися до повторення дій пунктів 1-4.

Приклад: Захист конфіденційних розробок ІТ-компанії.

Уявімо, що українська ІТ-компанія працює над новим програмним продуктом у сфері штучного інтелекту. Це перспективна розробка, яка має високий комерційний потенціал. Компанія стає об’єктом інтересу конкурентів та навіть іноземних спецслужб.

1. ***Збір запобіжної інформації***

Фахівці ІАР відстежують діяльність конкурентних фірм та груп осіб, які раніше були помічені у промисловому шпигунстві. Формується база даних «потенційних загроз», що включає осіб, які активно цікавляться командою розробників у LinkedIn чи на профільних конференціях.

2. ***Відстеження оперативної обстановки***

Моніторинг соцмереж і форумів показує, що з’явилися підозрілі акаунти, які ставлять провокаційні запитання співробітникам компанії. Аналіз мережевого трафіку виявив спроби сканування серверів з IP-адрес іншої країни. Це фіксується як ознака підготовки до кібератаки.

3. ***Приховані методи розслідування***
Внутрішнє розслідування виявляє співробітника, який без службової потреби завантажує велику кількість внутрішніх документів. Додатковий контроль за його електронною поштою та носіями підтверджує намір передати інформацію конкурентам. Виявляються канали витоку (USB-носії, особистий Gmail).
4. ***Формування системи зовнішніх взаємовідносин***
Компанія укладає меморандум із національним CERT (командою реагування на комп'ютерні інциденти (в Україні: Державний центр кіберзахисту ДССЗЗІ (CERT-UA). Він відстежує інциденти у державних установах та на об'єктах критичної інфраструктури, публікує попередження (наприклад, про фішингові кампанії чи поширення шкідливих програм)), щоб отримувати повідомлення про загрози в IT-секторі. Крім того, налагоджуються контакти із журналістами галузевих ЗМІ, які надають «фонову» інформацію про ринкову ситуацію та дії конкурентів.
5. ***Аналіз відкритих та конфіденційних джерел***
Аналітики компанії проводять контент-аналіз даркнет-форумів і знаходять обговорення продажу вихідних кодів, схожих на їхні розробки. Це підтверджує факт витоку. Зіставивши внутрішні журнали доступу, дані SOC (Security Operations Center — центр операцій інформаційної безпеки, який відповідає за моніторинг, виявлення, аналіз та реагування на кіберзагрози в організації в режимі реального часу) та інформацію від партнерів, компанія визначає джерело інциденту й оперативно вживає заходів: блокує облікові записи, змінює архітектуру доступу до даних, запроваджує додаткову багаторівневу автентифікацію.

У цьому прикладі всі п'ять функцій ІАР працюють разом: від раннього виявлення потенційних порушників до розкриття внутрішнього інсайдера; від моніторингу зовнішніх загроз до аналізу витоку в даркнеті; від превентивних заходів до взаємодії з офіційними структурами. Це демонструє, що ІАР — це не лише збір інформації, а ціла система попередження, виявлення й реагування на загрози.

2. Організація ІАР на об'єкті.

На сьогодні існують три підходи до організації ІАР на об'єкті.

Перший варіант: ведення ІАР власне організацією. Аналітична група є підрозділом організації (підприємства) - аналітичний відділ, відділ стратегічного планування, департамент ризик-менеджменту тощо, має прямий вихід на керівника і зв'язки з іншими структурними підрозділами, в тому числі службою безпеки. Такий варіант роботи характерний для великих корпорацій, що займаються виробництвом і реалізацією продукції. Це є наслідком того, що більшість ризиків пов'язані з комерційною діяльністю конкурентів і зміною стану ринку. В цьому випадку аналітичну роботу ведуть грамотні спеціалісти: економісти, маркетологи, фінансисти та ін.. Служба безпеки лише повідомляє о можливих загрозах з боку зловмисників. В такій моделі аналітики не обов'язково є фахівцями з інформаційної безпеки. Основні завдання тут - аналіз ринку і конкурентного середовища; прогнозування ризиків (зміни попиту, цін, законодавства); оцінка фінансової стійкості компанії; виявлення «слабких сигналів» із зовнішнього середовища. Роль служби безпеки в такій моделі

обмежується тим, що вона виступає як «датчик загроз»: повідомляє про можливі дії зловмисників (шпигунство, витоки даних, кібератаки). Проте глибоку аналітику щодо впливу цих загроз на бізнес роблять саме економісти та маркетологи. Таким чином, У цій моделі аналітики не є вузькими фахівцями з інформаційної безпеки, вони — експерти у своїх галузях (економіка, фінанси, ринок), їхнє завдання — бачити бізнес-ризики. Саме завдяки цьому керівництво отримує повну картину і про економічні, і про інформаційні загрози.

Другий варіант - замикання ІАР на службі безпеки організації. В цьому випадку аналітична група структурно входить в службу безпеки, підкоряється безпосередньо начальнику служби безпеки, який має прямий вихід на керівництво. Такий варіант характерний для кредитно-фінансових установ, торговельних та посередницьких підприємств регіонального та міжрегіонального рівня, коли основний масив загроз організації пов'язаний із неправомірними діями конкурентів, існує велика загроза інтересів з боку зловмисників. Аналітичну роботу проводять досвідчені фахівці в області недержавної безпеки, які обов’язково досконало володіють знаннями в сфері діяльності організації. Така організація ІАР застосовується практично в усіх банках, страхових компаніях. Головна відмінність від першої моделі полягає в тому, що у першій моделі аналітики - це економісти, маркетологи, фінансисти тощо, а головний фокус лежить на бізнес-ризиках і ринку, тоді як у другій моделі аналітиками є фахівці з безпеки, а головний фокус лежить на загрозах від конкурентів, шахрайстві, витоках даних і злочинних діях.

Третім можливим варіантом організації ІАР є гібридний, який поєднує в собі бізнес-аналітику та безпекову аналітику. Порівняння всіх трьох варіантів представлені в таблиці 1.1. Гібридний варіант — найбільш збалансований, але не завжди саме «кращий» у будь-якій ситуації. Тут важливо враховувати тип організації, масштаб і характер загроз.

Перевагами гібридного варіанту є:

- Комплексність: поєднує бізнес-аналітику (ринок, економічні ризики) і безпекову аналітику (загрози, шахрайство, кібератаки);
- Цілісна картина: керівництво отримує інформацію з двох площин — бізнес та безпека;
- Гнучкість: підходить і для прогнозування ринку, і для реагування на інциденти;
- Сучасність: відповідає викликам цифрової економіки, де бізнес-ризики й інформаційні ризики тісно переплетені.

Недоліками гібридного варіанту ІАР є:

- Вартість: утримання змішаної команди (економісти та фахівці з інформаційної безпеки) дороге;
- Координація: потрібно чітко вибудувати взаємодію між «бізнес-аналітиками» та «безпековими аналітиками», щоб не було конфлікту інтересів;
- Складність управління: подвійне підпорядкування (керівництво + служба безпеки) може ускладнювати процеси.

Тобто гібридний варіант — це універсальний і сучасний підхід, але він найефективніший тоді, коли організація справді має широкий спектр ризиків і достатньо ресурсів. В загальному ж випадку можна стверджувати, що:

- Для **великих корпорацій та транснаціональних компаній** найкращою є гібридна модель, бо охоплює всі ризики;
- Для **середніх організацій** достатньо другого варіанта (ІАР у службі безпеки), оскільки головні ризики там пов'язані із шахрайством і кібератаками;
- Для **виробничих чи ринково орієнтованих корпорацій** може вистачати першого варіанта, де головне — стратегічна економічна аналітика.

Таблиця 1.1. Порівняння моделей ІАР

Критерій	1-й варіант: ІАР у бізнес-підрозділі	2-й варіант: ІАР у службі безпеки	3-й варіант: Гібридна модель
Структурне підпорядкування	Прямо керівництву (аналітичний департамент)	Начальнику служби безпеки	Подвійне: окремий аналітичний центр, що працює і з керівництвом, і зі службою безпеки
Основні фахівці	Економісти, маркетологи, фінансисти	Фахівці з корпоративної та інформаційної безпеки	Змішана команда: економісти, фінансисти, маркетологи, кібер- та ІБ-фахівці
Головний фокус	Ринок, конкуренти, бізнес-ризики	Загрози від зловмисників, шахрайство, витоки	Комплексний: бізнес-ризики та інформаційні та безпекові ризики
Роль служби безпеки	Лише джерело сигналів	Керує аналітикою	Партнер: надає дані для аналізу, але не домінує
Типові сфери застосування	Великі промислові корпорації	Банки, страхові компанії	Транснаціональні корпорації, ІТ-компанії, державні структури
Основні ризики	Конкурентна боротьба, ринкові зміни	Кіберзлочинність, шахрайство	Одночасно бізнес-ризики та кібератаки, витоки, репутаційні загрози

Характер аналітики	Бізнесова, стратегічна	Безпекова, оперативна	Інтегрована: і стратегічна, і оперативна
Приклади результатів	Прогноз попиту, поведінки конкурентів	Виявлення шахрайських схем, зламів	Прогноз ринку та виявлення загроз (єдина аналітична картина для керівництва)

Зазначимо, що гібридна модель не є «сумою» двох попередніх моделей, як може здаватися на перший погляд, оскільки вона забезпечує:

1. Інтеграцію даних:
    - Бізнес-аналітики можуть бачити, що компанія втрачає ринок через нових конкурентів,
    - Аналітики з безпеки бачать зростання атак на бренд у кіберпросторі,
    - Разом: це не дві окремі проблеми, а один комплексний ризик — зниження довіри до компанії, що веде і до фінансових втрат, і до втрат клієнтів.
2. Спільне прогнозування:
    - Економісти прогнозують наслідки коливання валют,
    - Фахівці з інформаційної безпеки прогнозують нові методи шахрайства з картками;
    - Разом вони створюють сценарій: у разі девальвації зростає кількість атак на онлайн-банкінг, клієнти знімають кошти, падає ліквідність.
    - Управлінське рішення комплексного характеру: якщо працювати за окремими моделями, керівництво отримає два різні звіти, а у гібридній моделі аналітики узгоджують висновки і пропонують єдину стратегію, де враховані і бізнес-, і безпекові аспекти.

Таким чином, **суть гібридної моделі – це не «сума»,** а **інтеграція і взаємозбагачення двох перших моделей**:

- Бізнес-аналітики отримують від безпековиків сигнали про «технічні» загрози, які можуть вплинути на ринок;
- Безпековики отримують від економістів контекст, як та чи інша атака вплине на фінансові показники чи репутацію;
- Результат - **єдина картина ризиків**, яку неможливо отримати в межах лише однієї з моделей.

При будь-якій організації роботи ІАР для організації повинна вестися одною структурою. Паралельна аналітична діяльність служби безпеки і організації практично неприпустима. Це пов’язано з тим, що:

- Якщо бізнес-аналітики і служба безпеки працюють окремо, то кожен бачить тільки «свою» частину картини. Це веде до суперечливих висновків і до того, що керівництво отримує різні рекомендації;
- Обидві групи можуть аналізувати схожі дані (наприклад, інформацію про конкурентів), але робити це по-різному. Це збільшує витрати і знижує ефективність;

- Бізнес-підрозділ може вважати, що загрози перебільшені, аби не заважати розвитку ринку, а служба безпеки, навпаки, може наголошувати лише на ризиках, ігноруючи бізнес-аспекти. У результаті — замість синергії виникає конкуренція між аналітичними центрами;
- Якщо керівництво отримує два звіти з різними висновками, воно витрачає час на з'ясування, хто має рацію. У критичній ситуації (кібератака, фінансова криза) це може бути фатально

Ефективність ІАР на конкретному об'єкті залежить не тільки і не стільки від технічного забезпечення і масштабу оброблюваних інформаційних потоків, скільки від чіткої постановки задач і безпосередньої взаємодії зі споживачем аналітичних матеріалів. Жорстко сформулювати вимоги до аналітичних матеріалів досить складно. Найчастіше їх не усвідомлюють і самі замовники, тому визначення інформаційних інтересів конкретного кола споживачів є одним із найскладніших завдань для аналітиків. Уточнення інформаційних потреб зазвичай відбувається в ході самої роботи. Наведемо **приклад** аналітичної роботи в банку під час кібератаки. Припустимо, що має місце ситуація: у великому банку SOC фіксує підозрілу активність: на сервери йде масовий трафік із закордонних IP-адрес. Керівництво ставить первісне завдання аналітичній групі: «Підготуйте інформацію про характер атаки та її ризики для банку», результатом виконання якого стає аналітичний звіт, в якому аналітики описали технічні деталі - тип атаки (DDoS), джерела трафіку, IP-адреси ботнету. Керівництво відповіло: «Це занадто технічно. Нам потрібно знати, чи постраждають клієнти і репутація банку». Наступна ітерація аналітичного звіту прогнозує можливе уповільнення роботи онлайн-банкінгу, ризик скарг клієнтів, витрати на відновлення. Керівництво уточнює задачу: «Зясувати, чи може атака бути прикриттям для спроби проникнення у внутрішню мережу?». Третя ітерація аналітичного звіту: аналітики поєднали технічні дані SOC з OSINT-джерелами і виявили, що в даркнет-форумі обговорюють продаж доступу до банківських систем, результатом чого став звіт, що містив сценарії: DDoS як відволікаючий маневр і паралельна спроба проникнення у внутрішні бази, що вже стало основою для управлінського рішення - посилити контроль доступу і відпрацювати кризовий план. Таким чином, в інформаційній безпеці замовник (керівництво) часто думає у бізнес-категоріях («чи постраждають клієнти?», «чи вплине на репутацію?»), тоді як аналітики мислять технічними деталями. Ефективність ІАР полягає саме в тому, щоб «перекласти» технічну мову в зрозумілу управлінську інформацію, уточнюючи потреби у процесі.

Якість отриманої в результаті аналітичної обробки інформації залежить від кваліфікації аналітика. Тут необхідно враховувати особливості людської психології: часто на підтвердження свого погляду (чи погляду керівництва) відбираються "зручні" дані, а "небажані" недооцінюються, залишаються поза увагою, що може призвести до негативних наслідків. Наприклад, розглянемо таку конкретну ситуацію. У банку SOC виявив підозрілу активність: кілька співробітників завантажували великі обсяги даних у нічний час. Керівництво доручило аналітикам оцінити ризики. Аналітик, який хоче

підтвердити позицію керівництва («це технічна помилка, нічого серйозного»), обирає лише зручні факти: співробітники справді працювали над великим проєктом; вони мали офіційний доступ до даних; підозрілих з'єднань ззовні не зафіксовано, отримуючи висновок: ризиків немає, можна заспокоїти керівництво, який не відповідає дійсності. Об'єктивний аналітик врахує і «незручні» факти: один зі співробітників має зв'язки з конкурентною компанією; на даркнет-форумі за кілька днів до цього з'явилася пропозиція продажу «бази клієнтів українського банку»; логи показують, що копіювання відбувалося не лише з робочих каталогів, а й із систем, до яких співробітник не мав потреби звертатися у своїй роботі, що призводить до висновку: висока ймовірність інсайдерського витоку, потрібне службове розслідування та негайні заходи безпеки.

Досить часто окремі керівники залучають до ІАР колишніх співробітників різних академічних інститутів, що залишилися не при справах. Тут важливо розуміти, що хоча аналітична робота за своєю методологією дуже близька до наукових досліджень, але між ними є дві істотні відмінності (табл.1.2).

Таблиця 1.2. Порівняння: Наукове дослідження та ІАР

Критерій	**Наукове дослідження**	**Інформаційно-аналітична робота (ІАР)**
Мета	Отримати нові знання, сформулювати теорії, пояснити явища	Забезпечити керівництво практичною інформацією для рішень
Часовий горизонт	Дослідження можуть тривати роками	Потрібен швидкий результат, іноді протягом годин/днів
Рівень достовірності	Прагнення до максимальної точності, перевірка гіпотез	Робота з неповними даними, побудова ймовірнісних сценаріїв
Аудиторія	Академічна спільнота, науковці, експерти	Керівництво, менеджери, служби безпеки
Форма подання	Статті, монографії, наукові звіти	Аналітичні записки, короткі довідки, презентації
Стиль викладу	Детально, з повним обґрунтуванням і доказами	Стисло, з акцентом на висновках і рекомендаціях
Ступінь свободи	Дослідник сам обирає тему і глибину	Аналітик працює за запитом/потребами керівництва
Критерій успіху	Внесок у науку, публікації, нові знання	Корисність для управлінського рішення, своєчасність

Таким чином, наука шукає істину у глобальному сенсі, а ІАР шукає інформацію, яка допоможе конкретному керівнику прийняти рішення тут і зараз.

3. Інформація та джерела її отримання

Інформацією називаються будь-які відомості, що отримані при вивченні даного питання і допомагають дати більш повний та обґрунтований ***висновок***.

Слід розрізняти: ***факти*** (дані), ***думки*** (особисті припущення), ***інформацію*** (аналітично опрацьовані дані). Приклад:

Факт: «Продажі компанії зросли на 15% у другому кварталі».

Інформація: «Зростання продажів на 15% свідчить про успішність нової рекламної кампанії».

Думка: «15% — це замало, ми мали вийти хоча б на 25%».

Корисною виявляється будь-яка інформація навіть неперевірена чи та, що не може бути перевіреною, неправдива, неповна та ін., яка може бути використана для отримання обґрунтованого висновку. Тільки отримання максимально можливої в даних умовах інформації дозволяє зробити правильний та обґрунтований аналітичний висновок. Крім того, ця інформація використовується для перевірки надійності джерел інформації, визначення каналів дезінформації і т.д. Для вирішення будь-якої проблеми потрібна оптимальна, якісна, достовірна інформація.

Інформацію прийнято вважати цінною лише тоді, коли її можна використовувати, причому корисність інформації залежить від її повноти, точності та своєчасності.

Інформація дозволяє:

- Орієнтуватися в ситуації;
- Чітко планувати свої дії:
- відстежувати результативність акцій, що проводяться;
- Ухилятися від несподіванок;
- Маніпулювати окремими людьми та угрупованнями.

Існують різні способи класифікації інформації. Так загалом розрізняють два основних види інформації:

- *Біологічна* (ДНК)
- *Соціальна*.

Соціальна інформація представляє найбільший інтерес для дослідження в галузі життєдіяльності суспільства.

Соціальна інформація тісно пов’язана з практичною діяльністю людини, тому тут можна виділити стільки типів і різновидів, скільки є видів діяльності людини.

Прикладами можуть служити політична, військова, естетична, етична, економічна, технологічна (ноу-хау), вимірювальна, науково-технічна інформація. При цьому можливі різноманітні класифікації по різноманітних ознаках. Зокрема соціальна інформація ділиться на два класи:

- масова інформація;
- спеціальна інформація.

Масова інформація адресована всім членам суспільства незалежно від їхнього становища і роду діяльності. Спеціальна інформація адресована не всім членам суспільства, а певним соціальним групам (вченим даної спеціальності, економістам, військовим тощо). Ось найбільш важливі різновиди спеціальної соціальної інформації:

- ***Наукова інформація*** утворюється в результаті науково-технічної діяльності. Наукову інформацію можна визначити як передане в інформаційному процесі наукове знання. Наукова інформація, як і наукове знання, є результатом абстрактно-логічного мислення й адекватно відбиває об'єктивні закономірності, явища і процеси реального світу, суспільства і духовної діяльності людини, вона повинна бути природно отримана науковими методами, що забезпечують істинність знання.
- ***Технічна інформація*** створюється у сфері техніки і призначена для вирішення технічних задач (розробка нових технічних виробів, матеріалів, технологій). Структура і властивості наукової і технічної інформації досить близькі, тому ці два види часто об'єднують терміном «науково-технічна інформація». Проте, розрізняючи науку і техніку як сфери суспільного виробництва, розрізняють й інформаційні процеси, характерні для цих сфер, а також документи, призначені для техніки (патенти, стандарти, комп'ютерні програми, конструкторська документація) або переважно для науки (звіти про науково-дослідні роботи, монографії, теоретичні журнали, збірники наукових праць).
- ***Технологічна інформація*** безпосередньо використовується для створення матеріальних благ. Нові високоефективні технології створюють певний імідж суспільства, держави.
- ***Планово-економічна інформація*** про стан і перспективи розвитку народного господарства використовується для організації планового накопичення і впливу на управління суспільним виробництвом, у тому числі й в умовах ринкових відносин.

Інформація поділяється на:

- ***Тотальну або стратегічну*** (дає загальне оглядове уявлення про проблему та учасників – індивідів та організаторів ситуації) – ця інформація дає підстави приймати рішення про залучення до співпраці, джерелах витоку інформації різних видів секретності, спрямованості об'єкта інтересу, формах залежності та підконтрольності; виносити судження, прогнози у сфері політичних, економічних, комерційних та інших інтересів. Стратегічна інформація дозволяє робити довгострокові прогнози, і це її основне завдання;
- ***Поточну або оперативну (тактичну)*** (тримає в курсі подій, що змінюються) - оперативне встановлення фактів недружніх дій джерел витоку інформації всередині організації, сумлінності потенційних партнерів тощо. Оперативна інформація дійсна протягом певного проміжку часу та дозволяє скоригувати діяльність організації та служби безпеки шляхом видачі короткострокових прогнозів або прогнозів на задану операцію;

- ***Конкретну або сигнальну*** (заповнює виявлені прогалини у даних чи відповідає на певні питання) - достовірно вказує та підтверджує події, які мають відбутися, сигналізує про погрози, дозволяє достовірно визначити їх та вжити відповідних контрзаходів;
- ***Непряму*** (підтверджує або спростовує деякі припущення, будучи стикованою з останніми даними лише опосередковано);
- ***Оціночну*** (***доказову***) (розтлумачує події та дає прогноз щодо їх розвитку у майбутньому; це – оптимально оброблені дані) – дозволяє з великою часткою ймовірності довести зв'язки між подіями, об'єктами та ін. Використовується для створення таблиці зв'язків об'єкта, а також при аналітичному розслідуванні фактів витоку інформації тощо.

До основних **якісних** характеристик інформації слід віднести: ***достовірність*** (коректність), ***об'єктивність***, ***однозначність***, ***достовірність джерела*** (чистота) та ***порядок інформації***. Розглянемо кожну характеристику докладніше.

Достовірність (коректність) інформації – міра наближеності інформації до першоджерела чи точність передачі. Тут часто зустрічається той факт, що інформація, передана через третіх осіб в усній формі, мало відповідає як дійсності, а й вихідній інформації. При цьому першоджерело – це або сама подія/факт, що реально відбулося, або документ/джерело, максимально близьке до цієї події. Тобто достовірність означає, наскільки відображення цієї події в інформації відповідає дійсності. Чим менше спотворень при передачі, тим вища достовірність. Наприклад, першоджерело (подія): у місті відбувся мітинг на 2000 осіб. Джерело А (журналіст) повідомляє про 1900–2100 учасників. Джерело Б (чутки в соцмережах): «близько 20 000». Інформація з джерела А достовірніша, бо вона ближче до реального стану справ.

Основні фактори, що знижують достовірність інформації — тобто віддаляють її від першоджерела:

1. Людський фактор:
   - суб’єктивність: автор може мати власні інтереси чи упередження.
   - помилки сприйняття: неточності при спостереженні або запам’ятовуванні. В прикладі журналіст Б міг завищити кількість учасників мітингу, бо стояв на ділянці з більшою щільністю людей.
2. Джерело інформації:
   - надійність джерела: офіційні дані зазвичай достовірніші, ніж анонімні публікації;
   - зацікавленість: джерело може спеціально прикрашати або приховувати факти. Приклад: конкурент пише у ЗМІ, що «банк Х зазнав масового відтоку клієнтів», хоча цифри перебільшені для дискредитації.
3. Канал передачі:
   - Технічні спотворення: неточності через помилки комунікації, переклад, шум;
   - Маніпуляція при передачі: свідоме редагування тексту або відбір вигідних фактів. Приклад: у новині залишили лише драматичний фрагмент виступу політика, вирваний з контексту.
4. Обробка інформації:
   - Стиснення та узагальнення: при скороченні губляться важливі деталі;

- Вибірковість: аналітик може відкинути «незручні» дані. Приклад: у зведенні новин не згадали про мирні переговори, а лише про сутички.

5. Часовий фактор:
   - Застарівання: інформація з часом може втратити актуальність. Приклад: дані про фінансовий стан компанії за минулий рік уже не відображають поточну ситуацію.

Об'єктивність інформації – міра відображення інформацією реальності, це властивість інформації відображати реальний стан речей незалежно від поглядів, емоцій, інтересів чи упереджень того, хто її подає або сприймає.. В оперативному плані має на увазі інформацію, очищену від спотворень. Після процедур очищення багато фахівців схильні приписувати отриманій інформації стовідсоткову придатність для використання. Це неправомірно, оскільки об'єктивність у світі отримування інформації непроста: у будь-якій справі правд може бути безліч. Оцінювати об'єктивність інформації можна лише у ймовірнісних джерелах: «ймовірно…, ймовірно…, малоймовірно…» тощо.

Однозначність – поряд з об'єктивністю інформація має бути однозначною (табл.1.3). Однозначність інформації означає таку властивість повідомлення, коли воно інтерпретується однаково всіма користувачами, незалежно від їхнього досвіду чи контексту. Зауважимо, що достовірна інформація, навіть якщо вона є об'єктивною, не завжди є придатною для остаточних висновків та рішень. Достовірна й навіть об’єктивна інформація може виявитися недостатньою для прийняття остаточних рішень, якщо вона не має однозначності.

1. Брак конкретики: інформація може бути достовірною, але занадто загальною. Приклад: «Зростає кількість кіберзагроз у регіоні» — це правда й об’єктивно, але без уточнення «які саме загрози, коли, проти кого» рішення ухвалити неможливо.
2. Множинність інтерпретацій: навіть точні факти можуть мати різні трактування, якщо вони подані неоднозначно. Приклад: «Рівень безробіття виріс на 5%» — достовірний факт, але чи це результат кризи, чи сезонний фактор, чи зміна методики підрахунку? Без уточнень висновки будуть ризикованими.
3. Відсутність зв’язку з проблемою: інформація може бути об’єктивною, але не релевантною конкретному завданню. Приклад: для завдання оцінити ризики атаки на банк об’єктивна статистика злочинності у місті корисна лише частково — вона не дає прямої відповіді.
4. Складність прийняття рішень: рішення завжди потребує не лише факту, а й його чіткого формулювання, без подвійних смислів. Якщо інформація не однозначна, її можна трактувати різними способами, що створює простір для помилок.

Таблиця 1.3. Відмінність між однозначною і неоднозначною інформацією

Критерій	Однозначна інформація	Неоднозначна інформація
Сенс	Єдиний, чіткий, зрозумілий усім	Допускає кілька тлумачень

	однаково	
Приклад формулювання	«Температура в кімнаті 22°C»	«У кімнаті прохолодно»
Форма подання	Стандартизовані дані: числа, коди, точні терміни	Оціночні судження, метафори, загальні слова
Приклад у часі	«Зустріч о 14:00 у каб. 301»	«Зустрінемось після обіду»
Наслідки для роботи	Зменшує ризик помилок і непорозумінь	Може призвести до різних інтерпретацій і неправильних рішень
Використання в ІБ та аналітиці	Базис для точних моделей і прогнозів	Потребує уточнення або перекладу в однозначну форму

Достовірність джерела (чистота) інформації – це ступінь наближеності джерела до місця створення інформації. Достовірність джерела часто підмінюється рівнем довіри, що суб'єктивно склався між вами. Абсолютно достовірної інформації від джерела немає: джерело може володіти лише інформацією, доступом до якої має (іноді авторитет джерела підміняє його реальні можливості); не володіючи спеціальними знаннями, джерело може стати жертвою дезінформації чи зловмисного обману з боку третьої особи.

Очевидці події (прямі свідки) - високий рівень достовірності джерела;

Другорядні перекази («мені сказали, що він бачив…») - нижчий рівень, бо є проміжна ланка;

Чутки («кажуть, що десь відбулося…») - дуже низька достовірність, бо джерело віддалене від першоджерела.

Достовірність джерела - наскільки близько воно до створення інформації (об’єктивна міра); рівень довіри - ваша суб’єктивна думка про це джерело (може бути хибною).

Алгоритм оцінки достовірності джерела

1. Хто створив інформацію?
- Чи є джерело очевидцем події або учасником процесу?
- Чи воно лише переказує чужі слова?
2. Наскільки джерело компетентне в темі?
- Чи має воно спеціальні знання/доступ? Наприклад, лікар про діагноз достовірніше, ніж випадковий знайомий.
3. Ланцюжок передачі.
- Скільки «рук» пройшла інформація, перш ніж потрапила до вас?
4. Наявність підтверджень.
- Чи співпадає інформація з іншими незалежними першоджерелами? Якщо кілька незалежних свідків кажуть одне й те саме, достовірність вища.

Порядок інформації визначається в залежності від кількості передавальних ланок між джерелом та вами. Інформація може бути першого

(найвищого) порядку, другого, третього і нижчого. У міру падіння висоти порядку знижується і достовірність.

Кількісні характеристики інформації включають: ***повноту інформації та релевантність***.

Повнота інформації - відображає вичерпний характер відповідності отриманих відомостей цілям збору інформації, тобто ступінь, у якій інформація охоплює всі аспекти об'єкта чи події, необхідні для прийняття рішення (наскільки «картина світу» є цілісною). Якщо інформація фрагментарна — рішення може бути помилковим. Зауважимо, що повнота майже ніколи не досягає 100%, аналітик завжди працює з «обмеженою картиною». Формально кількісно з деяким ступенем наближення повноту можна розраховувати, як відношення кількості отриманих відомостей до загальної кількісті необхідних відомостей.

Релевантність інформації - ступінь наближення інформації до суті питання та ступінь відповідності інформації поставленому завданню її збору. В кількісному плані представляє частку необхідної інформації у загальному обсязі отриманої.

Ціннісні характеристики інформації: ***вартість та актуальність*** інформації.

Вартість інформації - оцінка цінності інформації для організації у порівнянні з витратами на її отримання та можливими втратами у разі відсутності цієї інформації («Чи варта інформація витрачених ресурсів?»).

Приклади:

- звіт аналітичної компанії коштує $10 000. Завдяки йому компанія ухиляється від угоди, яка могла б принести збиток $1 млн. Вартість цієї інформації — дуже висока, адже вона перевищує витрати на її отримання.
- Служба безпеки купує доступ до threat intelligence-платформи. Вартість підписки — $50 000 на рік, але завдяки цій інформації вчасно виявляють атаку, яка могла призвести до витрат у $5 млн, тобто інформація має високу цінність, бо захищає від великих збитків.

Актуальність інформації - ступінь відповідності інформації поточному моменту й своєчасності її використання. Навіть цінна інформація втрачає сенс, якщо вона застаріла.

Приклад: інформація про курси валют тижневої давності вже малоактуальна для трейдера, а от дані про курс «на зараз» — актуальні й цінні.

В процесі проведенні ІАР необхідно отримати відповіді на наступні питання:

- Що потрібно дізнатися?
- Де і в якому вигляді може бути потрібна інформація?
- Хто нею може мати чи може дістати?
- Як і в якому вигляді її можна отримати?

Відповіді ці питання забезпечують розуміння техніки вирішення задачі. Виходячи з цього необхідно:

- оцінити інформацію (за ступенем достовірності, важливості, секретності, стикуваності, можливості використання);

- інтерпретувати (у світлі інших даних та глибинної інтуїції), виявивши її місце у загальній картині фактів;
- визначити, чи необхідна і яка саме додаткова інформація;
- ефективно використати (врахувати в планах, передати інформацію потрібному адресатові або притримати до потрібного моменту…).

4.Інформаційна розвідка

Отримання інформації може відбуватися за допомогою розвідки. Між цими двома процесами є відмінності. Отримання інформації - це процес збору даних (будь-яких, навіть випадкових), при тому, що розвідка - це спеціально організований пошук потрібних даних з подальшою аналітикою.

Для ефективного вирішення проблем ІАР необхідно добре уявляти сенс отримання інформації (розвідувальної діяльності), її характеристики, методи, види і т.д.

Сенс розвідки полягає в наступному:

- Видобування та отримання інформації для прийняття рішень (стратегічних, оперативних або тактичних) у відповідних сферах діяльності;
- Отримання переваги над передбачуваним противником з урахуванням використання у своїх цілях його науково-технічних, технологічних та інших досягнень.

Розвідці притаманні такі характеристики:

1. Розвідка носить номінальний характер стосовно підвищення достовірності видобутої інформації, тобто сама по собі розвідка не гарантує абсолютної істини. Вона підвищує рівень впевненості у даних, але завжди залишається певний відсоток неповноти чи помилки;

2. Розвідка діє ешелоновано, тобто процес здобуття й обробки інформації відбувається **поетапно, у кілька рівнів**, де кожен наступний рівень уточнює, перевіряє й поглиблює результати попереднього, що дозволяє проводити детальну розвідку. На практиці це можна представити в такий спосіб:

Перший ешелон – збір «сирих даних» для створення загальної картини ситуації. Відбувається збір усіх доступних сигналів: відкриті джерела (OSINT), технічні логи, повідомлення CERT, чутки. Наприклад, SOC фіксує 1000 спроб входу до корпоративної пошти з підозрілих IP.

Другий ешелон – попередній аналіз і відсів «шуму». Тут відбувається відокремлення другорядного від важливого, видалення помилкових спрацювань. Наприклад, з 1000 спроб входу лише 50 виглядають організованою атакою, решта — випадковий трафік.

Третій ешелон – глибинна перевірка і кореляція. Відбувається залучення спеціальних методів: моніторинг даркнету, аналіз шкідливого коду, агентурні джерела. Наприклад, аналітики знаходять у даркнеті повідомлення тієї самої групи, яка стоїть за атаками на пошту.

Четвертий ешелон – інтегрований аналітичний продукт. Формування єдиного висновку для керівництва: сценарії, оцінка ризиків, рекомендації. Наприклад, «З високою ймовірністю група X готує атаку на онлайн-банкінг; необхідно вжити заходів Y і Z».

Таким чином, розвідка не діє «одним ударом». Вона будує **багаторівневу систему уточнення даних**. Кожен ешелон підвищує достовірність і корисність інформації.

3. Розвідка має координований характер, тобто вона діє як **система з єдиним управлінням**, усі джерела та канали працюють **узгоджено**, кінцевий продукт подається керівництву як **єдина картина ризиків і загроз**. Це є дуже важливою характеристикою розвідки. Інакше може відбуватися наступне: різні підрозділи можуть збирати **одне й те саме**, або навіть давати керівництву суперечливі звіти. Координація ж забезпечує **узгодженість дій** (ніхто не заважає іншому), **повноту** (кожен закриває свою частину завдання), **оперативність** (інформація сходиться в одному центрі), **економію ресурсів** (немає дублювання роботи).

4. Розвідка має глобальний характер. Розуміння цього має декілька аспектів:

- **Всеосяжність джерел:** Розвідка працює не лише з «місцевими» чи внутрішніми даними, а охоплює відкриті джерела - ЗМІ, соціальні мережі, бази даних; закриті джерела: агентурні мережі, даркнет, спеціалізовані форуми; технічні дані з різних країн (шкідливі програми, інфраструктура атак). Наприклад: кіберзагроза може виникнути в одній країні, але вразити компанію в іншій.
- **Відсутність кордонів для** загроз: кібератаки можуть запускатися з будь-якої точки світу; інформаційні кампанії в соцмережах поширюються миттєво; ринкові ризики й економічні кризи мають глобальний ефект.
- Розвідка враховує вплив різних сфер: політика (санкції, міжнародні відносини), економіка (світові ринки, ціни на ресурси), технології (нові методи атак, тренди в IT), соціальна сфера (суспільні настрої, репутаційні ризики). Наприклад, для компанії, що працює з енергоресурсами, аналітикам потрібно відслідковувати і кібератаки, і зміни цін на нафту, і геополітичні конфлікти;
- Мережевий обмін інформацією: розвідка не може бути ізольованою, компанії й державні структури обмінюються даними; аналітичні групи використовують міжнародні бази індикаторів компрометації, тобто розвідка має глобальну взаємопов’язаність.

Глобальний характер розвідки означає, що навіть локальна подія (атака на один банк) має бути розглянута у міжнародному контексті, бо загроза може бути частиною світової злочинної інфраструктури, значної широкої злочинної операції.

5. Розвідка спрямована насамперед на особливо важливі об'єкти.

Розвідцикл (intelligence cycle) — це класична модель, яка описує повний процес роботи розвідки, від появи потреби в інформації до використання результатів у прийнятті рішень. У класичному розумінні розвідцикл прийнято ділити на основні частини:

1. Планування та цілевказівку (керівництво формулює, які дані потрібні: «Чи готує конкурент інформаційну атаку?», «Чи є ознаки кібератаки на наш банк?»; визначаються пріоритети та ресурси);

2. Збирання-добування даних (Використовуються всі можливі джерела: відкриті (OSINT), технічні (SOC, лог-файли, сенсори), агентурні (HUMINT), спеціалізовані (даркнет-розвідка);

3.Обробка розвідданих (сирі дані очищаються від «шуму», структуруються, перетворюються у придатний для аналізу формат (наприклад: із 1000 подій у логах SOC відсіюють 950 випадкових спроб, лишають 50 підозрілих);

4. Аналіз та синтез розвідувальної інформації (аналітики співставляють факти, шукають закономірності, формують сценарії, в результаті чого отримуються не просто дані, а інформація з висновками, прогнозами та рекомендаціями);

5. Поширення (готовий аналітичний продукт передається керівництву або замовнику в зручній формі: аналітична записка, презентація тощо);

6. Зворотний зв'язок (керівництво оцінює корисність матеріалу і може скоригувати нові завдання). Цей крок замикає цикл і запускає новий виток роботи.

У світі роль розвідки надзвичайно висока, що необхідно враховувати під час розробки заходів з інформаційної безпеки. Сьогодні будь-які серйозні заходи, які проводяться в життя державами, корпораціями, а часом і злочинними спільнотами, починаються зі збору інформації про потенційного супротивника для її подальшого аналізу та прийняття рішення.

Необхідно відзначити, що за рівнем доступу та режимом використання інформація розподіляється на: **відкриту, напівзакриту та секретну**.

Відкрита інформація доступна всім без обмежень, поширюється офіційно або публічно; її джерелами є сайти, ЗМІ, наукові публікації, відкриті державні реєстри, соціальні мережі. Така інформація використовується в аналітичній роботі як **OSINT (Open Source Intelligence)**. Приклади відкритої інформації:

- Новини про зміни законодавства.
- Відкритий звіт компанії за рік.
- Пости клієнтів у соцмережах.

Напівзакрита інформація - інформація з обмеженим доступом, яка не є публічною, але й не становить державної чи комерційної таємниці. Доступ мають лише певні групи осіб (за реєстрацією, підпискою, договором, членством). Використовується для роботи фахівців, але потребує **регламентованого обігу**. Приклади напівзакритої інформації:

- Внутрішні методичні матеріали компанії.
- Бази даних, доступні лише зареєстрованим користувачам.
- Інформація, отримана в рамках партнерських угод чи платних сервісів.

Секретна інформація - дані, доступ до яких суворо обмежений законом або внутрішніми політиками організації; несанкціоноване розголошення може призвести до серйозних наслідків (економічних, політичних, репутаційних чи навіть кримінальних); має спеціальні режими захисту: гриф «таємно», технічні засоби безпеки. Приклади секретної інформації:

- Державна таємниця (військові плани, коди урядового зв'язку).
- Комерційна таємниця (рецептура Coca-Cola, алгоритми Google).
- Персональні дані клієнтів банку.

Розвідка спрямована насамперед на добування секретної інформації, проте розвідка не нехтує і відкритою інформацією: вона може отримувати секретну інформацію на основі збору та аналізу великого обсягу конфіденційної або навіть відкритої інформації. Саме тому роль розвідки в сучасному світі є надзвичайно високою, що необхідно обов'язково враховувати при розробці заходів з інформаційної безпеки. Сьогодні будь-які серйозні заходи, які проводяться державою, корпораціями, а часом і злочинними спільнотами, починаються зі збору інформації про потенційного супротивника для її подальшого аналізу та прийняття рішення.

Напівзакриту та секретну інформацію можна отримати з різноманітних джерел, більшу частину яких недосвідчена людина не бере до уваги. Слід враховувати найнеймовірніші можливості, хоч би якими нереалістичними вони не здавалися. Для цього необхідно виявити головні носії інформації, якими є:

- знаючі люди;
- документи;
- засоби бездротового та провідного зв'язку;
- електронні та паперові носії інформації;
- різні відстежуючі можливості (наведення, розмови, результати дій тощо).

Вийшовши на те чи інше джерело інформації, необхідно визначити:

- його наявні та потенційні можливості;
- допустимі межі використання;
- ступінь його надійності.

Методи отримання інформації

Для отримання інформації можуть використовуватись **легальні, напівлегальні та нелегальні методи.**

Легальні методи - офіційні та законні способи отримання інформації, які не порушують законодавства й прав інших осіб. Використовуються в **OSINT** та корпоративній аналітиці. До ***легальних*** методів належать: вивчення публікацій у засобах масової інформації, офіційних звітів і реєстрів; аналіз сайтів конкурентів; отримання статистики від державних органів; підписка на платні аналітичні платформи; участь у науково-технічних конференціях; аналіз суспільно-політичних, наукових та технічних видань; відвідування виставок, дослідження повідомлень електронних ЗМІ (телебачення, радіо, Інтернет та ін.).

Напівлегальні методи - методи, які прямо не заборонені, але можуть порушувати етичні норми, угоди чи внутрішні правила, і в окремих випадках призводять до юридичної відповідальності. Зазвичай це - «сіра зона» між дозволеним і забороненим, може зіпсувати репутацію або викликати претензії (цивільні позови, штрафи). До ***напівлегальних*** методів можна, зокрема, віднести: бесіди із співробітниками у неофіційній обстановці; уявні переговори щодо купівлі продукції; неправдиві конкурси; запрошення на роботу провідних спеціалістів; отримання інформації від загальних постачальників, споживачів, через фонди та благодійні організації, через контролюючі органи, використання фейкових акаунтів у соцмережах для збору інформації про конкурента; «соціальна інженерія» у вигляді «незначного» обману (наприклад, телефонний дзвінок від імені «журналіста», щоб отримати коментар) та ін.

Нелегальні методи - дії, які прямо порушують закон і можуть призвести до кримінальної відповідальності. Використовуються злочинними угрупованнями, іноді — державними спецслужбами.

До ***нелегальних*** методів належать: несанкціоноване проникнення в інформаційні системи (хакінг); підкуп співробітників для отримання конфіденційних даних; перехоплення приватних комунікацій; крадіжка документів чи носіїв інформації; викрадення образів продукції та/або технологічного обладнання; та ін. Для комерційних структур використання таких методів практично неприпустиме, бо загрожує серйозними санкціями.

Інформаційна безпека

Способи застосування засобів захисту в заходах щодо забезпечення інформаційної безпеки залежить від типу інформації, форми її зберігання, обробки та передачі, типу носія інформації, а також передбачуваного способу нападу та досліджень наслідків, його вплив на інформацію (копіювання, спотворення, знищення).

Досвід застосування систем захисту інформації показує, що ефективним може бути лише комплексний захист, що забезпечується наступними заходами:

- Законодавчі. Використання законодавчих актів, що регламентують права та обов'язки фізичних та юридичних осіб, а також держави в галузі інформаційної безпеки;
- Морально-етичні. Створення та підтримка на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників різко негативно;
- Фізичні. Створення фізичних перешкод для доступу сторонніх осіб до об'єкта інформації, що охороняється;
- Адміністративні. Організація відповідного режиму секретності, пропускного та внутрішньооб'єктового режиму;
- Технічні. застосування електронних технічних та інших пристроїв для захисту інформації;
- Криптографічні та стеганографічні. Застосування шифрування та кодування для приховування оброблюваної та інформації, що передається, від несанкціонованого доступу;
- Програмні. Застосування програмних засобів для забезпечення інформаційної безпеки та розмежування доступу до інформації.

Відповідно вивченню цих заходів приділяється певна наукова увага.

Сучасні досягнення в галузі інформаційної безпеки дозволяють по праву віднести її до наукового напряму теорії інформації. У найзагальнішому випадку інформаційна безпека — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Більш розгорнуте формулювання інформаційної безпеки — це стан захищеності потреб в інформації особистості, суспільства і держави, при якому **забезпечується їх існування і прогресивний розвиток** незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином:

- як забезпечення стану захищеності особистості, суспільства, держави від **впливу неякісної інформації**;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

Систематизація знань з наукової проблеми інформаційної безпеки, узагальнення теоретичних та технічних рішень дає можливість сформулювати сутність предметної галузі інформаційної безпеки:

1. Аналіз інформаційних процесів в інформаційних системах, включаючи пошук, збирання, накопичення, обробку та подання інформації, визначення та формування параметрів та характеристик інформаційного простору, що містять відомості та дані про об'єкт захисту;

2. Аналіз та оцінку можливості несанкціонованого доступу до інформаційної системи всередині та поза контрольованою зоною з урахуванням особливостей об'єкта та характеристик можливих каналів витоку інформації;

3. Встановлення каналів витоку інформації шляхом отримання відомостей про параметри інформаційних сигналів, що охороняються, про об'єкт за допомогою вилучення цих сигналів з інформаційних полів різної фізичної природи;

4. Встановлення каналів витоку інформації, одержуваних з допомогою наведень сигналів на неінформаційні ланцюги, які йдуть за межі контрольованого простору, оцінка їх параметрів і виділення змістовної інформації;

5. Класифікація та моделі можливих систем та засобів перехоплення сигналів та полів різної фізичної природи, засобів обробки сигналів.

У відповідності з вищенаведеним ***алгоритм проведення робіт по захисту інформації на об'єкті*** є наступним:

1. Визначити, чи є на об'єкті інформація, яку необхідно захистити, який ступінь захисту повинен бути забезпечений.

2. Визначити обсяг коштів, необхідних для забезпечення заданого рівня захисту.

3. Виявити або спрогнозувати всі загрози безпеці та можливі канали витоку інформації.

4. Провести аналіз заходів щодо захисту інформації об'єкта.

Комплекс проблем у сфері інформаційної безпеки можна умовно розбити на 4 групи: ***правові, технічні, організаційні, нормативно-методичні***.

Правові проблеми пов'язані з недосконалістю правової бази, що суттєво ускладнює, наприклад, розгортання діяльності в галузі технічного захисту інформації (приклад??)

Технічні проблеми. Розвиток технічних засобів розвідки базується, як правило, на останніх досягненнях науки, техніки, технологій. Тому засоби протидії, зокрема засоби технічного захисту інформації повинні створюватися з урахуванням цієї обставини.

Організаційні проблеми. Фахівець з питань інформаційної безпеки повинен мати високий рівень кваліфікації та володіти широким спектром знань. Кваліфікаційне забезпечення комплексної безпеки інформації вимагає від

спеціаліста знань у галузі політики, радіотехніки, радіоелектроніки, обчислювальної техніки, хімії, принципів побудови систем різного призначення та іншої спеціальної техніки та основ застосування тощо. Різнорідність областей знань унеможливлює підготовку фахівців з інформаційної безпеки на базі одного університету.

Нормативно-методичні проблеми. Закони та підзаконні акти складають верхній ешелон документів, що регламентують правові відносини у сфері безпеки. Вони концептуально визначають підходи до технології захисту інформації. Основний зміст робіт з інформаційної безпеки та технічного захисту інформації, щодо контролю за їх ефективністю викладається в спеціальній нормативно-технічній документації. Актуальним завданням тут є створення науково-обґрунтованої системи нормативно-технічних документів.

На підставі всього викладеного очевидною є необхідність використання системного комплексного підходу до забезпечення безпеки інформації, про який вже говорилося вище. Він передбачає побудову системи захисту з комплексним використанням основних методів та засобів захисту. При цьому безперервність захисту розуміється не тільки у сенсі безперервності функціонування системи, а й у сенсі безперервності запровадження заходів для їх вдосконалення, оскільки будь-яка система захисту не є абсолютно надійною. З цією метою необхідно здійснювати постійний контроль за роботою системи захисту та на підставі даних цього контролю проводити періодичну перевірку безпеки, що включає:

- оцінку ефективності використання заходів захисту;
- оцінку необхідності впровадження додаткових заходів захисту;
- вибір та реалізацію нових сфер захисту.

Це дозволяє постійно підтримувати ефективність захисту на належному і заданому рівні.

5. Зміст інформаційної та аналітичної роботи

Завдання інформаційно-аналітичного забезпечення органів управління інформацією є одним із пріоритетних завдань, від якості вирішення якого залежить політична, військова, соціальна, економічна стабільність держави та суспільства. В інтересах вирішення цього завдання інформаційно-аналітичними службами, що належать різним відомствам та організаціям, здійснюється аналітична обробка масивів даних. Джерелами таких даних є іноземні та вітчизняні інформаційні агентства, здійснюють збір та аналіз інформації, органи різної відомчої належності, органи державного та військового управління, а також інші суб'єкти, які продукують інформацію, що становить інтерес для ефективного управління.

Інформаційна робота - діяльність із забезпечення зацікавлених осіб відомостями, необхідними для рішення покладених ними завдань. Процес інформаційної роботи - це послідовна сукупність операцій (реєстрація, передача, накопичення, зберігання, обробка, видача інформації), що дозволяє швидко знайти в повному обсязі необхідні відомості, затребувані конкретними споживачами.

Аналітична робота призначена для оцінки інформації, підготовки прийняття рішень. Зміст аналітичної роботи - приведення розрізнених

відомостей у логічно обгрунтовану систему залежностей (просторово-часових, причинно-наслідкових та інших), що дозволяють дати правильну оцінку як усієї сукупності фактів, так і кожному з них окремо.

Засоби аналітичної роботи - це закони та методи розумової діяльності, а також інші технічні засоби, на основі та за допомогою яких здійснюється обробка фактичних даних. Процес аналітичної роботи - це сукупність операцій, здійснюваних у певній послідовності з використанням аналітичних засобів, що призводять до досягнення цілей та завдань роботи.

Відмінності між інформаційною та аналітичною роботою представлені в табл.1.3.

Таблиця 1.3. Порівняльна таблиця

Критерій	Інформаційна робота	Аналітична робота
Сутність	Збір, систематизація й збереження даних	Обробка даних, їхнє узагальнення та інтерпретація
Предмет	Факти, документи, повідомлення, статистика	Висновки, закономірності, сценарії, рекомендації
Питання, на яке відповідає	«Що ми маємо?»	«Що це означає?» та «Що робити?»
Методи	Моніторинг ЗМІ, робота з базами даних, спостереження, документування	Порівняння, класифікація, кореляція, прогнозування, моделювання
Засоби	Пошукові системи, бази даних, архіви, новинні агрегатори, системи збору логів (SOC)	Аналітичні платформи (BI-системи, Threat Intelligence, SIEM), статистичні пакети, системи візуалізації, методики SWOT, PEST, сценарний аналіз
Результат	Інформаційний масив (база даних, архів, зведення фактів)	Аналітичний продукт (записка, звіт, прогноз, рекомендація)
Користувач	Внутрішні підрозділи, які накопичують інформацію	Керівництво, яке приймає рішення
Приклад у бізнесі	Зібрано дані про ціни конкурентів	Висновок: «через місяць конкурент знизить ціни, потрібно переглянути стратегію»
Приклад в ІБ	SOC зібрав 1000 логів спроб входу	Аналітик: «50 з них належать до цілеспрямованої атаки групи X, мета — викрадення даних»

Таким чином, і**нформаційна робота** — це «заготовка», а**налітична робота** — це «готовий продукт для управлінського рішення».

6. Методи, закони та правила, що застосовуються в ІАР

Розглянемо основні з методів, законів та правил, що застосовуються в інформаційній та аналітичній роботі.

Одним з найбільш корисних методів в інформаційній, а також аналітичній роботі є метод аналогій.

Метод аналогій — це спосіб мислення «за зразком», який дозволяє аналітику використати досвід минулих подій для прогнозу майбутніх. Суть методу аналогій полягає в умовному перенесенні властивостей або закономірностей, виявлених в одному об'єкті (ситуації), на інший подібний об'єкт, припускаючи, що якщо явища мають спільні риси, вони будуть мати й подібні наслідки. Застосовувати Метод аналогій потрібно обережно й у поєднанні з іншими методами: аналогія не дає 100% гарантії, бо схожість ситуацій може бути лише поверхневою.

Метод вивчення окремих подій — це ще один з основних підходів в інформаційній та аналітичній роботі. Він полягає у глибокому дослідженні конкретної події, що відбулася, для виявлення її причин, учасників, наслідків і можливих повторень. На відміну від статистичного аналізу (який розглядається нижче і працює з масивом даних), цей метод концентрується на одиничному випадку, але розглядає його максимально детально, тобто дає глибоке розуміння конкретної ситуації, надає матеріал для методу аналогій (порівняння з іншими подіями). Недоліком цього методу є те, що він може виявитися надто вузьким: аналіз однієї події не завжди відображає загальну картину, потребує перевірки того, чи є подія типовою, чи винятковою.

Один з ключових інструментів в інформаційній та аналітичній роботі - **метод статистичного аналізу -** дослідження масивів даних для виявлення закономірностей, тенденцій і аномалій. Статистичний аналіз працює з великою кількістю спостережень, результатом чого є кількісні характеристики подій, що розглядаються (середні значення, частоти, ймовірності), які допомагають робити висновки й прогнози. І хоча цей метод дозволяє працювати з великими масивами даних, дає кількісні виміри, що знижує суб'єктивність, дає основу для прогнозів, він має значні недоліки: вимагає якісної бази даних (інакше статистика буде викривлена), не враховує унікальних обставин (може «розмити» поодинокі, але важливі події).

Хоча згадані методи різні, вони доповнюють один одного. В кожному дослідженні можна скоріш досягти успіху, якщо застосовувати окремі елементи різних методів.

Незважаючи на те, що завдання ІАР різні, існують деякі закономірності у плануванні часу на їх вирішення. Рекомендується витрачати трохи більше 50-60% часу на інфоомаційну роботу (збір " сирої " інформації). Решта часу розподіляється між обробкою цієї інформації (30-40%) та складання звіту (10-20%). В ІАР існує неписане правило: "Правильність важливіша за точність", яке означає, що якщо фахівець отримав інформацію з декількох джерел, перевіряв її ще раз і отримав у всіх випадках однаковий результат, що дозволяє

сформувати дані, то немає необхідності витрачати час на дослідження інших джерел.

ІАР відрізняється від будь-якої іншої роботи насамперед своєю логічністю, використовуючи логічні закони, серед яких найбільш поширені такі.

1. Закон причинно-наслідкових зв'язків - кожна подія у матеріальному світі має причину та тягне за собою слідство.

2. Закон форми та змісту - однаковість форми не передбачає однаковості змісту.

3. Закон тотожності - обсяг і зміст думок про якийсь предмет повинні бути суворо визначені та залишатися постійними у процесі міркування про нього.

4. Закон протиріччя - не можна одночасно затверджувати і заперечувати будь-що у відношенні до того чи іншого об'єкта (в одному місці та в один час). Інакше судження неможливо знайти одночасно істинними.

5. Закон виключення третього – кожне висловлювання може бути або істинним, або хибним, третього не дано.

6. Закон достатньої підстави - будь-яка справжня інформація має достатню підставу, якою може бути будь-яка інша інформація, з якої необхідно випливає істинність цієї інформації.

На основі логічних законів формулюються правила ІАР:

1. Правило формулювання мети - необхідно визначити, для яких цілей буде використано результати ІАР. Від цього залежить масштаб, методи та способи вирішення задачі. Перед аналітиком мають бути поставлені конкретні цілі.

2. Правило визначення понять - точне визначення сенсу кожного терміна, що використовується в ІАР. По суті, це закон тотожності.

3. Правило використання всіх можливих джерел інформації з цієї тематики. Аналітику доводиться працювати з інформацією, яку він має на даний момент, не чекаючи інформації від кожного джерела, втрачаючи при цьому час.

4. Правило інтерпретації фактів - розкриття сенсу значення фактів чи подій, зіставлення їх із аналогічними, що мали місце раніше.

5. Правило встановлення причинно-наслідкових зв'язків - встановлення причини події або факту, що розглядається, і виділення його слідства.

6. Правило визначення тенденцій розвитку подій - визначення можливих шляхів розвитку події, сигнальних подій кожному за варіанта розвитку, своїх майбутніх действий.

7. Правило коригування висновків – не допускає довільності висновків. Висновки мають підтверджуватись інформацією. У висновку необхідно мати відповідь на поставлене запитання або завдання.

Питання

1. Визначення інформаційно-аналітичної роботи. Етапи ІАР та їх характеристика
2. Задачі ІАР в області захисту інформації.

3. Моделі організації ІАР на об’єкті. Характеристики, переваги, недоліки кожної.
4. Поясніть, чому при будь-якій організації роботи ІАР для організації повинна вестися одною структурою.
5. Від чого, головним чином, залежить ефективність ІАР на конкретному об’єкті? Обгрунтуйте свою думку.
6. Чим відрізняються класичні наукові дослідження і ІАР?
7. Джерела та методи отримання інформації, їх класифікація.
8. Стратегічна, оперативна, непряма, оціночна інформація: визначення, приклади.
9. Якісні характеристики інформації: достовірність, об'єктивність, однозначність, достовірність джерела, порядок інформації.
10. «Алгоритм» оцінки достовірності джерела.
11. Кількісні характеристики інформації.
12. Розподіл інформації за рівнем доступу та режимом використання: відкрита, напівзакрита та секретна інформація.
13. Пояснити, якими заходами забезпечується комплексний ЗІ.
14. Пояснити, в чому полягає зміст інформаційної та аналітичної роботи.

ТЕМА 2. ІНФОРМАЦІЙНА РОБОТА

План

1. **Етапи інформаційної роботи**
2. **Робота з джерелами інформації**
3. **Інтернет як джерело інформації**
4. **Принципи обробки та первинний аналіз інформації**

1.Етапи інформаційної роботи

Інформаційна робота включає наступні **етапи**:

- ***Визначення потреб*** (постановка завдання) - з'ясування, яка інформація потрібна і для чого. На цьому етапі формулюються інформаційні інтереси замовника (керівництва, підрозділу).
- ***Пошук і збір інформації*** - відбір джерел: відкриті (ЗМІ, соцмережі), напівзакриті (платні бази, підписки), внутрішні (логи, звіти). Вибір використовуваних методів: моніторинг, спостереження, OSINT, контент-аналіз.
- ***Первинна обробка*** (фільтрація й систематизація) - видаляються дублікати та «шум», інформація групується за темами;
- ***Зберігання та документування*** - дані архівуються, заносяться в бази, ведуться інформаційні картки чи досьє (це потрібно для того, щоб до них можна було звернутися повторно);
- ***Передача інформації аналітикам***.

На виході ми ще не маємо «висновків», але створюємо впорядковану сировинну базу, без якої аналіз неможливий.

Процес, який починається з моменту постановки завдання її користувачами, і закінчується в момент надання користувачам інформації, що відповідає поставленим завданням та вимогам, - це процес добування інформації.

Організація добування інформації включає:

1. ***Декомпозицію завдань*** - завдання, поставлені у загальному вигляді, потребують конкретизації з урахуванням наявних перехідних даних про можливі джерела інформації, їх знаходження, способи доступу, параметри використовуваних технічних засобів добування тощо. Така конкретизація відбувається шляхом розбиття загального завдання на менші, конкретніші підзадачі, враховуючи, які джерела можуть дати відповідь; як до них отримати доступ (легально, технічно, організаційно); які інструменти будуть використані; які обмеження існують (час, ресурси, ризики). Таким чином загальна формула завдання перетворюється на чіткий алгоритм пошуку. **Наприклад**, нехай завданням є: «Дізнатися про плани конкурента щодо нового продукту». Результатом декомпозиції буде розбивка на задачі:
   - Перевірити сайт конкурента — чи є вакансії у відділі R&D (Research and Development);
   - Проаналізувати патентні бази на наявність нових заявок;
   - Моніторити галузеві форуми й виставки на предмет «витоків» від співробітників;

- Використати платні бази постачань обладнання.

2. ***Розробка задуму операції*** з добування інформації - у результаті аналізу загальних завдань та вихідних даних розробляється задум операції, у якому намічаються шляхи вирішення конкретних завдань, тобто це перехід від «поставленої задачі» до конкретного плану, який визначає: які цілі стоять перед групою (що саме потрібно добути); які джерела будуть використані (відкриті, напівзакриті, технічні, людські); якими методами це буде зроблено (моніторинг, опитування, технічні сенсори, аналіз документів); які ресурси та засоби потрібні (програмне забезпечення, доступи, фінанси); які терміни виконання та форма представлення результату. **Наприклад**, завдання (загальне): оцінити протестні настрої у регіоні. Задум операції:
   - Зібрати пости з соцмереж (ключові слова).
   - Зібрати статті з місцевих ЗМІ.
   - Зібрати статистику петицій та звернень.
   - Результат (інфо-робота): масив даних (1000 постів, 50 статей, 20 петицій).

   Таким чином, задум операції відповідає концептуальному рівню, визначає, як в цілому буде досягнута мета, формулює основні напрямки: що збирати, які джерела використовувати, якими методами; Містить варіанти дій і можливі шляхи вирішення проблеми. Його можна порівняти зі стратегією операції.
3. ***Планування -*** тактичний рівень, визначає конкретно: хто, коли, що робить, якими засобами, розписує етапи та ресурси у деталях. Планування - перетворення задуму на послідовність конкретних дій.

   У ході планування передбачаються заважні та випадкові фактори: дії протилежної сторони, недостатність вихідної інформації, відмова апаратури, погодні умови, пильність персоналу об'єкта розвідки тощо.
4. ***Постановку завдань виконавцям*** (завдання ставляться із зазначенням місця та часу дій всіх виконавців, а також використовуваних технічних засобів).
5. ***Корпоративне та оперативне управління*** діями виконавців та роботою технічних засобів (нормативне управління передбачає постановку завдань виконавцям перед проведення операції, оперативне внесення у ході її коректив, викликаних зміною обстановки).

2. Робота з джерелами інформації

Для перетворення опосередкованої інформації в проблемно-орієнтований інформаційний масив потрібно використовувати цілеспрямований підхід щодо активного сприйняття потоків, що постійно надходять. Найважливіше у цій роботі - правильно підібрати джерела інформації, обробити їх із використанням принципу "ключових слів" і організувати сортування, класифікацію та зберігання вже обробленої інформації.

Принцип «ключових слів» - дуже важливий принцип, що використовується в інформаційній роботі. Ключові слова – це своєрідні "маячки", за якими відбирається релевантна інформація з великих потоків даних, вони відображають тематику пошуку або ознаки проблеми, яка цікавить аналітика. Усі матеріали, де зустрічаються ключові слова, потрапляють у первинний масив для подальшої обробки. Тут треба зауважити, що

- якщо набір ключових слів підібрано невдало, можна або «пропустити» важливу інформацію, або отримати надто багато «шуму»,
- потрібно регулярно оновлювати словник ключових термінів, бо мова й терміни змінюються.

Інформаційна робота є фундаментом для наступної роботи аналітика, тому її організація і результати повинні враховувати специфіку роботи аналітика. Часто дані з різних джерел дублюють один одного, тому просте кількісне збільшення оброблюваних джерел призводить лише до перевантаження аналітика без видимих результатів покращення якості його роботи. **Ситуація з надлишком інформаційного шуму в оброблюваних інформаційних масивах набагато небезпечніша, ніж інформаційний голод**. Дійсно, людський мозок має обмежену пропускну здатність, і коли інформації занадто багато, аналітик витрачає ресурси не на аналіз, а на відсів «сміття», в результаті чого важливі сигнали можуть загубитися серед другорядних повідомлень; у потоці шуму легко «підібрати» дані, які підтверджують уже наявну гіпотезу, при цьому ігноруються малопомітні, але критично важливі факти, в результаті чого висновки стають суб'єктивними і викривленими; при інформаційному голоді аналітик знає, що у нього бракує даних, а от при інформаційному шумі створюється ілюзія «все відомо», хоча насправді релевантних даних може бути менше 5%, що призводить до помилкової впевненості у правильності рішень; обробка надмірних потоків займає час, який міг бути витрачений на аналіз дійсно важливого матеріалу, до того ж надлишок даних перевантажує й використовувані технічні системи, в результаті чого реагування запізнюється; в умовах шуму аномалії (наприклад, ознаки атаки чи підготовки конкурентом дії) можуть стати «невидимими».

Працюючи з відкритими джерелами, треба враховувати, що ступінь уваги, що приділяється у них деяким обставинам, не завжди відповідає дійсній значимості цих обставин. На зміст повідомлень відкритих джерел впливає, серед іншого, конкурентна боротьба. Крім того, у кожній країні відкриті джерела використовуються тією чи іншою мірою як для маніпулювання цивільною громадською думкою цієї країни, так і спецслужбами інших країн, що вивчають ці джерела.

Значна частка відкритих джерел, що використовуються під час інформаційної роботи, це періодичні видання. При обробці періодики насамперед необхідно з'ясувати: засновників цього видання; спонсорів; головного редактора; тираж; форми розповсюдження; основну категорію читачів. Більшість цих відомостей розміщені у вихідних даних. Виходячи з перелічених вище відомостей, можна з'ясувати такі дані: потенційна достовірність гостро спрямованих матеріалів; перспективи спільної роботи з виданням; необхідність видання для подальшої роботи. Гострі матеріали завжди кимось використовуються. Знаючи можливості замовника або коло його інтересів, можна прогнозувати достовірність інформаційних матеріалів. Знаючи засновників та спонсорів цього видання, можна визначити перспективи спільної роботи. Видання можна використовувати для власних матеріалів з прихованої реклами, для відпрацювання гострих матеріалів в конкурентній боротьбі і т.д.

У плані практичного застосування методології роботи з відкритими джерелами інформації ЗМІ пропонуються ***два організаційні підходи до первинної обробки матеріалів ЗМІ***:

1. Використання власних можливостей. Тут також можливі два варіанти. Перший варіант: усі матеріали ЗМІ, що надходять до організації (фірми) можуть оброблятися відповідальною за це особою та згідно з розробленим класифікатором сортуватися та зберігатися. Другий варіант: співробітники служби безпеки починають свій робочий день із вивчення ЗМІ (наприклад, за кожним з них закріплені по 2-3 центральні або місцеві джерела). Протягом дня на зустрічах із джерелами інформації у напівофіційних чи неофіційних розмовах ця інформація уточнюється, набуваючи необхідної надійності.

2. Використання сторонніх можливостей для обробки ЗМІ. Інформація може закуповуватися на стороні, чим повинні займатися спеціально виділені люди, що пов'язано з тим, що іноді функції первинної обробки матеріалів ЗМІ дешевше передати стороннім людям, ніж проводити її силами своїх співробітників. Наприклад, використання для первинної обробки матеріалів ЗМІ співробітників бібліотек.

Слід враховувати, що у відкритих джерелах багато тверджень є не первинними, а запозиченими з інших джерел, що часто призводить до спотворення інформації, що подається.

Враховуючи тісний зв'язок між інформаційною та аналітичною роботою, виділяючи інформаційні джерела, які можуть бути цікавими в подальшому для аналітика, треба брати до уваги, що аналітик, який працює на стратегічному рівні, не повинен нехтувати, серед іншого, роботою з художніми текстами, тому що викладене в них не завжди є вигадкою. Творча свобода, якою користуються автори художніх творів (і яка відсутня в авторів "серйозних публікацій"), іноді забезпечує значні прориви інтуїції та дає цінні результати, яких ніколи не привів би обережний аналіз. Наприклад, у романі «1984» Джорджа Орвелла, автор дуже яскраво демонструє, що інформація - це ресурс влади, а контроль над нею - це контроль над суспільством, що підтверджується сьогодні. Процес інформаційної маніпуляції обовязково повинен враховуватися аналітиком при проведенні ІАР.

3. Інтернет як джерело інформації

Найпотужніше і найдинамічніше джерело інформації, яке використовується в інформаційно-аналітичній роботі сьогодні — це Інтернет: офіційні сайти; ЗМІ та онлайн-видання (новини, інтерв’ю, репортажі); соціальні мережі (Facebook, Telegram, TikTok та ін.), які відображають настрої суспільства; блоги й форуми (думки експертів, «інсайдерська» інформація); спеціалізовані бази даних (наукові публікації (Google Scholar та ін.), технічні ресурси); Darknet та deep web (нелегальні ринки, хакерські форуми, витоки даних). Це джерело, як і всі інші, має як переваги, так і недоліки. Переваги Інтернету як джерела інформації:

- Оперативність (інформація з’являється майже миттєво);
- Масштабність (доступ до глобальних даних) - дані можна отримати з будь-якої точки світу; кількість інформації в Інтернеті зростає

експоненційно; Інтернет об’єднує офіційні (державні портали, наукові бази) і неофіційні (чати, блоги, даркнет) джерела;

- Доступність: більшість ресурсів відкриті.
- Різноманітність форматів: текст, відео, зображення, бази даних.

Небезпечності в Інтернеті:

- Недостовірність (велика кількість фейків, маніпулятивних матеріалів);
- Інформаційний шум (надлишок даних, дублювання, що гірше, ніж інформаційний голод, про що говорилося вище);
- Анонімність джерел (складно перевірити автора, притягнути до відповідальності);
- Правові обмеження (не вся інформація в Інтернеті є «відкритою»; у різних країнах є закони, які регулюють доступ до певних типів інформації; порушення авторських прав, законів про персональні дані (див.табл.2.1)).
- Небезпека маніпуляцій («інформаційні вкиди», ботоферми тощо (див.табл.2.2)).

Таблиця 2.1. Законність використання Інтернет-джерел

Метод роботи	Законність	Ризик
Моніторинг офіційних сайтів (державних, корпоративних)	Абсолютно легально	Низький — хіба що інформація може бути упередженою
Читання ЗМІ, блогів, соцмереж (відкриті публікації)	Легально	Середній — достовірність інформації часто сумнівна
Використання платних баз даних за ліцензією (Scopus)	Легально при підписці	Низький, якщо дотримано умов ліцензії
OSINT-інструменти для збору відкритих даних (наприклад, пошук по ключових словах)	Легально, якщо збір не порушує правил платформи	Середній — можливе блокування акаунта або претензії від сервісу
Скрапінг (автоматизоване копіювання сайтів, соцмереж)	Умовно легально (залежить від правил ресурсу)	Високий — може порушувати умови користування або авторські права
Збір персональних даних без згоди (email, профілі користувачів, геолокація)	Незаконно (порушення GDPR, законів про персональні дані)	Дуже високий — штрафи, кримінальна відповідальність
Використання даркнет-ресурсів (форуми, чорні ринки)	Доступ легальний, але робота із забороненим контентом незаконна	Дуже високий — ризик кримінальної відповідальності та зараження шкідливим ПЗ
Злам сайтів, фішинг, експлойти для доступу	Абсолютно незаконно	Кримінальна відповідальність,

до даних		серйозні санкції

Таблиця 2.2. Маніпуляції в Інтернеті

Тип маніпуляції	Як виглядає	Чим небезпечна
Фейки	Повністю вигадані новини (вигадана подія, фото, цитата)	Викликають паніку, дискредитують осіб чи компанії
Дезінформація	Цілеспрямовано поширені неправдиві відомості	Використовується як інструмент політичної або інформаційної війни
Маніпуляція контекстом	Факти подані вибірково, з акцентом на потрібній інтерпретації	Створює викривлене уявлення про події
Ботоферми і тролі	Масові акаунти поширюють одні й ті самі повідомлення	Створюють ілюзію «громадської думки» або підтримки
Алгоритмічні маніпуляції	Підбір контенту соцмережами/пошуковиками для підштовхування до певних тем	Люди потрапляють в «інформаційні бульбашки», втрачають об’єктивність
Deepfake (підробки)	Штучно згенеровані відео/аудіо, схожі на реальні	Можуть зруйнувати репутацію, спровокувати конфлікти чи кризи довіри

Враховуючи переваги та недоліки використання Інтернету як інформаційного джерела для інформаційної роботи, можна зробити наступний висновок: Інтернет як джерело не може розглядатися як «готова інформація» - це лише сировина, яку потрібно відбирати (ключові джерела, релевантні тематиці), фільтрувати (усувати шум і дублювання), верифікувати (перевіряти достовірність з кількох незалежних джерел), структурувати (перетворювати хаотичні дані у впорядкований інформаційний масив).

4. Принципи обробки та первинний аналіз інформації

Характер і склад множини джерел інформації визначається можливостями системи збору інформації, яку має конкретний суб'єкт ІАР. Тому тут дуже важливим є ***технологічний цикл інформаційної роботи***. Технологічний цикл є організованою в часі сукупністю операцій і методів, що призводить до отримання заданого результату.

Технологічний цикл інформаційної роботи можна поділити на такі етапи:

1. Встановлення характеру завдання, опис проблемної ситуації.
2. Синтез головної (або глобальної) мети як прямого наслідку поставленого завдання.

3. Уточнення цілей отримання інформації, стилю ІАР споживача інформації.

4. Формування групи виконавців.

5. Декомпозиція цілі в залежності від характеру проблеми.

6. Виявлення цілей споживача інформації, що потребують поповнення інформаційних ресурсів для їх досягнення.

7. Синтез цілей інформаційної роботи за напрямами, визначеними споживачем інформації.

8. Виділення кадрових та інших ресурсів для інформаційно-пошукових робіт, постановка завдань на пошук інформації.

9. Пошук джерел інформації із заданими властивостями.

10. Оцінювання реальної інформативності джерел та вибір найбільш інформативних.

11. Збір та накопичення даних, аналіз представницькості вибірки.

12. Аналіз несуперечності масиву даних, отриманих від джерела.

13. Інтеграція масивів даних, виявлення протиріч та/або неповноти.

14. Проведення аналізу на повному масиві, встановлення стану об'єктів та систем, що є предметом розвідки.

15. Синтез моделі об'єкта, системи чи процесу розвідки.

16. Підготовка висновків про об'єкт розвідки, синтез простору альтернатив.

17. Визначення критичних точок у об'єкті розвідки.

18. Проведення імітаційного моделювання.

19. Оцінювання ефективності виконання завдань інформаційної роботи.

20. Синтез комплексних стратегій, оцінювання ефективності та порівняльний аналіз стратегій інформаційної роботи.

Розглянемо цей процес в дії на **прикладі:** інформаційна робота у сфері кіберзахисту банку:

1. *Встановлення характеру завдання:* у банку зафіксовано різке зростання фішингових атак на клієнтів. Завдання - з’ясувати, чи готується масштабна цілеспрямована атака на банк.

2. *Синтез головної мети:* отримати достовірну інформацію про потенційні кіберзагрози, які можуть вплинути на банк.

3. *Уточнення цілей та стилю ІАР споживача:* керівництво банку хоче прогноз і рекомендації: не технічні деталі, а бізнес-орієнтовані висновки.

4. *Формування групи виконавців*: створюється група: фахівці SOC, OSINT-аналітик, експерт із фінансових кіберзагроз, представник служби безпеки. Тут треба врахувати, що хоча «в полі зору» з’являються аналітики та експерти, ми говоримо про технологічний цикл інформаційної роботи, а він охоплює не лише механічний збір даних, а й організацію цього процесу. Якщо звузити рамки до «інформаційного пошуку», то: аналітик ще не працює з даними, але групу треба сформувати, щоб розподілити інформаційні задачі (хто моніторить офіційні сайти, хто збирає дані з соцмереж, хто перевіряє даркнет-джерела). Це все ще інформаційна робота, бо мова йде не про висновки, а про організацію добування інформації.

5. *Декомпозиція цілі*: зрозуміти: хто атакує? Які методи використовує? Чи є підготовка до масштабнішої атаки?

6. *Виявлення цілей споживача*: керівництво цікавлять фінансові ризики, репутаційні втрати, стабільність роботи онлайн-банкінгу.

7. *Синтез цілей інформаційної роботи*: моніторинг даркнет-форумів (продаж баз даних банку); пошук фішингових доменів, схожих на сайт банку; аналіз телеграм-каналів хакерських угруповань.

8. *Виділення ресурсів*: SOC отримує задачу моніторити домени; OSINT-аналітик працює з даркнетом; служба безпеки — з правоохоронними структурами.

9. *Пошук джерел*: даркнет-форуми; бази злитих даних; антифішингові сервіси; кіберрозвідка партнерів.

10. *Оцінка інформативності*: даркнет-форуми - дають ранні сигнали; телеграм-канали - швидкі, але неперевірені; офіційні CERT-звіти - надійні, але із запізненням.

11. *Збір та накопичення даних*: зібрано близько 200 повідомлень про можливі продажі даних клієнтів і 50 нових фішингових доменів.

12. *Аналіз несуперечності*: частина повідомлень дублюється; деякі домени неактивні, тому відсіюються.

13. *Інтеграція масивів*: зіставлення даних - 10 доменів пов'язані з тією ж IP-адресою, що і відомі фішингові сайти.

14. *Аналіз на повному масиві*: встановлено, що атака йде з групи, яка раніше атакувала банки Східної Європи.

15. *Синтез моделі*: модель атаки - підготовка до «фішингової кампанії + продаж крадених акаунтів у даркнеті».

16. *Підготовка висновків*: імовірність масштабної атаки висока; критичні напрямки - онлайн-банкінг, клієнтські акаунти.

17. *Визначення критичних точок*: система автентифікації клієнтів; канали розсилки SMS/емейлів.

18. *Імітаційне моделювання*: проводиться симуляція атаки - якщо фішинг «успішний», то банк втрачає до 10 млн грн.

19. *Оцінювання ефективності роботи*: виявлені загрози за 2 тижні до можливої атаки, тому інформаційна робота виконана результативно.

20. *Синтез стратегій*: впровадження додаткових антифішингових рішень; інформування клієнтів; співпраця з CERT для блокування доменів.

Інформація, отримана в результаті пошуку, має аналізуватися. Аналіз спрямовано на оцінку повноти, точності, своєчасності.

Інформації властива властивість старіння. Зазвичай вважається, що оперативно-тактична (інформація, яка відображає ситуацію «тут і зараз», використовується для прийняття швидких і точкових рішень, найчастіше застосовується службами безпеки, військовими, кібероперацийними центрами та бізнес-структурами для негайного реагування) інформація втрачає половину своєї цінності через тиждень після її отримання, наукова – 20% на рік. Перед аналізом інформацію слід відсортувати за достовірністю та ступенем оперативності. Якщо немає можливості перевірити достовірність інформації, то опосередковано про неї можна судити з надійності джерела.

При накопиченні інформації в інформаційних ресурсах та базах даних організації використовуються два основні способи її представлення: неструктуроване та структуроване.

Неструктуроване представлення здійснюється за відсутності спеціальних засобів підтримки структури інформаційної моделі предметної області. Цей вид реалізується за допомогою накопичення текстових та графічних файлів. Неструктурована форма представляє різні види контекстного пошуку. У результаті за ключовим словом ми отримуємо всі тексти, у яких воно згадується. Для того, щоб дослідити зв'язки об'єкта, аналітик повинен буде досліджувати отримані тексти щодо виявлення в них зв'язкових об'єктів, і для кожного з них організувати окрему процедуру пошуку. Такий процес аналізу може бути досить тривалим за часом. До цієї категорії належать повнотекстові бази даних, в яких накопичуються електронні версії ЗМІ, дайджести, нормативна та службова документація.

В рамках структурованого представлення зазвичай реалізується така модель предметної області, в якій інформаційні об'єкти мають достатню еволюційну самостійність, що дозволяє їм "обростати" новими подробицями та зв'язками в міру надходження нових даних. У разі такого опису структур предметної області достатньо вийти на один інформаційний об'єкт, щоб по зв'язках досліджувати його оточення. Таким чином, інформаційні об’єкти - ключові сутності предметної області (наприклад: «компанія», «особа», «подія», «документ»), які, маючи еволюційну самостійність, можуть доповнюватися новими атрибутами й зв’язками: коли з’являється нова інформація, її не додають як окремий факт, а «прикріплюють» до вже існуючого об’єкта. Наприклад: якщо в базі є компанія X, і надходить новина про її партнерів чи фінансовий стан, ці відомості стають новими зв’язками та характеристиками компанії X. Об’єкти пов’язані між собою: «особа → працює у → компанії», «компанія → бере участь у → тендері», «подія → відбулася у → місті». Достатньо знайти один вузол у цій мережі (наприклад, людину), і по зв’язках можна «розплутати» її оточення: роботодавців, колег, участь у подіях, згадки в медіа тощо.

Дуже важливим етапом інформаційної роботи є **первинна обробка** отриманих даних, яка може проводитися в наступному порядку:

- синтез загальної класифікації завдань, що коли-небудь вирішувалися під час проведення ІАР;
- встановлення класу нового завдання та виявлення завдань, подібних до даного;
- аналіз досвіду вирішення аналогічних завдань та зчитування масиву даних та моделей, асоційованих з ними;
- відбір з отриманого масиву даних та моделей тих, які релевантні в даній задачі;
- встановлення відмінностей даного конкретного завдання від раніше вирішуваних;
- встановлення тих блоків даних та компонентів моделей, які не можуть бути застосовані для вирішення цього завдання;
- пошук методів адаптації існуючих моделей та встановлення напрямів пошуку;

- відновлення відомостей про джерела інформації, що залучаються для отримання даних при вирішенні аналогічних завдань, формування гіпотези щодо напрямів інформаційно-пошукових заходів;
- аналіз парку інструментальних засобів проведення пошуку та їх доступності на поточний час;
- аналіз потреб у розвитку парку технічних засобів та можливостей повторного використання новопридбаних засобів;
- оцінка трудомісткості окремих операцій;
- встановлення факту досягнення/недосягнення поставленої мети інформаційної роботи;
- підготовка укладання та передача документів замовнику.

Розглянемо етапи первинної обробки інформації на конкретному прикладі: первинна обробка даних у випадку витоку інформації з банку.

1. Синтез загальної класифікації завдань: фахівці з інформаційної безпеки фіксують, що подібні завдання вже були - фішингові атаки, зараження робочих станцій, витоки через співробітників.

2. Встановлення класу нового завдання: нинішня ситуація схожа на витік клієнтської бази, бо дані з'явилися на даркнет-форумі.

3. Аналіз досвіду вирішення аналогічних завдань: в минулих випадках перевіряли: чи дані дійсні, чи збігаються з реальними акаунтами, як відреагували клієнти.

4. Відбір релевантних даних і моделей: із загального масиву старих кейсів беруть лише ті, що стосуються банківських витоків, а не технічних збоїв чи шахрайства з картками.

5. Встановлення відмінностей: цього разу дані злиті не через злом серверу, а через недобросовісного співробітника, що раніше не фіксувалося.

6. Встановлення непридатних блоків: методики реагування на DDoS-атаки не підходять, бо інцидент зовсім іншого типу.

7. Пошук методів адаптації моделей: беруть за основу модель роботи з фішинговими витоками, але адаптують її до внутрішньої загрози (інсайдер).

8. Відновлення відомостей про джерела інформації: у попередніх розслідуваннях використовували:

- даркнет-моніторинг,
- співпрацю з CERT,
- перевірку внутрішніх журналів доступу.

Ці ж джерела знову залучають.

9. Аналіз інструментальних засобів: є доступ до SIEM-системи, логів Active Directory, сервісів моніторингу даркнету.

10. Аналіз потреб у розвитку технічних засобів: виявлено, що бракує системи DLP (Data Loss Prevention), яка б у майбутньому попереджала подібні витоки.

11. Оцінка трудомісткості:

- Перевірка бази даних клієнтів — 2 людини × 3 дні.
- Аналіз даркнет-форумів — 1 спеціаліст × 2 дні.
- Опитування співробітників — 1 тиждень.

12. Встановлення факту досягнення мети: встановлено - дані справді злиті інсайдером, масштаби витоку — 20 000 клієнтів. Мета розслідування досягнута.

13. Підготовка висновку та передача документів: аналітики готують звіт для керівництва:

- підтверджено факт витоку,
- виявлено джерело (співробітник),
- розроблено рекомендації: впровадити DLP, посилити контроль доступу, провести навчання співробітників.

Таким чином, інформаційна робота зосереджена на зборі, сортуванні та первинному аналізі даних, результатом стає якісний масив інформації (що сталося, масштаби, джерела), далі вже підключається аналітика для формування стратегічних висновків і рекомендацій (рис.2.1).

Рис.2.1. **Піраміда ІАР**

Дані — це найнижчий рівень: факти, які ще не перевірені (новини, пости в соцмережах, показники датчиків).

Інформація — результат інформаційної роботи: дані перевірені, очищені від шуму, систематизовані.

Аналітика — рівень осмислення: побудова моделей, виявлення закономірностей, формування прогнозів.

Рішення — найвищий рівень, коли на основі аналітики ухвалюються конкретні управлінські або безпекові кроки.

Інформаційна робота є середнім шаром між хаотичними даними та аналітичними висновками.

Без якісного «фундаменту даних» піраміда завалиться, а без інформаційної роботи аналітика залишиться домислами.

Приклад **Інформаційного звіту**

(тема: активність у соцмережах щодо компанії «Х»)

1. Період моніторингу

01.08.2025 – 07.08.2025

2. Джерела

- Twitter, Facebook, Telegram, новинні сайти: *Укрінформ, Ліга, Forbes Україна*.

3. Зібрані матеріали

- Всього публікацій: **327**
- З них у соцмережах: **280**
- У ЗМІ: **47**

4. Тематика публікацій

- Новий продукт компанії — **110 згадок**
- Затримка доставки — **75 згадок**
- Загальні новини про компанію — **142 згадки**

5. Динаміка

- Найбільший пік публікацій — **5 серпня 2025 р. (68 повідомлень)** у зв'язку з виходом офіційного прес-релізу.

6. Приклади публікацій

- *Telegram-канал «Технології UA»*: «Компанія Х анонсувала новий мобільний застосунок».
- *Forbes Україна*: «Затримка доставки викликала невдоволення серед клієнтів».

У звіті є тільки факти: скільки публікацій, де, коли, про що. Тут немає висновків і прогнозів на кшталт «це призведе до падіння репутації» — бо це вже аналітична робота.

В темі 3 розглядається аналітична форма цього звіту.

Питання

1. Охарактеризувати етапи інформаційної роботи.
2. Що включає в себе процес добування інформації? Пояснити, для чого відбувається декомпозиція завдань.
3. Пояснити, чому надлишок інформаційного шуму в оброблюваних інформаційних масивах набагато небезпечніший, ніж інформаційний голод.
4. Два організаційні підходи до первинної обробки матеріалів ЗМІ.
5. Інтернет як джерело інформації: переваги, недоліки.

ТЕМА 3. АНАЛІТИЧНА РОБОТА

План

1. Специфіка аналітичної роботи.
2. Методи аналітичної роботи.
3. Способи аналітичного дослідження.
4. Обробка і використання результатів аналітичної роботи.

1. Специфіка аналітичної роботи

Обробка отриманої інформації - справа, що вимагає скрупульозності в урахуванні найдрібніших деталей та точності в оформленні.

Інформаційна робота передує аналітичній. Завдання інформаційного етапу - створити такий масив даних, який буде придатним для подальшої аналітики. Аналітик не повинен «чистити» дані, його роль - інтерпретація, моделювання, прогнозування, а не боротьба з дублями, шумом чи суперечностями. Якість аналітики прямо залежить від якості інформаційного масиву. Якщо дані не відповідають певним вимогам (достовірність, повнота, актуальність тощо), то аналітичні висновки будуть хибними.

Таким чином, оброблений масив інформаційної документації має відповідати вимогам: доступності, інваріантності, коригування, повноти (розглядалося раніше), своєчасності (розгл.раніше), достовірності (розгл.раніше), несуперечності, захищеності. Це стандарти інформаційної роботи, щоб передати аналітику чистий, придатний масив.

Під **доступністю** розуміється наступне: інформаційний масив має бути зрозумілим і придатним для використання навіть тими аналітиками, які не брали участі в його створенні. Це означає, що дані повинні мати опис (метадані, словники термінів), у документації має бути структура, зрозуміла будь-якому користувачу, відсутність «особистих шифрів» чи надто специфічних позначень, зрозумілих лише автору. Наприклад, якщо базу даних клієнтів створив один співробітник, то інший аналітик повинен без додаткових пояснень зрозуміти, де контакти, де історія покупок, де статус співпраці.

Інваріантність передбачає, що дані мають залишатися однаковими та коректними для всіх користувачів, незалежно від того, як і хто їх переглядає. Наприклад, фінансовий звіт у системі зберігає одні й ті ж показники, навіть якщо різні аналітики будують на його основі різні графіки.

Коригування передбачає можливість модифікації бази даних. Під модифікацією можуть розумітися видалення відомостей, що стали непотрібними або небезпечними, додавання нової інформації, внесення змін до кодування і т.д. Але інформаційний масив повинен допускати оновлення та уточнення без втрати його цілісності й історії. Наприклад, у базі змінюється адреса компанії, але попередні адреси зберігаються для відстеження історії змін. На перший погляд тут виникає начебто протиріччя: з одного боку, коригування - це оновлення, уточнення й навіть видалення непотрібних відомостей, а з іншого боку є потреба фіксувати, що було зроблено раніше. Для з’ясування цього тут треба розрізнити два рівні коригування:

- *Робоче коригування* (активна база) - дані можуть видалятися або змінюватися, щоб підтримувати актуальність. Наприклад: у масиві новин дубльована стаття видаляється, щоб уникнути інформаційного шуму та зменшити перевантаження аналітика, бо вона не додає цінності.
- *Архівне коригування* (історична база) - навіть якщо інформацію видаляють із «робочої вибірки», у системі зберігається лог або історія змін з метою зберегти сліди розвитку інформаційного масиву, щоб не втратити контекст.

Розглянемо ***приклад***: в аналітичному центрі була база з моніторингу Telegram-каналів. Через рік виявили, що 40 каналів неактивні й створюють «шум». Їх видаляють з активної бази, щоб вони не заважали у пошуку, але в архіві залишився запис: «Канал X існував 2020–2021, далі неактивний». Таким чином, робочий масив чистий, але історія збережена.

Несуперечність - дані в масиві не повинні містити внутрішніх протиріч. Наприклад, якщо в одному документі йдеться, що компанія має 500 співробітників, а в іншому - 200, потрібно вказати джерела та уточнити, а не залишати суперечність.

Захищеність (конфіденційність і цілісність) - масив повинен бути захищений від несанкціонованого доступу та спотворень. Наприклад: система з логами доступу, резервними копіями й рівнями прав користувачів.

Для наочності див.табл.3.1.

Таблиця 3.1. Узагальнена таблиця основних вимог до обробленого масиву інформаційної документації

Вимога	Суть	Приклад
Доступність	Масив повинен бути зрозумілим і придатним для роботи навіть для аналітика, який не створював базу	Новий співробітник легко орієнтується у базі конкурентів завдяки чіткій структурі та словнику термінів
Інваріантність	Дані мають залишатися стабільними й незмінними у змісті, незалежно від форм подання	Фінансовий показник однаковий у таблиці, графіку чи звіті
Коригування	Масив допускає оновлення, уточнення та навіть видалення, але з фіксацією історії змін	Видалені дублікати новин відмічені в журналі дій, щоб не втратити контекст
Повнота	Дані повинні охоплювати всі ключові аспекти завдання	У базі про конкурентів є фінанси, PR-активність, вакансії, партнерства
Своєчасність	Інформація має бути актуальною і регулярно оновлюватися	Моніторинг кібератак оновлюється щодня, а не раз на рік
Достовірність	Використовуються перевірені дані з	Чутки з соцмереж позначені як «низька

	надійних джерел	надійність»
Несуперечність	Масив не повинен містити суперечливих даних без пояснення	Якщо в різних джерелах різні цифри співробітників, робиться примітка з уточненням джерел
Структурованість	Інформація впорядкована за логікою та категоріями	База поділена на «події», «організації», «персони»
Захищеність	Масив має бути захищеним від несанкціонованого доступу та спотворень	База з багаторівневими правами доступу і резервними копіями

Успіх усієї аналітичної роботи залежить від знаходження правильного балансу між принципами надмірності та розумної достатності. Аналітик зобов'язаний врахувати та оцінити всі отримані дані, якими б суперечливими вони не були. Дійсно, суперечливі відомості часто є ключовими сигналами: вони показують різні точки зору, наявність дезінформації або інформаційні атаки. Ігнорування таких даних може призвести до однобічної картини. Наприклад, джерело А пише, що компанія-конкурент має 200 працівників, а джерело Б - 700. Якщо відкинути якесь з цих джерел як «незручне», аналітик може зробити хибні висновки про масштаби конкурента. Правильний підхід тут передбачає наступне: зафіксувати обидва числа, перевірити достовірність і пояснити у звіті, чому виникла суперечність.

Ще одною рисою аналітичної роботи є принцип, що будь-яке ставлення до інформації має бути аргументовано. Дійсно, якщо аналітик визнає дані достовірними, він повинен показати, чому саме (посилання на джерело, репутація, незалежні підтвердження); якщо аналітик відкидає дані як сумнівні, то тут також потрібна аргументація (джерело ненадійне, факти не співпадають з іншими даними, є ознаки маніпуляції). Можна сказати, що аргументація - це захист від суб'єктивізму, без неї аналітична робота перетворюється на набір особистих думок, а не на професійний продукт.

Аналітична робота має свою специфіку (табл..3.2), про що вже згадувалося раніше, яка визначає її зміст та цінність для організації:

1. ***Перетворення даних в знання*** - інформаційна робота дає факти та масиви даних, аналітик має встановити зв'язки між цими даними, побачити тенденції та закономірності. Наприклад, зі статистики продажів, наданої в результаті інформаційної роботи, визначити, що падіння відбувається лише у певному регіоні через конкурента.
2. ***Інтерпретація та оцінка*** - аналітик не просто описує факти, а пояснює, чому вони відбулися і що це означає. Наприклад, виявити, що серія протестів не випадкова, а координується певною організацією.
3. ***Робота з невизначеністю і суперечностями*** - на відміну від інформаційника, який збирає дані, аналітик має працювати з неповнотою інформації, суперечливими відомостями, ймовірнісними оцінками, не

дивлячись на те, що інформаційник повинен був позбавити інформаційний масив від всього цього. Все це вимагає від нього застосування логічних методів, моделювання та висунення гіпотез.

4. ***Прогнозування*** - головне завдання аналітики не тільки пояснити минуле і теперішнє, а й спрогнозувати майбутнє. Наприклад: на основі зібраних даних передбачити, що конкурент через 3 місяці вийде з новим продуктом.
5. ***Формування альтернатив і рекомендацій*** - аналітична робота завжди орієнтована на споживача, тобто керівництво чи службу безпеки. Аналітик має представити варіанти рішень із плюсами та мінусами кожного.
6. ***Аргументованість*** - кожен висновок аналітика має спиратися на факти. Будь-яка інтерпретація повинна бути пояснена.

Таблиця 3.2. Специфіка аналітичної роботи

Ознака	Суть	Приклад
Мета	Перетворення інформаційного масиву на знання для прийняття рішень	З даних про активність конкурентів зробити висновок, що вони готують новий продукт
Об’єкт роботи	Не окремі факти, а зв’язки, тенденції, закономірності	Побачити тренд у зростанні атак з певного регіону
Характер даних	Неповні, суперечливі, ймовірнісні	У різних джерелах різні цифри – аналітик їх зіставляє
Основні дії	Інтерпретація, оцінка, синтез, прогнозування	На основі статистики передбачити розвиток подій
Інструменти	Логіка, методи аналізу, моделювання, сценарії	SWOT-аналіз, сценарне прогнозування
Результат	Висновки, прогнози, варіанти рішень із аргументацією	Рекомендація: посилити кіберзахист або співпрацювати з CERT
Адресат	Керівництво, служба безпеки, стратегічні замовники	Аналітична записка для топ-менеджменту
Відповідальність	За точність інтерпретації та логіку висновків	Якщо прогноз хибний, керівництво прийме неправильне рішення

2. Методи аналітичної роботи

Усі методи аналітичної роботи обертаються довкола основних: ***аналіз-синтез***. Під аналізом розуміється розбиття події на деталі, оцінка кожного фрагмента. Синтезом є складання всіх фрагментів у структуру події, що розглядається. Ці дві частини нерозривні та обов'язкові. Як часткові прояви аналізу та синтезу застосовуються: ***індукція та дедукція, абстракція та аналогія*** (розглянуто вище).

Індукція віддає перевагу роботі від часткового до загального, будучи варіантом синтезу. Дедукція передбачає шлях від загального до конкретного,

моделюючи аналіз. Абстракція передбачає спрощення ситуації та приведення її до ряду подібних. Методом абстракції користуються під час моделювання ситуацій. Насправді - це синтез. Аналогія - розбиття ситуації на складові та порівняння їх із існуючими. По суті аналогія – аналіз.

Вирізняють дві основні групи методів:

- ***стратегічні*** (або узагальнені), які дозволяють розглянути ситуацію цілком;
- ***тактичні*** методи, які дозволяють деталізувати картину того, що відбувається, і виділити ключові події.

Основні **стратегічні** методи аналітичної роботи - моделювання та системний аналіз. **Моделювання** - створення узагальнених та спрощених представлень (моделей) ситуації. Часто подію (набір фактів) складно аналізувати як таку. І тут може підбиратися подія, що відповідає основними характеристиками поданій, але є більш простою для аналізу. Модель може бути не лише математичною. Важливо зрозуміти, що моделювання є найпростіший спосіб визначити ймовірний результат або причину події, що аналізується, а тип моделі вибирається, виходячи з доступності і зручності. **Системний аналіз** передбачає оцінку ситуації як самостійної системи, що має два основні параметри: вхід та вихід. Під входом маються на увазі фактори, що вносять зміни до системи, а під виходом – результат впливу цих факторів. Вихід зіставляється із існуючими ресурсами. За невідповідності висновку ресурсам шукається інший вихід. Аналіз відбувається по кожній з можливих "збурних дій" без урахування інших факторів, крім ресурсного забезпечення.

Основними **тактичними** методами аналітичної роботи є: інтеграція та розпізнавання. **Інтеграція** передбачає визначення зв'язків між різними подіями, фактами, сигналами та побудову "інтегральної схеми", де окремі події поєднуються у загальну картину (це як складання пазлу: окремо шматочки нічого не означають, але разом утворюють цілісний образ). **Наприклад**, у службі безпеки компанії з’явилися дані, що на форумі обговорюють вразливість у її програмному продукті, зростає кількість фішингових листів на адресу співробітників, конкурент різко активізував рекламу у цьому ж сегменті. Аналітик інтегрує ці факти й бачить: можлива підготовка інформаційної атаки для підриву репутації компанії. **Розпізнавання** проводиться зіставленням внутрішніх характеристик досліджуваної проблеми із зовнішнім оточенням, щоб класифікувати її. Це процес «розуміння, з чим ми маємо справу». Першим етапом розпізнавання є обробка проблеми, виявлення її основних ознак (Наприклад, у банку зафіксовано серію несанкціонованих доступів до акаунтів клієнтів. Ознаки: однаковий спосіб атаки, часові збіги, використання проксі). На другому етапі виділяються можливі зовнішні описи, що характеризують проблему (це можуть бути: фішинг, атака бот-мережі, або витік внутрішніх паролів). Далі проводиться зіставлення проблеми та описів (внутрішнього та зовнішнього) (порівняння з базою даних CERT показує, що ознаки збігаються з відомою технікою фішингу. Результат: проблема класифікована як «фішингова кампанія», а не витік паролів). Таким чином, інтеграція відповідає на питання: як пов’язані різні факти між собою? Розпізнавання відповідає на питання: що це за явище? До якого класу проблем воно належить? Разом ці методи дозволяють аналітику побудувати цілісну картину (інтеграція), правильно

класифікувати проблему (розпізнавання), підготувати основу для прогнозу й рішень.

Один із дуже важливих тактичних методів аналізу інформації - це ***зіставлення*** фактів, подій тощо. Ознаки зміни подій проявляються в різні часи на різних об'єктах, фіксуються різними джерелами. Взагалі це є інтеграція, тобто взаємне доповнення різнорідних відомостей по одним і тим самим об'єктам шляхом послідовного виявлення подробиць у міру надходження нових даних. Аналіз зазвичай виявляє причинно-наслідкові зв'язки між фактами та подіями, іноді для цього достатньо навіть смислового збігу даних із об'єктивно незалежних джерел. Наприклад, маємо такі факти з різних джерел:

Факт 1 (із новин): у місті різко зросли продажі генераторів;

Факт 2 (із соцмереж): мешканці публікують фото й скарги про часті відключення електроенергії;

Факт 3 (від енергокомпанії): офіційно повідомлено про ремонтні роботи на лінії після обстрілу РФ.

Кожне джерело окремо надає лише інформацію, але їхній збіг за змістом показує причинно-наслідковий зв’язок: причина - ремонтні роботи, наслідок - відключення, підвищений попит на генератори.

В результаті застосування методу зіставлення нарощується деяка інформаційна структура зв'язків об'єкта і може навіть виникнути "похідна інформація", відсутня в явному вигляді в джерелах (Приклад: у відкритій вакансії компанії зазначено: «Шукаємо інженера з квантових технологій»; у новинах повідомляють: компанія отримала грант на перспективні дослідження; у соцмережах співробітник пише: «Нарешті будемо працювати над чимось революційним!». У жодному джерелі прямо не сказано, що компанія запускає проєкт у сфері квантових обчислень, але при зіставленні ці дані складають єдину картину. Це - похідна інформація.). За такого підходу стає можливим простежити ланцюжки зв'язків об'єктів, фактів і подій, що приймають участь у досліджуваній ситуації.

Всі методи аналітичної роботи, як стратегічні, так і тактичні, переслідують одну мету - ***вони використовуються для прогнозування розвитку*** обстановки і подій.

3. Способи аналітичного дослідження.

Існує три основні способи аналітичної роботи: ***одиночний, парний та "мозковий штурм***".

Одиночний спосіб – робота окремого аналітика, який сам обирає методи дослідження, проводить необхідну роботу, готує висновок. Виділяється кілька типів аналітичних працівників залежно від використовуваних ними прийомів роботи.

Парна робота передбачає обслуговування проблеми кількома аналітиками. При цьому зазвичай йде робота на протилежностях оптиміст-песиміст, синтетик-критик, кореспондент-респондент тощо. Оптиміст розглядає проблему з погляду бажаного результату, а песиміст передбачає найгірший варіант. Синтетик створює логічний ланцюжок подій, а критик висловлює зауваження навіть у найменших деталях. Кореспондент ставить незручні питання, а респондент намагається на них відповісти. У результаті формується думка, що влаштовує обох аналітиків. Як варіант парної роботи може

застосовуватися робота двох груп. **Приклад** парної роботи: ситуація - запуск нового онлайн-сервісу банку. Потрібен аналітичний висновок доцільності цієї дії. Оптиміст: новий сервіс залучить тисячі клієнтів; позитивний імідж банку як інноваційного; збільшення прибутків за рахунок нових операцій. Песиміст: високий ризик кібератак у перші тижні роботи, можливі технічні збої, що зіпсують репутацію, конкуренти можуть швидко скопіювати рішення. Результат парної роботи - спільний висновок: запускати варто, але з посиленими заходами кіберзахисту і «пілотною фазою» для обмеженої кількості користувачів.

Мозковий штурм є дуже ефективним прийомом роботи групи спеціалістів. Це - оперативний метод аналізу проблеми та ситуації групою фахівців з усіх ракурсів та пошук можливо, на перший погляд, неадекватних та несподіваних способів її вирішення. Мозковий штурм — це колективне генерування ідей для вирішення проблеми, де важливий кількісний потік пропозицій, а не їхня відразу ж оцінка: кілька людей (група) висловлюють будь-які ідеї; жодна ідея не критикується на етапі генерації; далі йде етап відбору, коли з усіх варіантів обирають найбільш придатні. При цьому правилами мозкового штурму є:

- Чим більше ідей, тим краще, навіть фантастичні пропозиції вітаються;
- Жодної критики на старті: навіть «безглузда» ідея може наштовхнути на правильне рішення;
- Комбінування й розвиток ідей: одна пропозиція може стати «цеглинкою» для іншої;
- Обовязкова фіксація всіх ідей: ведеться протокол/дошка, щоб нічого не загубити.

Розглянемо ***приклад***: як університету залучити більше абітурієнтів на ІТ-спеціальності (на власному досвіді)?

Генерація ідей: створити TikTok-канал з історіями студентів, організувати безкоштовні онлайн-курси з програмування для школярів, провести шкільний хакатон з призами, зробити віртуальну екскурсію лабораторіями, запустити партнерство зі школами.

Після аналітичного відбору залишають найбільш реалістичні та ефективні: хакатон, онлайн-курси, партнерство зі школами.

4. Обробка і використання результатів аналітичної роботи

Аналітична робота не закінчується на етапі аналізу даних. ***Найголовніше - правильно обробити результати і подати їх так, щоб вони були корисні для прийняття рішень***.

У роботі аналітика можна назвати такі ***основні*** операції: формування інформації, її аналіз, підготовка аналітичного документа.

У розпорядженні спеціаліста є різні види інформації, отримана різними шляхами. Він може відстежувати цю інформацію, але яку використовуватиме у кожному конкретному випадку – це вибір аналітика. Від того, наскільки правильно він його зробить і як буде визначено стратегію аналізу, багато в чому залежить результат роботи.

Етапи обробки результатів аналітичної роботи:

- Систематизація: усі висновки впорядковуються за логікою: від фактів до причин, від причин до прогнозів, від прогнозів до рекомендацій.
- Оцінка надійності результатів: перевірка достовірності джерел;
- Формулювання висновків: чітке розмежування між фактами (об'єктивні дані), оцінками (аналітичні інтерпретації), прогнозами (можливі сценарії).
- Розробка рекомендацій: інформація повинна перетворитися на корисну дію для керівництва, кожна рекомендація має бути конкретною: «збільшити фінансування кіберзахисту на 20%» замість «посилити захист».
- Подання результатів: вибір форми (аналітична записка, презентація), мова - чітка, без зайвого наукового «туману».

Приклад: інформаційна атака на компанію в соцмережах

1. Систематизація (збір і впорядкування): аналітики фіксують 7000 згадок у соцмережах за останні 2 тижні, при цьому 60% негативних, 30% нейтральних, 10% позитивних, а найбільше негативу стосується «якості сервісу».
2. Оцінка надійності результатів: джерела - соцмережі, форуми, новинні сайти. Частина акаунтів виявлена як «боти», тому достовірність повідомлень середня, але після уточнення маємо, що дані підтверджуються незалежними ЗМІ, а тому рівень довіри до тенденції високий.
3. Формулювання висновків: у компанії погіршується репутація через проблеми з сервісом; кампанія виглядає як частково організована; репутаційний ризик високий, можливі втрати клієнтів.
4. Розробка рекомендацій:

4.1. Служба підтримки клієнтів:

Завдання: скоротити час відповіді операторів з 10 хвилин до 5 хвилин у найближчі 2 тижні;

Ресурс: додати 5 нових операторів у пікові години (бюджет — 100 тис. грн/міс).

4.2.Комунікаційна кампанія:

Завдання: створити 3 офіційні пости у Facebook та Instagram до кінця тижня з поясненнями ситуації;

Формат: відео-звернення керівника, інфографіка з конкретними цифрами.

4.3.Кіберзахист від ботів:

Завдання: виявити й заблокувати не менше 80% бот-акаунтів протягом 10 днів;

Ресурс: залучення національного CERT та 2 додаткових фахівців з кіберзахисту.

Бюджет: 200 тис. грн на моніторинг і захист.

5. Подання результатів: підготовлено аналітичну записку з графіками динаміки згадок і прикладами бот-повідомлень; проведено коротку презентацію керівництву компанії.
6. Використання (управлінське рішення): керівництво ухвалює наступні рішення:

- посилити контроль сервісу (оперативні наради в службі підтримки),
- виділити бюджет на комунікаційну кампанію,
- доручити ІТ-відділу співпрацю з національним CERT для ідентифікації ботів.

В попередній темі 2 було наведено приклад інформаційного звіту. Порівняйте з ним аналітичний звіт по тій самій тематиці:

Аналітичний звіт (тема: активність у соцмережах щодо компанії «Х» за період 01.08.2025 – 07.08.2025)

1. Загальна оцінка ситуації

Упродовж тижня компанія «Х» була предметом активних обговорень у соцмережах та ЗМІ (327 згадок). Найбільший інтерес викликали два фактори:

- Анонс нового мобільного застосунку (110 згадок).
- Проблеми із затримкою доставки (75 згадок).

2. Тенденції
   - Позитивний тренд: запуск продукту отримав значну підтримку у соцмережах, що може свідчити про високий попит.
   - Негативний тренд: затримка доставки зумовила хвилю критики, яка може мати довготривалий ефект на репутацію бренду.
3. Причинно-наслідкові зв’язки
   - Пік публікацій 5 серпня безпосередньо пов’язаний з офіційним прес-релізом.
   - Кількість негативних згадок про доставку зросла після статті у Forbes Україна, яка стала «тригером» для поширення теми в соцмережах.
4. Прогноз
   - За умови відсутності реакції компанії на проблему з доставкою, можна очікувати подальшого зростання негативних згадок.
   - Якщо компанія запустить рекламну кампанію, пов’язану з новим продуктом, кількість позитивних згадок ймовірно перевищить негативні.
5. Рекомендації
   - Публічно відреагувати на проблему доставки, запровадивши компенсаційні механізми для клієнтів;
   - Доцільно використати інтерес до нового продукту через рекламну кампанію з залученням лідерів думок (мінімум 5 осіб);
   - Встановити щоденний моніторинг тональності з метою зниження негативу на 30% упродовж двох тижнів.

Питання

1. Пояснити, в чому полягає специфіка аналітичної роботи.
2. Основні вимоги до обробленого масиву інформаційної документації. Пояснити їх доцільність.
3. Методи аналітичної роботи.
4. Способи аналітичного дослідження: одиночний, парний та "мозковий штурм". Пояснити переваги та недоліки кожного.
5. Основні операції в роботі аналітика.

Тема 4. ЗАСОБИ ПІДТРИМКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ

План

1. **Засоби підтримки ІАР як інструменти, технології та ресурси**
2. **Моніторинг у межах ІАР**
3. **Прогнозування як ключовий інструмент ІАР**
4. **Методи прогнозування в ІАР, які застосовуються для інформаційної безпеки**
5. **Прогнозування в залежності від ситуації**
6. **Особливості прогнозування в інформаційній безпеці**

1. Засоби підтримки ІАР як інструменти, технології та ресурси.

Засоби підтримки ІАР - це інструменти, технології та ресурси, які допомагають аналітикам збирати дані, обробляти їх, аналізувати, зберігати та представляти результати у зручному вигляді для прийняття рішень.

Вибір засобів підтримки залежить від:

- масштабу організації:

  - ***невеликі організації*** мають обмежений бюджет, невеликий штат, вузьке коло завдань, тому засоби тут, як правило, прості, дешеві, часто - хмарні сервіси, наприклад, Google Alerts для моніторингу, Excel/Google Sheets для збереження даних, Trello/Slack для комунікацій. Витрати на складні системи тут не виправдані;

  - ***середні організації*** (регіональний чи міжрегіональний рівень) мають більш широкий спектр завдань, більші обсяги інформації, повинні враховувати зростаючу конкуренцію. Засоби тут вже передбачаються більш комплексними, наприклад, системи бізнес-аналітики (Power BI, Tableau), моніторинг соцмереж (Brandwatch), оскільки тут вже треба забезпечити поєднання інформації з різних джерел і побудову прогнозів;

  - ***великі корпорації та державні структури*** мають величезні обсяги даних, складні завдання (глобальний моніторинг, аналітика ринків, кібербезпека), тому потребують потужні засоби, часто - спеціалізовані системи, які інтегрують аналітику, прогнозування, збереження і безпеку, наприклад, Data Lakes, системи Big Data, SIEM, системи імітаційного моделювання. Наявний тут масштаб потребує централізованих платформ, автоматизації та високого рівня кіберзахисту.

  Таким чином, масштаб організації визначає обсяг даних, з яким працюють, рівень загроз і завдань, які вирішуються, ресурси (бюджет, кадри), доступні для ІАР. Чим більша організація — тим складніші та дорожчі засоби підтримки їй потрібні, бо і ризики, і відповідальність зростають.

- доступних ресурсів: ресурси визначають «стелю» засобів підтримки ІАР (якщо ресурсів мало - використовуються готові хмарні сервіси; якщо ресурсів більше - створюється єдине інформаційне середовище з інтеграцією; якщо ресурси високі - будуємо повноцінну аналітичну екосистему з Big Data і кіберзахистом);

- рівня загроз і завдань. У сфері ІАР загрози та завдання поділяють за рівнями - оперативним, тактичним і стратегічним. Це допомагає зрозуміти, які саме засоби підтримки потрібні та яка глибина аналізу необхідна. Оперативний рівень - короткострокові події, що потребують негайної реакції. Прикладами завдань тут можуть бути: відстеження появи критичного повідомлення в ЗМІ/соцмережах, виявлення іциденту безпеки в ІТ-системі, швидке інформування керівництва, а засобом підтримки ІАР, наприклад, моніторинг у реальному часі (SIEM). Тактичний рівень передбачає середньострокові завдання (тижні-місяці), аналіз тенденцій та закономірностей. Прикладами завдань тут можуть бути аналіз трендів ринку, виявлення нових схем атак конкурентів чи зловмисників, оцінка ефективності заходів інформаційної безпеки, а засобами підтримки ІАР - системи бізнес-аналітики, інтегровані бази даних, аналітичні пакети (Python). Стратегічний рівень завдань - довгострокове планування (місяці-роки), оцінка глобальних загроз, формування політик, наприклад, прогноз розвитку галузі, сценарний аналіз ринкових або політичних ризиків, розробка стратегій кіберзахисту чи конкурентної розвідки. Засобами підтримки ІАР можуть виступати Big Data-платформи, системи моделювання, машинне навчання, експертні системи.

Зауваження: хоча масштаб організації напряму впливає і на ресурси, і на рівень загроз та завдань, ці фактори вибору засобів підтримки виокремлюють. Це дійсно має сенс, оскільки масштаб організації - це базова характеристика, вона зазвичай корелює з ресурсами та загрозами, але не завжди визначає їх однозначно. Навіть великі організації можуть обмежувати фінансування ІАР (економія, інші пріоритети), мати нестачу кадрів (наприклад, аналітиків з кібербезпеки), використовувати застарілі інструменти, тобто масштаб – це потенціал ресурсів, але реальні ресурси можуть бути значно меншими. Так само рівень загроз не завжди визначається масштабом організації, наприклад, малий бізнес у критичній сфері (невелика компанія-розробник дронів або сенсорів для військових потреб) може мати ризики кібератак набагато вищі, ніж велика компанія в традиційній галузі (наприклад, видобуток сировини).

Засоби підтримки ІАР охоплюють як *технічні (інформаційно-технологічні),* роль яких полягає в тому, щоб робити роботу аналітика оперативною, масштабованою, автоматизованою (все, що стосується збору, збереження, обробки та візуалізації інформації), так і *організаційні* складові, які дозволяють перетворювати сирі дані на готову аналітику.

Основні групи інформаційно-технологічних засобів підтримки ІАР:

- Засоби збору інформації (пошукові системи, агрегатори даних; системи моніторингу ЗМІ, соцмереж (OSINT-платформи); бази даних (наукові, технічні, патентні, комерційні); спеціальні сенсори, логери (у сфері інформаційної безпеки — SOC, SIEM));
- Засоби збереження та управління інформацією (бази даних і сховища (SQL, NoSQL), системи керування документами, корпоративні бази знань);
- Засоби обробки й аналізу (статистичні пакети, інструменти візуалізації, системи Big Data та машинного навчання для виявлення закономірностей;
- Засоби представлення результатів (аналітичні записки та звіти,

презентаційні системи (MS PowerPoint);

- Засоби комунікації та взаємодії (корпоративні месенджери (Teams), системи колективної роботи над документами, захищені канали обміну даними).

Організаційні засоби підтримки ІАР: це правила, методи, структура та регламенти, які забезпечують правильне застосування техніки і створюють умови для ефективної ІАР. Наприклад, необхідною умовою ефективної ІАР є певна організаційна структура, а саме наявність окремої аналітичної групи чи аналітичного відділу; регламенти роботи: порядок збору інформації, перевірки достовірності, підготовки аналітичних матеріалів; встановлені чіткі механізми зв'язку між аналітиками та керівництвом; розподіл відповідальності: хто шукає, хто аналізує, хто приймає рішення. Особливу увагу тут треба приділяти системі навчання та підготовки кадрів, враховуючи необхідність постійного підвищення кваліфікації аналітиків. Дійсно, техніка може бути найдосконалішою, але без правильної організації якість результату може значно страждати.

2. Моніторинг у межах ІАР

Важливими функціями ІАР є моніторинг і прогнозування.

Моніторинг у межах ІАР – це регулярне, комплексне та повне спостереження за інформаційними потоками та подіями у просторі, що становить інтерес, із проведенням первинного аналізу.

Можливі **цілі** моніторингу в межах ІАР:

- накопичення даних для формування уявлень про характеристики спостережуваних подій, що повільно або рідко змінюються: створення бази знань про такі події. Наприклад, моніторинг використання корпоративних ресурсів, а саме: які системи співробітники відвідують, який середній обсяг мережевого трафіку. Це дозволяє створити **«базову модель»** нормальної поведінки, при цьому базова модель - це представлення того, як система або користувач звичайно функціонує у штатному режимі. Вона створюється саме завдяки накопиченню даних у процесі моніторингу: ми спостерігаємо події тривалий час і фіксуємо їхні закономірності. Коли ця модель вже є, будь-яке відхилення від неї може бути сигналом про інцидент або загрозу. Наприклад, SOC протягом місяця відстежує роботу співробітників у корпоративній мережі (моніторинг), в результаті чого формується базова модель нормальної поведінки: співробітники логіняться з 9:00 до 19:00; середній обсяг завантаження файлів до 200 Мб на день; доступ до конфіденційних баз здійснює лише фінансовий відділ. Фіксація відхилення від базової моделі, а саме те, що користувач Іванов входить у систему о 03:00 ночі; обсяг завантажених файлів за ніч перевищує 5 Гб; доступ здійснено з IP-адреси іншої країни сигналізує про аномалію, бо поведінка не відповідає базовій моделі. Це може бути ознакою компрометації облікового запису;
- виявлення змін, які потребують швидкого реагування, тобто фіксація аномалій або подій, що вимагають негайних дій. Наприклад, виявлення спроби масового входу з невідомих IP-адрес або різке зростання кількості помилкових логінів. Це - тригер для реагування SOC;
- виявлення реакцій подій на ті чи інші впливи, тобто оцінка того, як система

або середовище змінюється у відповідь на певні дії. Наприклад, після введення багатофакторної автентифікації аналітики відстежують зниження кількості спроб несанкціонованого доступу. Це показує ефективність заходів безпеки.

Виділяються такі **різновиди** моніторингу:

- стеження за подіями/процесами, що проходять - безперервне спостереження за вже активними подіями. Наприклад, постійний моніторинг мережевого трафіку для виявлення аномалій у роботі системи;
- виявлення початку події/процесу у певному місці - вчасно зафіксувати момент «старту» важливої події. Наприклад, система **SIEM** фіксує першу спробу входу з підозрілого IP - початок атаки brute force;
- пошук події/процесу у певній області простору - активний пошук сигналів у визначеному середовищі. Наприклад, моніторинг даркнет-форумів для виявлення продажу доступів до корпоративної мережі;
- виділення нових типів подій/процесів - ідентифікація раніше невідомих, нетипових загроз. Наприклад, SOC виявляє новий метод фішингової атаки, який ще не описаний у базі відомих індикаторів компрометації.

Під час моніторингу можуть реєструватися (табл..4.1):

- кількісні характеристики подій/феноменів (такий моніторинг називається ***параметричним***);
- події (такий моніторинг називається ***подієвим***);
- оцінні характеристики феноменів/подій (***концептуальний*** моніторинг.)

Таблиця 4.1. Види моніторингу за типом даних

Тип моніторингу	Суть	Приклад у сфері інформаційної безпеки
Параметричний	Реєстрація кількісних характеристик (числових показників).	Вимірювання кількості спроб входу в систему за хвилину; обсяг мережевого трафіку; середній час відповіді сервера.
Подієвий	Фіксація самих подій і часу їхнього настання.	Логування: «користувач Петренко увійшов у систему о 14:03»; «спроба доступу до забороненої директорії».
Концептуальний	Оцінка якісних характеристик або інтерпретація подій.	Аналіз тональності згадок компанії у соцмережах («позитивні», «негативні»); експертна оцінка загрози як «критична/середня/низька».

Таким чином, кожен тип моніторингу відповідає на різні запитання:

- параметричний - «Скільки?»;
- подієвий - «Що сталося?»;
- концептуальний - «Що це означає?».

Тобто параметричний і подієвий моніторинг - це інформаційна робота (фіксація), а концептуальний - це вже «місток» до аналітики (інтерпретація).

Розрізняється **формальний та інформальний** моніторинг.

Формальний (об'єктивний) є виявлення кількісних характеристик, об’єктивних даних. Фіксується: числа, факти, вимірювані показники. Наприклад, кількість фішингових листів за день; кількість спроб входу в систему; середній час реакції на інцидент. Такий моніторинг дає точні, але «сухі» характеристики без пояснення контексту.

Інформальний (суб'єктивний) моніторинг орієнтується на суб’єктивні оцінки, думки, настрої; фіксує якісні характеристики (думки, оцінки, тональність). Наприклад, відстеження настроїв співробітників у внутрішніх чатах; аналіз реакцій користувачів у соцмережах на кібератаку проти компанії («люди вважають, що організація не контролює безпеку»); експертна оцінка ризику як «високий/середній/низький». Такий моніторинг дає розуміння «як це сприймається» суспільством або експертами.

Таким чином, **моніторинг** — це фундаментальна складова ІАР, без якої неможливе ефективне інформаційно-аналітичне забезпечення інформаційної безпеки.

Критична важливість моніторингу полягає в наступному:

- це базовий рівень інформації - моніторинг дає сирові дані (кількісні, подієві, оцінні), на яких будується подальша аналітика;
- це раннє попередження загроз - саме завдяки моніторингу можна виявити атаки або підготовку до них на ранніх стадіях (аномалії у трафіку, підозрілі входи, негативні згадки у ЗМІ);
- це комплексне бачення середовища - моніторинг дозволяє охопити і технічні події (кількість логінів, атаки), і соціальні процеси (настрої, репутаційні ризики), що створює цілісну картину;
- це оцінка ефективності заходів безпеки - тільки через регулярне спостереження можна зрозуміти, чи дійсно нові політики або технічні рішення працюють;
- це «місток до аналітики» - моніторинг не дає готових рішень, але він створює основу для аналізу, прогнозування й вироблення рекомендацій для керівництва.

Таким чином, моніторинг - це «очі й вуха» інформаційно-аналітичного забезпечення. Він не замінює аналітику, але без нього аналітика була б неможлива. Саме якісний моніторинг забезпечує достовірність, повноту й актуальність даних, на яких ґрунтуються управлінські рішення в сфері інформаційної безпеки.

3. Прогнозування як ключовий інструмент ІАР

Наступним ключовим інструментом ІАР є **прогнозування**.

Прогнозування — це процес передбачення розвитку подій, процесів або загроз на основі: даних, зібраних під час моніторингу, виявлених закономірностей і трендів, експертних оцінок та моделей. Якщо моніторинг відповідає на питання «що відбувається зараз?», то прогнозування - на питання «що може статися далі?».

Дуже важлива роль прогнозування в сфері інформаційної безпеки. Прогнозування дозволяє підготуватися до атак ще до того, як вони почнуться (раннє попередження); допомагає визначати, які загрози найбільш імовірні та небезпечні; дає змогу будувати довгострокові стратегії захисту.

Розглянемо **приклади** прогнозування в області інформаційної безпеки:

- На основі аналізу зростання кількості фішингових кампаній у регіоні отримано прогноз хвилі атак на фінансові установи;
- На основі відстеження поведінки співробітників (різке збільшення копіювання файлів) зроблено прогноз можливого витоку даних;
- На основі опублікованої інформації про нову «критичну» вразливість у популярному програмному забезпеченні, яке використовується в компанії, робиться прогноз про те, що протягом наступних 1–2 тижнів групи зловмисників почнуть активно її експлуатувати.

Таким чином, прогнозування завжди базується на фактах, але виходить за їхні межі, створюючи ймовірні сценарії майбутнього розвитку подій.

Цілі прогнозування в ІАР

- Раннє попередження про загрози: виявити ознаки підготовки атак або кризових подій ще до того, як вони проявляться. Наприклад: фіксується поява експлойтів у даркнеті, результат - прогноз масового використання упродовж 1–2 тижнів;
- Оцінка ймовірності розвитку подій: визначення, які з можливих сценаріїв є найбільш вірогідними. Наприклад, при виявленні вразливості в корпоративному ПЗ аналітик прогнозує, що зловмисники використають її з 70% ймовірністю, якщо патч не буде встановлено протягом 10 днів;
- Оцінка масштабів можливих наслідків: передбачення того, наскільки серйозними будуть результати події. Наприклад, прогноз, що DDoS-атака на онлайн-сервіси призведе до повного відключення платформи щонайменше на 6 годин;
- Підтримка управлінських рішень: надання керівництву інформації для вибору оптимальної стратегії дій. Наприклад, прогноз репутаційної кризи у разі мовчання компанії при певних подіях;
- Стратегічне планування: створення довгострокових сценаріїв розвитку ситуації. Наприклад, прогноз зростання кібератак на енергетичний сектор у найближчі 2 роки, з якого необхідно випливає підготовка програми інвестицій у кіберзахист;
- Виявлення слабких місць і критичних точок: визначення, де саме можливі найуразливіші місця, які можуть бути використані зловмисниками. Наприклад, прогноз, що через відсутність сегментації мережі потенційний злом одного акаунта призведе до повного компрометування системи.

Зазначимо, що хоча цілі моніторингу і прогнозування формально можуть перетинатися (наприклад, раннє попередження про загрози), змістовно вони відрізняються (див.табл.)

Таблиця 4.2. Порівняння цілей моніторингу і прогнозування

Ціль	Моніторинг (теперішнє)	Прогнозування (майбутнє)

Раннє попередження	Виявлення початкових сигналів уже наявної або щойно запущеної події. *Приклад:* SOC бачить перші спроби входу з підозрілих IP.	Передбачення можливого розвитку події, яка ще не почалася. *Приклад:* на основі трендів прогнозується хвиля атак на компанію протягом 2 тижнів.
Оцінка ситуації	Фіксація та опис фактів у реальному часі. *Приклад:* «кількість фішингових листів зросла у 2 рази за добу».	Оцінка ймовірності розвитку сценаріїв. *Приклад:* «якщо зростання триватиме, через тиждень атаки досягнуть піку».
Реакція на зміни	Своєчасне виявлення змін у параметрах чи подіях. *Приклад:* з'явилися нові індикатори компрометації у логах.	Передбачення наслідків цих змін. *Приклад:* «нові індикатори можуть означати перехід атаки на внутрішні системи».
Виявлення нових загроз	Фіксація незнайомих або нетипових подій. *Приклад:* виявлено нову схему фішингу.	Прогноз еволюції цих загроз. *Приклад:* «цей метод фішингу може поширитися у фінансовому секторі протягом місяця».
Підтримка управління	Забезпечення керівництва актуальними даними про стан середовища.	Надання керівництву сценаріїв розвитку подій для вибору стратегії дій.

4. Методи прогнозування в ІАР, які застосовуються для інформаційної безпеки

Розглянемо **методи прогнозування** в ІАР, які застосовуються для інформаційної безпеки.

1. ***Екстраполяція трендів***: продовження в майбутнє наявних тенденцій. Наприклад, якщо кількість фішингових листів зростає на 10% щотижня, можна очікувати, що через місяць вона збільшиться ще на 40–50%. Цей метод є простим і швидким, але працює лише тоді, коли тенденція зберігається.
2. ***Сценарний аналіз***: побудова кількох можливих сценаріїв розвитку подій від оптимістичного до кризового. Наприклад, при виявленні критичної вразливості побудовані 3 сценарії:
    - сценарій 1: компанія швидко ставить патч, загроза нейтралізована;
    - сценарій 2: патч затримується, що призводе до часткового компромісу

систем;

- сценарій 3: патч не ставиться, що призводить до масштабної атаки.

Перевагою цього методу є врахування різних варіантів, але він вимагає експертних знань, використовує порівняно (з першим) багато часу.

3. ***Експертні оцінки***: прогнозування на основі знань і досвіду спеціалістів. Наприклад, група експертів оцінює, що ймовірність масованої атаки ransomware на банки України у найближчі 3 місяці складає 60–70%. І хоча такий метод дозволяє врахувати неочевидні фактори, але суб'єктивність, можливі упередження є його значними недоліками.
4. ***Моделювання***: створення моделі об'єкта або процесу і «програвання» різних впливів. Наприклад, моделювання розповсюдження шкідливого ПЗ у корпоративній мережі залежно від наявності/відсутності сегментації. Цей метод дозволяє тестувати різні сценарії «що, якщо», але він є досить складним, може вимагати великі обчислювальні ресурси.
5. ***Статистичні методи***: використання статистики для виявлення ймовірних подій. Наприклад, на основі історії атак визначається, що пік фішингу завжди припадає на святкові дні, з цього отримується прогноз зростання атак у грудні. Плюсами методу є відносна об'єктивність, він ґрунтується на даних. Але його ефективність сильно залежить від якості оброблюваних даних.
6. ***Машинне навчання та ШІ***: алгоритми навчаються на великих масивах даних і виявляють закономірності, які важко помітити людині. Наприклад, SIEM-система на основі ML (Machine Learning) прогнозує можливі «ланцюжки атак» (attack chain) до того, як вони завершаться. Цей метод забезпечує високу точність при великих обсягах даних, але як і будь-який метод, заснований на ШІ, представляє «чорний ящик» та критично залежить від навчальної вибірки.

У практиці інформаційної безпеки методи прогнозування часто комбінують залежно від ситуації, що дозволяє підвищити якість прогнозу.

5. Прогнозування в залежності від ситуації

Можливості та способи прогнозування (або передбачення) ситуації визначаються тим, якою саме є ситуація: ***повторюваною, рідко повторюваною або унікальною***.

Для ситуацій, що повторюються, тобто відбуваються регулярно, за сталими закономірностями, прогнози формуються у вигляді наукових законів або строгих правил. Тут науковий закон - це типовий прогноз, вірний у час і у різних місцях, якщо складаються певні умови. Наприклад, **завжди** перед святами зростає кількість фішингових атак (бо користувачі активніше роблять покупки), наслідком чого є прогноз: «У грудні очікується пік фішингових листів».

Відносно ситуацій, що ***рідко повторюються,*** не є регулярними, виявляються тимчасові закономірності (тимчасові типові прогнози). Тобто такі ситуації можна прогнозувати, але не так надійно, як повторювані події. Тимчасові типові прогнози засновані на тому, що у розвитку подій є схожі риси, але вони проявляються не завжди й не з однаковою силою. Наприклад,

після значних політичних подій (вибори, міжнародні саміти) зазвичай зростає активність кібератак з боку певних груп, але не після кожних виборів, а лише тоді, коли у груп є інтерес або ресурс. Складність у прогнозуванні тут полягає в тому, що ці тимчасові закономірності мають «строк придатності» - сьогодні вони діють, а завтра можуть зникнути. Тому необхідно заздалегідь визначити індикатори, які показують, що закономірність ще актуальна, та контролювати їхній стан. Наприклад, розглянемо наступну ситуацію: під час «чорної п'ятниці» та великих онлайн-розпродажів майже завжди зростає кількість фішингових атак (зловмисники надсилають підроблені листи від імені магазинів). Закономірність: атаки зазвичай починаються за 3–5 днів до старту акції і тривають ще 1–2 тижні після неї. Індикатори: у спам-пошті з'являються листи з темами «знижка», «акція», «Black Friday»; зростає кількість реєстрацій доменів, схожих на відомі бренди (amaz0n-sale.com). Складність: ця закономірність спрацьовує не завжди однаково (в один рік атаки можуть бути масовими, в інший — менш відчутними); прогноз треба коригувати, якщо індикатори не підтверджують активності зловмисників.

Найскладнішою у прогнозуванні є робота з ***унікальними*** ситуаціями. Тут необхідно виявити ті елементи події, що вивчається, які не унікальні, а рідкісні і регулярні, оскільки «унікальна подія» рідко є повністю новою у всьому, часто - це нова комбінація вже відомих елементів (акторів, мотивів, технік, умов). Прогнозування працює саме з цими неунікальними «цеглинками». При виявленні достатньої кількості таких елементів можна будувати прогноз з урахуванням законів, регулюючих їх розвиток. У цій ситуації важливо зрозуміти, що відіграє першорядну роль у досліджуваній ситуації і саме ці елементи піддати більш глибокого аналізу. Власне, прогнозування застосовується щодо ситуацій чи подій, які насправді унікальні, але мають деталі, схожі з деталями інших ситуацій чи подій. Чому це працює? Навіть «унікальні» інциденти підпорядковані відносно стійким законам:

- обмеженням ресурсів атакувальника;
- типовым людським помилкам;
- економіці атаки (легші/дешевші вектори - частіші);
- життєвим циклам вразливостей і кампаній.

Тож ми шукаємо повторюваність у деталях, виділяємо, накладаємо відомі закономірності і лише потім комбінуємо це у прогноз.

Прогнозування має свої обмеження та не дає однозначної відповіді на запитання "Що буде завтра?". Дійсно, дані не можуть бути абсолютно повними, ми ніколи не маємо абсолютно всієї інформації. Наприклад, у кібербезпеці частина атак залишається прихованою, деякі індикатори ще не виявлені. Умови змінюються. Подія прогнозується в умовах «стану сьогодні», але завтра середовище може різко змінитися. Наприклад, компанія встигла оновити всі сервери, і прогноз «масова експлуатація вразливості» стає неактуальним. Невизначеність в те, "Що буде завтра?", вносить людський фактор і випадковість: поведінка людей і груп (користувачів, зловмисників, політиків) може бути непередбачуваною. Наприклад, хакерська група може переключитися на іншу ціль з економічних мотивів. Тому, даючи прогноз, завжди необхідно обумовлювати умови та межі розвитку конкретної ситуації.

Умови - це обставини, за яких прогноз буде справджуватися. Наприклад, маємо прогноз: «Якщо компанія не випустить патч протягом 2 тижнів …». Межі тут - це часові або ситуаційні рамки, поза якими прогноз може втратити актуальність: «Прогноз діє для періоду до кінця місяця; після цього дані потребують оновлення». Розглянемо приклад. Прогноз: «Ймовірно, протягом найближчих 10 днів відбудуться атаки через нову вразливість у VPN-сервісі». Умови: якщо вразливість залишиться непатченою; якщо зловмисники мають інтерес саме до цього сектора. Межі: до моменту виходу стабільного оновлення (патчу) прогноз діє; після - його потрібно переглянути.

Таким чином, прогноз - це гіпотеза з умовами, а не абсолютна істина. Тому в аналітичній роботі завжди вказують: що саме прогнозується, за яких умов він справджується, до якого часу або за яких обставин прогноз діє.

6. Особливості прогнозування в інформаційній безпеці

Прогноз у ІБ не дає гарантії, він лише підвищує готовність. Щоб зменшити ризик помилок, треба регулярно оновлювати прогнози, перевіряти дані з кількох джерел, працювати із сценаріями, а не з «єдиним варіантом майбутнього».

У прогнозуванні в ІАР (зокрема в інформаційній безпеці) виділяють епізодичне, регулярне та постійне.

Епізодичне прогнозування: виконується «разово», коли потрібно прийняти конкретне рішення, тут немає системності, а лише реакція на певну ситуацію. Наприклад, компанія планує запустити новий онлайн-сервіс і проводить прогноз атак на нього, щоб визначити необхідний рівень захисту.

Регулярне прогнозування: виконується періодично (раз на квартал, рік чи перед плануванням нових стратегій), має системність, але не є безперервним процесом. Наприклад, банк щоквартально прогнозує зростання DDoS-атак і коригує бюджет на кіберзахист.

Постійне прогнозування: вбудоване в систему управління та моніторингу - працює безперервно, часто із застосуванням автоматизованих систем (SIEM, ML). Наприклад, SOC використовує машинне навчання, щоб постійно прогнозувати можливі «ланцюжки атак» і попереджати інциденти в реальному часі.

Прогнозування в інформаційній безпеці (ІБ) має свої особливості, які відрізняють його від прогнозів у економіці чи, наприклад, політиці (див.табл.).

Таблиця 4.3. Особливості прогнозування в ІБ

Особливість	Що означає	Приклад з ІБ
Динамічність загроз	Загрози швидко змінюються, прогноз діє обмежений час.	Zero-day у VPN: через кілька днів з’являється експлойт → масові атаки.
Асиметричність	Захисник має враховувати десятки сценаріїв, нападнику достатньо одного.	SOC прогнозує 10 можливих векторів атаки, а зловмисники використовують лише

		один — але успішно.
Залежність від технологій	Нові технології майже відразу створюють нові ризики.	Поширення IoT → нові ботнети (типу Mirai).
Невидимі фактори	Дані часто неповні, багато чого приховано у даркнеті чи закритих каналах.	Прогноз базується на кількох витоках даних і непрямих ознаках активності групи.
Людський фактор і мотивація	Важливі не лише технічні дані, а й наміри та цілі атакуючих.	Anonymous прогнозують атаки на держсайти у відповідь на політичну подію.
Ймовірнісний характер	Прогноз не дає «так/ні», лише ступінь ймовірності.	«Є висока ймовірність зростання фішингових атак у грудні через сезон покупок».

Таким чином, засоби підтримки ІАР (бази знань, інструменти моніторингу, аналітичні системи, моделювання) забезпечують аналітиків технологічною та методичною основою, вони дозволяють збирати, структурувати та обробляти інформацію з різних джерел; моніторинг виконує роль «радару»: він постійно відстежує середовище, формує базову модель «нормального стану», виявляє відхилення та сигнали загроз, що дає можливість своєчасно реагувати на зміни; прогнозування доповнює моніторинг, дозволяючи не лише бачити теперішнє, але й оцінювати майбутні сценарії розвитку ситуації, і хоча у сфері інформаційної безпеки прогнози завжди ймовірнісні, проте саме вони дають керівництву можливість діяти на випередження. Усе це інтегрується в систему інформаційно-аналітичного забезпечення інформаційної безпеки, яка поєднує технічні засоби, організаційні структури й професіоналізм аналітиків.

Таким чином, ІАЗ інформаційної безпеки — це комплексний процес, де: засоби підтримки дають інструменти, моніторинг створює картину поточного стану, прогнозування дозволяє передбачати розвиток подій, а все разом забезпечує захист організації від сучасних і майбутніх загроз.

Питання

1. Пояснити, від чого залежить вибір засобів підтримки ІАР.
2. Пояснити, що представляє моніторинг у межах ІАР, його цілі. Різновиди моніторингу.
3. Пояснити, що таке формальний та інформальний моніторинг.
4. Пояснити, в чому полягає важливість моніторингу у межах ІАР.
5. Прогнозування як ключовий інструмент ІАР. Цілі прогнозування в ІАР.
6. Порівняння моніторингу і прогнозування в межах ІАР.
7. В чому полягають особливості прогнозування в інформаційній безпеці.

Тема 5. УНІКАЛЬНІСТЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

План

1. **Технічна насиченість інформаційно-аналітичного забезпечення в інформаційній безпеці**
2. **Короткий життєвий цикл даних**
3. **Взаємодія людини й автоматики як унікальна риса інформаційно-аналітичного забезпечення в інформаційній безпеці**
4. **Мультидоменність даних в інформаційно-аналітичному забезпеченні інформаційної безпеки**

1. Технічна насиченість ІАЗ в ІБ

Інформаційно-аналітичне забезпечення у сфері інформаційної безпеки принципово відрізняється від аналогічних процесів в економіці, політології чи соціології. Якщо в гуманітарних чи соціальних дослідженнях аналітик переважно працює з текстами, документами, інтерв'ю та звітами, то в інформаційній безпеці 80% і більше інформації надходить із машинних джерел: це системні та прикладні логи, мережевий трафік, телеметрія від захисних агентів, сповіщення SIEM і SOC-систем.

Система SIEM (Security Information and Event Management) - це один із ключових інструментів в інформаційній безпеці. Вона поєднує дві функції:

- збір, зберігання і базова обробка логів та безпекових подій з різних систем (серверів, мережевого обладнання, додатків, баз даних тощо);
- аналіз подій у реальному часі, виявлення підозрілих патернів та формування тривог (alerts).

SIEM збирає логи з усіх систем (хто увійшов, що робив, які помилки, які з'єднання були відкриті); уніфікує ці дані у спільний формат (бо логи з різних систем різні); використовує кореляційні правила або машинне навчання (ML), щоб зрозуміти, ця подія сама по собі не підозріла, але разом із іншими вона виглядає як атака; генерує тривоги для аналітиків SOC.

SIEM **потрібна** у контексті ІАЗ інформаційної безпеки для постійного збору і контролю подій; виявлення складних сценаріїв атак (ланцюжки подій); іноді SIEM з ML може передбачити потенційну атаку ще до того, як вона завершиться.

Але SIEM не замінює аналітика:

SIEM вміє збирати дані, співставляти події за заданими правилами або шаблонами, іноді - застосовувати машинне навчання, але інтерпретувати, що це означає для конкретної організації, SIEM не здатна. Вона часто генерує «шум». У середньому до 80% алертів SIEM виявляються хибними (false positives). **Лише аналітик може відфільтрувати, що справді небезпечно, а що випадковість**.

SIEM не знає бізнес-контексту. Наприклад, вона побачить масове копіювання файлів і може сигналізувати витік. А аналітик знає, що сьогодні відбувається планове резервне копіювання.

SIEM не робить стратегічних висновків. Вона не відповість на питання: «Чи пов’язана ця активність із кампанією певної хакерської групи?», «Які ризики для компанії на рівні репутації чи фінансів?». **Це робота аналітика**.

SOC (Security Operations Center) - це центр моніторингу та реагування на інциденти інформаційної безпеки; це не лише система чи програма, а організаційна структура (підрозділ), де працюють фахівці з кібербезпеки, які постійно стежать за подіями у мережі та IT-інфраструктурі; реагують на інциденти; проводять розслідування атак; готують аналітичні звіти для керівництва. SOC - комплекс: оперативна робота + аналітика + стратегія, можна сказати, що це «серце кіберзахисту» організації, де щодня відбувається і технічне реагування, і аналітичне осмислення подій. Якщо в організації є аналітичний відділ, то SOC може бути його «кіберпідрозділом» або окремою структурою в службі безпеки. Все залежить від масштабу й профілю компанії.

По-перше, це визначає масштаб і обсяг даних. Кожна операційна система, сервер або навіть окремий додаток може генерувати тисячі повідомлень на хвилину. У великій інфраструктурі цей потік легко досягає мільйонів подій на добу. Аналітик уже не може переглянути всі записи вручну, як у класичній документальній роботі, — потрібні автоматизовані методи збору, нормалізації й попереднього аналізу даних.

По-друге, важливою проблемою інформаційно-аналітичного забезпечення у сфері інформаційної безпеки є різноманітність форматів даних, з якими доводиться працювати. Частина джерел подає інформацію у чітко структурованому вигляді, наприклад у вигляді таблиць або журналів із фіксованими полями «дата», «час», «IP-адреса», «результат входу». Інші формують напівструктуровані повідомлення у форматах JSON чи XML, де певні поля чітко виділені, але одночасно міститься вільний текст на кшталт «user login failed due to invalid password». А бувають і зовсім неструктуровані дані — це звіти у PDF, електронні листи, повідомлення користувачів чи статті в інтернеті.

Ситуацію ускладнює ще й те, що різні виробники обладнання та програмного забезпечення описують однакові події у власних специфічних форматах. Наприклад, Cisco, Microsoft і Palo Alto можуть фіксувати невдалу спробу входу кожен по-своєму. Для людини така відмінність не критична, але для аналітичних систем — це перешкода, адже для автоматизованого аналізу всі події мають бути приведені до єдиного стандарту.

Щоб впоратися з цим завданням, аналітик має володіти не лише методами аналізу, але й технічними інструментами для обробки даних. Найпростіший спосіб - використання регулярних виразів, які дозволяють автоматично «витягати» ключові фрагменти з тексту. Наприклад, у повідомленні про невдалий вхід регулярний вираз може виділити ім’я користувача та IP-адресу. У більш складних випадках застосовуються скрипти мовою Python, Bash чи PowerShell, які перетворюють «сирі» журнали у стандартизований вигляд, придатний для завантаження в SIEM. Для великих обсягів даних зазвичай організовуються ETL-процеси: спершу дані витягуються з різних джерел, далі трансформуються — очищуються та уніфікуються, і зрештою завантажуються в аналітичні системи.

Таким чином, сучасний аналітик у сфері інформаційної безпеки - це «гібридний» фахівець. Він повинен не лише вміти встановлювати причинно-наслідкові зв'язки та робити висновки, але й мати технічні навички попередньої обробки інформації. Без здатності підготувати дані за допомогою регулярних виразів, скриптів або ETL-процесів аналітична робота у сфері інформаційної безпеки просто неможлива.

По-третє, варто підкреслити обмежену інформативність окремих записів. Один рядок у журналі подій здебільшого майже нічого не «розповідає» про ситуацію. Наприклад: запис «невдала спроба входу користувача admin» може означати як випадкову помилку при наборі пароля, так і початок атаки перебору паролів. Повідомлення «отримано пакет із зовнішньої IP-адреси» може бути нормальним трафіком, а може - першим етапом сканування портів. Цінність виникає лише тоді, коли аналітик або система безпеки виконує кореляцію подій, тобто встановлює взаємозв'язки між різними повідомленнями з різних джерел. Саме в кореляції сутність роботи з великими потоками технічних даних. **Наприклад**, якщо з одного й того ж IP надходить понад 50 невдалих спроб входу за короткий час, паралельно спостерігається підозрілий мережевий трафік і раптові зміни в реєстрі Windows - це вже не випадковість, а комплексна подія, що свідчить про спробу атаки.

Ще одна важлива особливість - **часовий фактор**. Машинні дані приходять у режимі реального часу. Від швидкості їхньої обробки й аналізу залежить, чи встигне організація відреагувати на атаку. На відміну від економічних чи політичних процесів, де часто можна дозволити собі дні чи навіть тижні для обдумування, в інформаційній безпеці час реакції вимірюється хвилинами й секундами.

Таким чином, **специфіка** роботи з машинно-генерованими даними в ІАЗ для ІБ полягає у трьох ключових моментах:

- величезні обсяги, що потребують автоматизації;
- різноманітність форматів і необхідність нормалізації;
- потреба в кореляції та контексті, оскільки окремі події самі по собі нічого не означають.

Приклад. Ситуація: Система SIEM зафіксувала збільшення кількості невдалих входів у корпоративну пошту з однієї IP-адреси. Згодом надійшли тривоги з IDS/IPS про спроби сканування внутрішньої мережі.

Оперативні дії (фахівці з ІБ):

- заблокували підозрілий IP-адрес;
- перевірили облікові записи, де були спроби входу;
- провели первинний аналіз логів.

Аналітична робота:

- Встановлення контексту: аналіз трендів у логах показав, що подібна активність спостерігається вже кілька днів із різних IP-адрес. Це свідчить не про випадкову атаку, а про цілеспрямовану кампанію.
- Виявлення причинно-наслідкових зв'язків: невдалі входи та сканування мережі свідчить про етап розвідки перед реальною атакою.
- Прогноз розвитку подій: наступними кроками, ймовірно, буде використання вразливостей у веб-серверах або фішинг для отримання

паролів.

- Висновки для керівництва: існує загроза початку скоординованої атаки на корпоративну пошту, яка може призвести до витоку комерційної інформації.
- Рекомендації:
  - підсилити моніторинг входів у поштові сервіси;
  - провести позачергове оновлення систем автентифікації;
  - організувати інструктаж співробітників щодо фішингу.

У результаті керівництво отримує не просто факт («були невдалі входи»), а аналітичний продукт: розуміння що це означає, які наслідки можливі та що робити далі.

Таким чином, **аналітик ІБ** - це не лише «читач документів», а й інтерпретатор машинних сигналів, тому в ІБ формується новий профіль аналітика: знання ІТ-інфраструктури, навички роботи з великими даними, здатність до швидкої кореляції технічних індикаторів із реальними загрозами.

2. Короткий життєвий цикл даних

У сфері ІБ інформація швидко втрачає цінність. Те, що було індикатором атаки сьогодні, завтра вже може бути непридатним. Це дуже важливе питання для розуміння специфіки інформаційно-аналітичного забезпечення у сфері інформаційної безпеки.

Дані в ІБ дійсно мають короткий життєвий цикл: подія виникає, фіксується у логах або телеметрії, через деякий час вона вже втрачає актуальність, а далі стає просто історичною довідкою. Це принципово відрізняє ІБ від багатьох інших сфер, де дані можуть залишатися корисними десятиліттями (наприклад, у демографії чи економіці).

Для ІАЗ це має кілька **наслідків**:

- Пріоритет оперативності над глибиною аналізу. Аналітик часто не може дозволити собі тривале вивчення даних: загроза розвивається у реальному часі, і рішення треба ухвалювати швидко.
- Необхідність безперервного збору та оновлення. Моніторинг і логування мають бути постійними, інакше можна пропустити критичний момент. Дані не можна накопичувати «на потім» - у багатьох випадках у ІБ пізній аналіз втрачає сенс.
- Високі вимоги до автоматизації. Людина фізично не встигає реагувати на весь потік подій. Тому SIEM-системи, системи поведінкового аналізу (UEBA), алгоритми машинного навчання беруть на себе завдання миттєвої обробки та фільтрації.
- Ризик інформаційного «шуму». Оскільки дані постійно народжуються і швидко застарівають, надмірна їх кількість може паралізувати роботу аналітика. Завдання ІАЗ - відсіяти несуттєве і вчасно виділити те, що дійсно має значення.
- Особлива роль історичних даних. Попри короткий цикл актуальності, старі журнали можуть зберігати аналітичну цінність у вигляді шаблонів чи «базових моделей нормальної поведінки». Але їх цінність уже не оперативна, а стратегічна: вони потрібні для тренування моделей

прогнозування, пошуку закономірностей або судових розслідувань.

Таким чином, короткий життєвий цикл даних робить ІАЗ в ІБ дуже «швидкісним» і технологічно насиченим процесом. Тут аналітик повинен не тільки розуміти суть подій, а й вміти працювати в умовах дефіциту часу, коли вартість затримки вимірюється не годинами чи днями, а хвилинами або навіть секундами.

Розглянем практичний **приклад** із SOC (центру безпеки), де короткий цикл даних змушує працювати інакше, ніж у звичайній аналітиці. Уявімо, що в компанії спрацювало правило SIEM: на одному з серверів виявлено серію невдалих спроб входу під адміністраторським обліковим записом. З урахуванням короткого життєвого циклу даних ця інформація актуальна буквально хвилини. Якщо зараз хтось намагається підібрати пароль і проб'є захист, то сервер буде зламано. Завтра цей лог може бути лише «слідством», але вже не дасть змоги запобігти інциденту. Коли аналітик SOC отримує цю подію у SIEM, його завдання - відрізнити, чи це легітимна активність (наприклад, адміністратор забув пароль) чи атака (brute force). Для цього він швидко перевіряє:

- чи є ці спроби входу з незвичної IP-адреси;
- чи збігається час активності з робочим графіком співробітника;
- чи є паралельні підозрілі події (наприклад, спроби з інших серверів).

На це у нього буквально 5–10 хвилин, бо якщо аналітик «зависне» у тривалому аналізі, подія стане історичною, сервер уже буде зламано. Через день цей лог все ще має значення - його додають у базу для статистики атак, будують модель «нормальної поведінки» і тренують систему розпізнавання brute force. Але для оперативної роботи він уже не корисний. Тому рішення ухвалюється швидко, SOC може заблокувати підозрілий IP або тимчасово відключити акаунт, при цьому у SOC завжди існує ризик помилкових рішень, якщо діяти занадто швидко, наслідки яких є негативними. Наприклад, адміністратор дійсно кілька разів неправильно ввів пароль із дому, бо клавіатура була з іншим розкладом, SOC блокує його IP, і він не може підключитися до системи. У результаті зупиняється планове оновлення, що мало бути проведено терміново. Ще один приклад: блокування акаунта може зачепити критичний бізнес-процес. Якщо це акаунт сервісу, який обслуговує клієнтські запити в реальному часі, кілька хвилин простою приведе до значної втрати грошей і довіри клієнтів. Але дії аналітика в галузі ІБ повинні все одно бути швидкими, бо тут діє принцип: краще переблокувати, ніж пропустити атаку. Але щоб уникнути шкоди від неправильних рішень, у SOC існують механізми «страховки»:

- Playbooks (заздалегідь підготовлені сценарії), які визначають, які дії дозволені аналітику першого рівня, а які потребують підтвердження старшого колеги. Наприклад, заблокувати IP можна відразу, а відключати акаунт сервісу - лише після узгодження;
- Multi-source correlation (перевірка з інших джерел): SIEM і SOAR системи автоматично перевіряють, чи збігається підозріла активність із іншими сигналами (геолокація, поведінка користувача, попередні логи). Якщо підтвердження немає - діють більш обережно;
- Рівні доступу: молодший аналітик може тільки сповістити або тимчасово

ізолювати подію. Остаточне рішення - за старшим аналітиком.

Отже, швидкі рішення в SOC - це завжди баланс між ризиком «пропустити атаку» і «нашкодити своїми діями». Саме тому важлива чітка регламентація та багаторівнева система перевірок. В SOC дуже добре видно, як короткий життєвий цикл даних впливає на інформаційно-аналітичне забезпечення: дані мають найбільшу цінність «тут і зараз», а згодом перетворюються на історичний матеріал.

3. Взаємодія людини й автоматики як унікальна риса ІАЗ в ІБ

У ІТ-галузі, зокрема ІБ, жоден рівень автоматизації **не знімає потреби** в аналітику-людині, бо саме він визначає контекст (чи подія критична саме для цієї організації), ухвалює управлінські рішення, прогнозує сценарії. Особливість ІАЗ тут - це поєднання машинної швидкості та людського розуміння контексту.

В ІТ-галузі, зокрема в інформаційній безпеці, автоматика не просто «допомагає» людині, як у класичній економічній чи соціологічній аналітиці. Вона виступає першою лінією сприйняття світу, адже жодна людина фізично не здатна переглянути мільйони логів, пакетів чи системних подій. Машини беруть на себе сенсори й попередню фільтрацію, але саме людина додає те, чого не може автоматика:

- ***Контекстуальність***: система може бачити підозрілу активність, але не знає, що в цей момент у компанії відбувається, наприклад, міграція серверів. Аналітик здатен «поставити крапку над і»;
- ***Етичність і відповідальність***: автоматика може запропонувати блокування доступу, але рішення про вплив на реальних користувачів приймає людина, бо воно може зачепити бізнес-процеси;
- ***Креативність і інтуїція***: автоматика працює на основі заданих правил чи моделей. Людина здатна побачити атиповий збіг подій, який не вписується в шаблони.

Таким чином, в ІАЗ для ІТ-галузі, зокрема для ІБ, формується **симбіоз**: автоматика забезпечує швидкість, повноту та масштабність, а аналітик забезпечує осмислення, пріоритезацію та стратегічне бачення. Але ***для інформаційної безпеки ця взаємодія має кілька специфічних унікальних рис***, яких немає в інших галузях:

1. ***Непередбачуваність протидіючої сторони***: у більшості ІТ-завдань автоматика працює з відносно стабільними процесами (бізнес-аналітика, прогнозування трафіку). В ІБ проти системи завжди стоїть активний опонент - зловмисник, який адаптується, маскується, намагається обдурити алгоритм. **Унікальністю тут є те, що автоматика без людини обов'язково програє, бо злочинець швидко знайде спосіб обійти шаблон. Аналітик має передбачати дії супротивника**;
2. ***Ціна помилки:*** в будь-якій сфері ІТ помилка автоматики може дорого коштувати - збій у банківській системі, втрата клієнтських даних тощо. Але в інформаційній безпеці «ціна помилки» має свою специфіку:

- Невидимість і відкладений ефект: у розробці чи експлуатації збій видно одразу: система падає, додаток не працює. В ІБ помилка «не помітили атаку» може проявитися лише через тижні чи місяці, коли дані вже

вкрадені або мережу захоплено. Тобто шкода накопичується непомітно й стає явною занадто пізно, що обов'язково треба передбачати аналітику;

- Прямий контакт із супротивником: у більшості ІТ-проблем немає «противної сторони». Це просто технічний збій. В ІБ завжди є зловмисник, який **використовує** помилку на свою користь. Він може спеціально створювати умови для хибних спрацьовувань, «засипати» систему шумом, щоб відволікти аналітиків. У такому випадку одна помилка - це виграна атака супротивника.
- Репутаційна втрата: у класичних ІТ-проектах збитки вимірюються у втрачених годинах роботи чи фінансах. В ІБ головний удар часто припадає по довірі користувачів і партнерів. Наприклад, після витоку даних навіть компанія, що швидко відновила сервіси, може втратити клієнтів назавжди.
- Каскадний характер: помилка безпеки рідко обмежується одним інцидентом. Компрометація одного сервера може призвести до компрометації всієї мережі. Це принципово відрізняє ІБ від «звичайних» ІТ-системних помилок, де збитки локалізовані.

Отже, унікальність «ціни помилки» в інформаційно-аналітичному забезпеченні інформаційної безпеки - вона затримана в часі, використовується супротивником, руйнує довіру та може мати каскадний ефект. Саме тому автоматика і людина в ІБ повинні бути «заплетені» в багаторівневий цикл перевірок, чого так строго не роблять в інших ІТ-сферах.

3. Постійне нарощування «арсеналу»: в ІБ автоматика постійно збагачується новими індикаторами компрометації, сигнатурами, моделями ML. У жодній іншій ІТ-галузі немає такої масової проблеми «false positive», що змушує автоматику й людину працювати тандемом.

Але унікальність взаємодії людини й автоматики в ІАЗ для ІБ не лише в тому, що «зловмисники активні» чи «ціна помилки висока». **Тут формується особлива модель довіри**:

- аналітик не може повністю довіряти автоматиці, бо знає про false positives і обхідні шляхи атак;
- автоматика не може повністю «довіряти» людині, бо без неї швидкість реагування буде недостатня.

В результаті створюється гібридний контур довіри, де рішення приймаються на стику алгоритмічного й людського мислення. Це радше соціотехнічна специфіка інформаційної безпеки, а не просто ще один технічний аргумент. У жодній іншій ІТ-галузі поняття «довіра між людиною й машиною» не стоїть настільки гостро, як у кібербезпеці, де «помилка довіри» може коштувати компрометації всієї системи і навіть вимірюватися життями людей.

Таким чином в кібербезпеці формується унікальна **соціотехнічна система довіри**, де жодна зі сторін - ані людина, ані автоматика - не має монополії на істину. Автоматика «довіряє» людині завершальне тлумачення, а людина «довіряє» автоматиці попереднє сприйняття подій. У підсумку рішення формується в точці перетину цих двох довір. Цей баланс робить інформаційно-аналітичне забезпеення для інформаційної безпеки відмінним від будь-якої іншої сфери. У наукових дослідженнях, економіці чи соціології аналітик може

покладатися на автоматику як на інструмент. В ІБ автоматика стає рівноправним партнером, з яким потрібно будувати відносини довіри, перевірок і взаємної валідації.

4.Мультидоменність даних в інформаційно-аналітичному забезпеченні інформаційної безпеки

Особливістю інформаційно-аналітичного забезпечення інформаційної безпеки є необхідність працювати одночасно з кількома різними доменами даних. Це означає, що аналітик не може зосередитися лише на технічних або організаційних аспектах, а повинен інтегрувати інформацію з різних рівнів:

- ***Технічний рівень***: найбільш очевидне джерело даних, яке ми детально розглядали вище (логи серверів, мережевий трафік, сигнали SIEM, повідомлення від IDS/IPS-систем, антивірусів). Тут аналітик має справу з великими потоками машинної інформації, де важлива швидкість обробки та виявлення аномалій.
- ***Організаційний рівень***: без знання бізнес-процесів і політик безпеки навіть найкращий технічний сигнал буде відірваним від реальності. Наприклад, для однієї компанії масове копіювання файлів на флешку може бути нормальною процедурою (резервне копіювання відділу), а для іншої — серйозною загрозою витоку даних.
- ***Людський рівень***: користувачі — це **завжди слабка ланка** в інформаційній безпеці. Аналітик має враховувати соціальні та психологічні фактори: фішингові кампанії, ризики інсайдерів, поведінкові аномалії. Дані з цього рівня часто неструктуровані: звіти служби кадрів, відгуки співробітників, навіть публікації у соцмережах.
- ***Зовнішній контекст***: жодна організація не існує у вакуумі. Нові уразливості (CVE), діяльність хакерських угруповань, кібервійни, геополітичні загрози - усе це теж дані, які аналітик повинен інтегрувати в роботу.

В ІТ-аналітиці теж можуть з’являтися всі ці рівні, але у специфіці інформаційної безпеки важливе не саме існування цих рівнів. В інформаційній безпеці аналітик працює не просто з різними рівнями даних, а з їхньою постійною інтеграцією. Якщо в інших напрямах ІТ-аналітики можна обмежитися переважно одним доменом, наприклад, бізнес-аналітик працює з організаційними процесами й людською поведінкою, а інженер моніторингу з технічними даними, то в кібербезпеці цього категорично недостатньо. Тут аналітик змушений одночасно враховувати технічні логи й телеметрію, внутрішні політики компанії, поведінку користувачів та зовнішній фон загроз. Лише **синтез** усіх рівнів дає можливість побачити реальну картину подій.

Особливе значення має здатність «зшивати» ці дані. В інформаційній безпеці цінним є не окремий сигнал, наприклад, факт аномалії в мережевому трафіку, а саме зв’язок цього сигналу з поведінкою користувача, поточними політиками доступу чи глобальними кібератаками. Саме завдяки такому крос-доменному аналізу виявляються складні багатоступеневі атаки, які неможливо зафіксувати, аналізуючи дані лише в межах одного рівня.

Людський фактор у сфері інформаційної безпеки теж набуває особливого значення. Якщо в класичних ІТ-системах користувач розглядається здебільшого

як клієнт або кінцевий споживач, то в безпеці він може виступати у кількох ролях одночасно. Це і потенційна жертва фішингових атак чи соціальної інженерії, і випадковий порушник правил, що нехтує політиками безпеки, і навіть свідомий інсайдер, який має доступ до критичних ресурсів. Ця подвійна природа людини - як активу та водночас загрози - є унікальною саме для сфери ІБ.

Не менш важливим є зовнішній контекст. Якщо в інших ІТ-напрямах зовнішнє середовище - ринок, конкуренція чи нові технології - важливе, але не завжди критичне, то в інформаційній безпеці воно є невід'ємною частиною аналітичної картини. Атака може прийти звідки завгодно: від міжнародної хакерської групи, конкурентів, державних акторів або ж бути наслідком появи нових вразливостей у програмному забезпеченні. Тому постійний моніторинг зовнішніх факторів - це органічна частина інформаційно-аналітичного забезпечення безпеки.

Таким чином, специфіка ІАЗ у сфері інформаційної безпеки полягає не лише у багаторівневості даних, а насамперед у необхідності їх постійного поєднання, інтерпретації та контролю. Без цього аналітика стає безсилою, а ціна помилки - набагато вищою, ніж у більшості інших ІТ-дисциплін.

Розглянемо **приклад** мультидоменного підходу. SOC отримує сигнал від SIEM:

- Технічний рівень: виявлено аномальний мережевий трафік із внутрішнього сегмента;
- Організаційний рівень: цей сегмент належить фінансовому відділу, де працюють із конфіденційними документами;
- Людський рівень: у цей час у компанії звільняється працівник, який мав доступ до цього сегмента й конфліктував із керівництвом;
- Зовнішній контекст: на форумах даркнету з'явилися оголошення про продаж доступу до корпоративних систем у цьому регіоні.

Лише інтеграція цих шарів дозволяє зробити правильний висновок: це не просто аномальний пакет даних, а потенційно інсайдерський витік, пов'язаний із конкретною особою і підсилений зовнішніми загрозами.

Таким чином, мультидоменність — це унікальна риса ІАЗ для ІБ. Вона змушує аналітика поєднувати машинні дані, бізнес-контекст, людський фактор і зовнішні події, щоб побудувати цілісну картину загроз.

Питання

1. В чому полягає специфіка роботи з машинно-генерованими даними в ІАЗ для ІБ?
2. Поясніть, що означає, що дані в ІБ мають короткий життєвий цикл. Які це має наслідки для ІАЗ?
3. Взаємодія людини й автоматики як унікальна риса ІАЗ в ІБ. Поняття соціотехнічної системи довіри.
4. Мультидоменність даних в інформаційно-аналітичному забезпеченні інформаційної безпеки.

Рекомендована література та інші джерела інформації

Базова

1. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. https://duikt.edu.ua/uploads/l_2230_88161692.pdf

2. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. ; під ред. В. В. Остроухова. – К. : Видавництво Ліра-К, 2021. – 412 с. https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf

3. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т.В.Магеровська. – Львів : ЛьвДУВС, 2024. –192 с. https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf

4. Отрешко В. Інформаційна безпека в контексті мовних пріоритетів українського державотворення/ В.Отрешко // Гілея: науковий вісник: збірник наукових праць.– К. : Видавництво “Гілея”, 2014.

Допоміжна

4. Маковій В. П. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави / Морська безпека та оборона, N 1, 2023, с.62-68.
https://www.bing.com/search?q=%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D0%B5+%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F+%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8&pc=MOZI&form=MOZTSB

Інтернет ресурси

1. https://pidru4niki.com/16520415/politologiya/sutnist_informatsiyno-analitichnogo_zabezpechennya_derzhavnogo_upravlinnya_sferi_bezpeki
2. https://vestnik-pravo.mgu.od.ua/archive/juspradenc42/part_2/15.pdf
3. https://pidru4niki.com/15830523/politologiya/viznachennya_tsili_zavdannya_informatsiyno-analitichnogo_zabezpechennya_iaz