ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ ЗАСОБІВ БАГАТОВИМІРНОГО ВІЗУАЛЬНОГО АНАЛІЗУ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Євгеній ГАВРИЛЕНКО

Виконав: здобувач вищої освіти групи БСДМ-63
ГАВРИЛЕНКО Євгеній
(ПРІЗВИЩЕ, Ім'я)

Керівник: БОРСУКОВСЬКИЙ Юрій
к.т.н, доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: Туровський О.Л.
(Прізвище, ініціали)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гавриленку Євгенію Дмитровичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
корпоративна інформаційна система;
технологія управління розслідуванням кіберінцидентів на базі рішення i2 Analyst’s Notebook;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності розслідування кіберінцидентів.
2. Методи та засоби розслідування кіберінцидентів.
3. Розроблення варіанта технології застосування засобів багатовимірного

візуального аналізу на базі рішення i2 Analyst’s Notebook.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми розслідування кіберінцидентів в корпоративній інформаційній системі.	26.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	02.11.2023 р.	
3.	Аналіз необхідності розслідування кіберінцидентів.	09.11.2023р.	
4.	Методи та засоби розслідування кіберінцидентів.	23.11.2023 р.	
5.	Розроблення варіанта технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst’s Notebook.	07.12.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату.	15.12.2023 р.	
7.	Підготовка доповіді до захисту.	15.01.2024 р.	

Здобувач вищої освіти _____ Євгеній ГАВРИЛЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Гавриленко Є.Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ГАВРИЛЕНКО Євгеній*** обрав тему роботи, метою якої було дослідити зміст технології застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ГАВРИЛЕНКО Євгеній*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ГАВРИЛЕНКА Євгенія*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач ***ГАВРИЛЕНКО Євгеній*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Гавриленка Євгенія
на тему: «Технологія застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів».

Актуальність:

Метою кожної компанії є організація процесу швидкого та ефективного розслідування кіберінцидентів. Занадто повільний, зовсім неефективний процес розслідування кіберінцидентів, чи відсутність процесу як такого може призвести до втрати активів і репутації компанії, тому компаніям потрібно зосередити свою увагу на впровадженні технологій застосування засобів багатовимірного візуального аналізу. Одним із таких рішень є i2 Analyst's Notebook, яке розкриває зв'язки між об'єктами даних, щоб виявити шаблони та надати розуміння даних. Саме тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми розслідування кіберінцидентів.
2. Досліджено методи та засоби розслідування кіберінцидентів.
3. Запропоновано варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. Запропонований варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook доцільно було б показати на прикладі конкретної компанії.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ГАВРИЛЕНКО Євгеній** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ Туровський О.Л.
підпис *Прізвище, ініціали*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 82 сторінки, 17 рисунків, 1 таблиця, 15 джерел.

Об'єкт дослідження – процес розслідування кіберінцидентів у корпоративній інформаційній системі.

Предмет дослідження – технологія застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів на базі рішення i2 Analyst's Notebook.

Мета роботи – розробити варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook для корпоративної інформаційної системи та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу розслідування кіберінцидентів на базі рішення i2 Analyst's Notebook.

В роботі проведено аналіз проблеми розслідування кіберінцидентів. Проаналізовано існуючі технології розслідування кіберінцидентів.

Досліджено методи та засоби розслідування кіберінцидентів.

Запропоновано варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook. Визначено призначення, основні функції та склад компонентів даної технології.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, БАГАТОВИМІРНИЙ ВІЗУАЛЬНИЙ АНАЛІЗ, МЕТОДИ ТА ЗАСОБИ ЗАСТОСУВАННЯ ЗАСОБІВ БАГАТОВИМІРНОГО ВІЗУАЛЬНОГО АНАЛІЗУ, ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ ЗАСОБІВ БАГАТОВИМІРНОГО ВІЗУАЛЬНОГО АНАЛІЗУ

ABSTRACT

The text part of the master's qualification work consists of 82 pages, 17 figures, 1 table, and 15 sources.

The purpose of the work is to develop a variant of the technology for the use of multidimensional visual analysis tools based on the i2 Analyst's Notebook solution for the corporate information system and recommendations for the use of the technology.

Object of research – the process of investigating cyber incidents in the corporate information system.

Subject of research – the technology of using multidimensional visual analysis tools during the investigation of cyber incidents based on the i2 Analyst's Notebook solution.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison, modeling of the cyber incident investigation process based on the i2 Analyst's Notebook solution.

The paper analyzes the problem of investigating cyber incidents. Existing technologies for investigating cyber incidents have been analyzed.

The methods and means of investigating cyber incidents have been studied.

A variant of the technology for the use of multidimensional visual analysis tools based on the i2 Analyst's Notebook solution is proposed. The purpose, main functions and composition of the components of this technology are defined.

The field of use is cyber security of the corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, MULTIDIMENSIONAL VISUAL ANALYSIS, METHODS AND MEANS OF APPLICATION OF MULTIDIMENSIONAL VISUAL ANALYSIS TOOLS, TECHNOLOGY OF APPLICATION OF MULTIDIMENSIONAL VISUAL ANALYSIS TOOLS

ЗМІСТ

ВСТУП

Актуальність дослідження. Дослідження технології застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів має значну актуальність у швидкозмінному ландшафті кібербезпеки. Оскільки кіберзагрози стають все більш складними, потреба в передових методологіях для аналізу інцидентів і реагування на них стає першорядною.

Засоби багатовимірного візуального аналізу дозволяють значно підвищити ефективність і точність розслідувань кіберінцидентів. Візуалізації можуть спростити складні набори даних, дозволяючи фахівцям швидше визначати закономірності та аномалії.

Дослідження актуальне для надання підтримки у прийнятті рішень фахівцям з кібербезпеки. Візуальне представлення може допомогти швидко зрозуміти складні зв’язки між різними точками даних, сприяючи більш обґрунтованим і своєчасним реакціям на кіберзагрози.

Враховуючи динамічний характер кіберзагроз, дослідження в цій галузі сприяють розробці інструментів і стратегій, які адаптуються до нових викликів. Ця адаптивність має вирішальне значення для випередження кіберзагроз, що розвиваються.

Підсумовуючи, дослідження технології застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів є дуже актуальним для підвищення можливостей фахівців з кібербезпеки, покращення процесів прийняття рішень і зміцнення організацій проти кіберзагроз, що постійно змінюються.

Об’єкт дослідження – процес розслідування кіберінцидентів у корпоративній інформаційній системі.

Предмет дослідження – технологія застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів на базі рішення i2 Analyst’s Notebook.

Мета роботи – розробити варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook для корпоративної інформаційної системи та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз питання щодо необхідності розслідування кіберінцидентів;
- проаналізувати основні загрози корпоративним інформаційним системам;
- проаналізувати методи та засоби розслідування кіберінцидентів;
- розробити варіант технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook для корпоративної інформаційної системи та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу розслідування кіберінцидентів на базі рішення i2 Analyst's Notebook.

Практичне значення одержаних результатів полягає в розробці варіанту технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook для корпоративної інформаційної системи та рекомендацій щодо застосування технології, що дозволить забезпечувати необхідний рівень кібербезпеки організації.

1 АНАЛІЗ НЕОБХІДНОСТІ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

1.1. Аналіз необхідності розслідування кіберінцидентів

Інцидент кібербезпеки є подією чи цілим рядом подій ненавмисного характеру, або таких, які мають ознаки можливої кібератаки, які є загрозою безпеці систем електронних комунікацій, систем керування технологічними процесами, створюють ймовірність порушення нормального режиму роботи таких систем, або ставлять під загрозу безпеку електронних інформаційних ресурсів [1].

Інцидент кібербезпеки має відношення до будь-якої події або ситуації, при якій безпека систем інформаційних технологій організації чи даних скомпрометована чи є під загрозою. Ці інциденти здатні приймати доволі різні форми та відрізнятися ступенем тяжкості від доволі незначних до вкрай критичних. Ось огляд ключових аспектів, які пов’язані з інцидентами кібербезпеки:

1. **Типи інцидентів кібербезпеки:**
    - **Витік даних**: неавторизований доступ, розголошення чи крадіжка таких конфіденційних даних, як особиста інформація, фінансові записи чи інтелектуальна власність.
    - **Шкідливе програмне забезпечення**: віруси, хробаки, програми-вимагачі, а також трояни, що порушують цілісність системи і конфіденційність інформації.
    - **Фішингові атаки**: небезпечні електронні листи, повідомлення чи сайти, що обманом змушують користувачів розкривати свої конфіденційні дані чи завантажувати інфіковане програмне забезпечення.
    - **Атаки на відмову в обслуговуванні (DoS) та розподілені атаки на відмову в обслуговуванні (DDoS)**: перенавантаження мережі, служби чи сайту трафіком, аби унеможливити їх доступність для користувачів.

- **Внутрішні загрози**: зловмисні чи ненавмисні дії внутрішнього персоналу, наприклад співробітників чи контрагентів.
- **Злом та несанкціонований доступ**: несанкціоноване отримання доступу до комп'ютерних систем, мереж або даних, використовуючи вразливості.
- **Соціальний інжиніринг**: маніпуляція людьми, аби вони розкрили конфіденційні дані чи виконали дії, які загрожують безпеці системи.
- **Порушення фізичної безпеки**: отримання неавторизованого фізичного доступу до об'єктів, серверних кімнат чи обладнання, яке містить конфіденційну інформацію.

2. **Вплив інцидентів кібербезпеки:**
   - **Втрата фінансів**: організації можуть зазнати вагомих втрат фінансів через інцидент кібербезпеки, в тому числі витрати, які пов'язані з відновленням даних, судовими позовами, штрафами від регуляторів, а також репутаційні наслідки.
   - **Втрата чи викрадення даних**: конфіденційна інформація може бути розкрита чи викрадена, що в свою чергу може призвести до порушення конфіденційності і можливих правових наслідків.
   - **Порушення роботи**: кібератаки мають можливість суттєво порушити роботу організації, викликати простої, втрату ефективності, а також підірвати довіру клієнтів.
   - **Репутаційні наслідки**: інцидент кібербезпеки має можливість завдати такої шкоди репутації організації, що для її відновлення може знадобитися доволі тривалий час та чималі зусилля.
   - **Регуляторні наслідки**: недотримання принципів захисту конфіденційної інформації може призвести до юридичних наслідків та штрафів.
   - **Втрата інтелектуальної власності**: втрата інтелектуальної власності може призвести організацію до втрати конкурентоспроможності.

3. **Реагування на інциденти:**
    - Ефективний план реагування на інциденти має дуже важливе значення для менеджменту та пом’якшення наслідків можливих інцидентів кібербезпеки. Він повинен передбачати виявлення, стримування, знищення і відновлення після інциденту.
    - Ключовими компонентами плану реагування на інциденти є призначення групи реагування на інциденти, а також наявність чіткої процедури зв’язку і документації.
4. **Профілактичні заходи:** Організації мають вживати профілактичні заходи задля зниження ризику виникнення інцидентів кібербезпеки. Це включає в себе регулярне оновлення програмного забезпечення, постійне навчання співробітників, наявність контролю доступу і найкращих методів безпеки, а також використання надійних технологій безпеки, як-от брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення.
5. **Звітування та відповідність:**
    - В деяких випадках організації за законом мають повідомляти відповідальні органи влади та постраждалих осіб про інциденти кібербезпеки.
    - Дотримання нормативних актів, які стосуються захисту даних, як-от Загальний регламент захисту даних (GDPR), має вкрай важливе значення задля уникнення штрафів.
6. **Розслідування інцидентів**: Після того, як відбувся інцидент, організації мають провести детальне розслідування, аби визначити масштаб, причину і можливі наслідки цього інциденту. Для збору доказів можна використовувати цифрову криміналістику.
7. **Розкриття інциденту**: Організації, можливо, будуть повинні розкрити деталі інцидентів кібербезпеки постраждалим сторонам, клієнтам та громадськості, в залежності від серйозності і відповідних правових вимог.

8. **Страхування кібербезпеки**: Якісь організації можуть інвествати в страхування кібербезпеки, аби знизити фінансові ризики, що пов’язані з інцидентами кібербезпеки.
9. **Постійне вдосконалення**: Організаціям варто використовувати уроки та знання, які вони отримали у результаті інцидентів кібербезпеки задля поліпшення політик безпеки, процедур та технологій, одночасно вдосконалюючи свій захист від майбутніх можливих загроз.

У підсумку, інцидент кібербезпеки може включати в себе доволі широкий спектр порушень безпеки чи компрометації. Для всіх організацій вкрай важливо мати заздалегідь підготовлені плани реагування на інциденти і інвестувати у надійні заходи безпеки, аби максимально захистити свої IT-системи і дані від можливих загроз.

Під час розслідування встановлюються усі обставини інциденту кібербезпеки. Кожен інцидент кібербезпеки потребує детального розслідування, а такі ресурси розслідування, як інструменти криміналістики, «брудні мережі», мережі карантину і співпраця із правоохоронними органами, можуть бути в нагоді задля ефективного і швидкого вирішення надзвичайної ситуації.

Розслідування інцидентів кібербезпеки – вкрай важливий процес для адекватного сприйняття масштабу, впливу і причин інциденту, а також визначення ефективних способів реагування. Процес розслідування кіберінцидентів, як правило, включає наступні етапи:

1. **Виявлення і ідентифікація:**
   - Виявлення інцидентів кібербезпеки може відбуватися різними засобами, як-от системами моніторингу безпеки, засобами виявлення вторгнень чи звітами від співробітників чи користувачів.
   - Розслідування розпочинається із визначення характеру інциденту, до прикладу витік чутливих даних, зараження шкідливим програмним забезпеченням чи мережеве вторгнення.

2. **Ізолювання і стримування:**
    - Після виявлення інциденту кібербезпеки вкрай важливо ізолювати уражені системи чи частини мережі, аби запобігти його поширенню.
    - Цей етап передбачає ізолювання уражених пристроїв, деактивацію скомпрометованих облікових записів чи вживання будь-яких інших заходів, аби запобігти інциденту кібербезпеки.
3. **Збереження доказів:**
    - Дуже важливо зберегти усі можливі докази, що будь-яким чином пов’язані з інцидентом кібербезпеки. Це може включати в себе системні журнали, дані мережевого трафіку, файли та інші цифрові докази.
    - Таке збереження є важливим кроком для подальшого аналізу і можливих юридичних або нормативних цілей.
4. **Цифровий криміналістичний аналіз:**
    - Експерти із цифрової криміналістики потім аналізовують наявні докази, аби визначити приблизну хронологію і вектор інциденту кібербезпеки, а також розрахувати приблизні масштаби вторгнення.
    - Такий аналіз допомагає визначити, як саме стався інцидент, до яких даних було отримано несанкціонований доступ, а також будь-які ознаки компрометації.
5. **Аналіз причин:**
    - Експерти визначають, через що стався інцидент кібербезпеки, це включає виявлення вразливостей, що були використані, чи слабких місць в засобах безпеки.
    - Аби у подальшому запобігти виникненню подібних інцидентів, потрібно перш за все зрозуміти їх першопричину.
6. **Оцінка впливу:**

- Експерти мають оцінити вплив інциденту кібербезпеки на організацію, у тому числі фінансові, операційні і можливі репутаційні наслідки.
- Ця оцінка в подальшому допоможе організації приймати обґрунтовані рішення щодо відновлення.

7. **Повідомлення і звітність:**
   - В залежності від законодавчих та нормативних вимог організації, можливо, потрібно буде повідомити про виникший інцидент кібербезпеки відповідні органи влади, причетних осіб, а також громадськість.
   - Потрібно чітко слідувати процедурам сповіщення, аби не порушувати відповідні закони про захист даних.
8. **Виправлення і відновлення:**
   - Щойно буде повне розуміння виникшого інциденту кібербезпеки, організації повинні швидко розробити і реалізувати план виправлення. Це означає ліквідацію вразливостей, посилення контролю безпеки і відновлення систем, що були уражені.
   - Процес відновлення спирається на відновлення звичної роботи, гарантуючи при цьому те, що подібний інцидент кібербезпеки не повториться в майбутньому.
9. **Документування і звітність**: Детальне документування розслідування інциденту кібербезпеки має вкрай важливе значення для юридичних цілей та дотримання відповідних вимог. Сюди можна віднести звіт щодо інциденту, в якому детально викладено хронологію інциденту, висновки, дії, що були вжиті, а також розробка рекомендацій щодо покращення.
10. **Здобуті знання та постійне вдосконалення:**
    - Організаціям рекомендується зробити після інциденту відповідний аналіз, аби визначити отримані знання і напрямки задля покращення стану кібербезпеки.

- Слідування рекомендаціям та постійне посилення заходів безпеки, скоріш за все, допоможе запобігти майбутнім інцидентам кібербезпеки.

11. **Відповідність законодавству і нормам:** Під час та після розслідування інциденту кібербезпеки потрібно слідувати правовим та нормативним вимогам. Недотримання нормативних актів щодо захисту даних і повідомлення про порушення потенційно може привести до відповідних правових наслідків.
12. **Співпрацювання із правоохоронними органами:** При кіберзлочинах організації мають співпрацювати із правоохоронними органами, аби притягнути винних до відповідальності.

Розслідування інцидентів кібербезпеки вимагає наявність досвіду з цифрової криміналістики, комп’ютерної безпеки і доволі часто передбачає співпрацювання із юридичними і правоохоронними органами. У актуальних і детальних розслідувань є вирішальне значення задля мінімізації впливу подібних інцидентів на кібербезпеку і їх запобіганню в майбутньому.

Взагалі, можна виділити 10 типових помилок, які заважають швидко та грамотно розслідувати інциденти кібербезпеки:

1. **Відсутність плану реагування.**

У організації викрали гроші. З засобів інформаційної безпеки у неї є лише антивірус. Керівництво не дозволяє відключити сервер і облікові записи, так як не знає, яким чином це може вплинути на бізнес. Вони витрачають декілька днів, аби з'ясувати, хто ж володіє зламаним комп'ютером та яка його роль в організації, в той час як хакери вже можуть спустошувати банкомати, виводити гроші чи викрадати дані. На додачу до реагування на інцидент додається ще й безліч організаційних проблем. Інша справа, коли в організації наявне логування, хоча б базове управління активами і розуміння бізнес-процесів, що дозволяє співробітникам виявити хакерів в мережі ще на проміжній стадії атаки, а експертам, якщо інцидент все ж таки стався,

відразу почати вирішувати проблему, не витрачаючи і так обмежений час. Використання такого підходу дуже підвищує ефективність розслідування інциденту кібербезпеки та дозволяє запобігти вкрай серйозним наслідкам.

2. **Недосліджені інциденти.**

Організація перевстановлює операційну систему на вже ураженому комп'ютері, ставить галочку, що «інцидент закрито», а вже за тиждень втрачає доволі серйозну суму грошей із рахунку. Таке буває часто – не можна обмежуватися лише «напівзаходами». Потрібно зрозуміти, яким чином атакуючим вдалося проникнути у мережу, спробувати відновити хронологію розвитку інциденту кібербезпеки і затвердити заходи з локалізації і усунення загрози. В іншому випадку все ще можуть залишитися заражені вузли, завдяки яким атаку буде продовжено.

3. **Відсутність інфраструктури зі збору подій.**

Проникнення у мережу організації могло статися доволі давно та слідів вже не залишилося. Windows, як і будь-яка інша операційна система (ОС), має функціонал зберігання подій, проте зберігає їх локально і лише обмежений час, частіше всього – лише до перезавантаження ОС. Проте ще гірша ситуація з мережевими пристроями, що зазвичай мають доволі невеликий об'єм пам'яті для зберігання подій, що не дає змогу дізнатися, чи підключався якийсь комп'ютер до шкідливого сервера 3 місяці назад, чи ні.

4. **Відсутність інформації щодо активів.**

В найкращому випадку експерти зустрічаються із описом, із яких компонентів складається бізнес-система, які конкретні люди за неї відповідають і яке завдання вона вирішує. Проте найчастіше ситуація вкрай гірша – в більшості організацій asset management просто-таки відсутній, чи інформація щодо активів вже не є актуальною. Можна подивитися на папери 3-річної давності та зрозуміти, що у них описано лише одну конфігурацію мережі, в той час як насправді мережа зросла як мінімум удвічі. В

такому випадку про швидку і ефективну реакцію на інцидент кібербезпеки не може бути й мови.

5. Відсутність документації.

У даному випадку документацією є схема процесу нормальної та звичайної взаємодії між відділами, що визначає, до прикладу, чи можуть бухгалтери мати доступ до комп'ютерів ІТ-відділу, а умовні Маша і Петро ділитися корпоративними документи за допомогою особистої пошти. Технічна документація, що описує, яким чином взаємодіють між собою системи, також є важливою. Наприклад: в документації вказано те, що один компонент функціонує лише з одним модулем, але в реальності функціонує із трьома. В іншому випадку, особливо якщо ІТ-спеціаліст, який все це знав, вже давно звільнився, то експерт з розслідування інцидентів кібербезпеки «бігатиме» за хоча б якимись зачіпками і підозрілими подіями, які насправді жодним чином не належать до інциденту. І усі ці взаємодії, що склалися історично чи еволюціонували, вже з'ясовуються у неформальних розмовах зі співробітниками — наприклад, Маша і Петя просто-таки не мають будь-якого іншого інструменту задля обміну файлів. Хоча буває й гірше, коли співробітників, які могли б допомогти зрозуміти усі ці історичні зв'язки, немає взагалі.

6. Псування доказів.

Доволі розповсюдженою помилкою є спроба розслідування інциденту кібербезпеки, не маючи при цьому потрібну кваліфікацію. Буває так, що намагаючись зняти образи диску, неправильно роблять цю операцію, стираючи диск з доказами. Іноді можна віднайти ключовий вузол, за допомогою якого розвивалася атака, та дізнатися, що власниками було перевстановлено систему, через що критично важливі для розслідування інциденту артефакти було видалено. В деяких випадках, знімаючи дамп пам'яті, ні в якому разі не можна вимикати комп'ютер, оскільки інформацію буде знищено. Але при цьому в SIEM не завжди має усі необхідні дані, та «розкрутити» ланцюжок далі, не маючи при цьому жодних історичних копій, найчастіше за все не

представляється можливим. І саме тому повинен бути чіткий план щодо правильного поводження із вузлами, що були атаковані, найголовніший пункт якого – усі такі зміни із самого початку розслідування потрібно узгоджувати із профільними експертами.

7. Провокування зловмисника.

Працівники, у яких немає потрібних знань і досвіду, можуть легковажно спробувати заблокувати усе підряд чи навіть погрожувати хакеру у переписці, не усвідомлюючи при цьому наслідків такої поведінки. В такому випадку існує ризик того, що хакер може почати «спалювати мости», при чому не тільки усуваючи за собою сліди, але і завдаючи організації при цьому вагомої шкоди — до прикладу, «натруївши» вірус-шифрувальник на усю інфраструктуру організації чи «поклавши» будь-який критично важливий сервіс. Потрібно заздалегідь спрогнозувати, як може повести себе зловмисник, у тому випадку, якщо його буде виявлено, а також максимально підготуватися до цього.

8. Невивчені уроки.

Деякі організації не хочуть робити жодних висновків із інцидентів кібербезпеки. Бувають такі випадки, коли атака розслідується, встановлюється хронологія, надаються рекомендації, а організація після цього не приймає жодних дій — не розробляє моніторинговий процес і не усуває знайдені вразливості. За словами одного експерта, одного разу влітку він допомагав розібратися із наслідками злому, видалити шкідливе ПЗ, скинути скомпрометовані паролі, а також провести заходи із «зачистки» мережі. А вже восени ця ситуація повторилася знову, і зловмисники повернулися до цієї мережі, як до себе додому. Добре, що більшість організацій усе-таки впроваджують необхідні заходи захисту після того, як стався інцидент кібербезпеки, хай і не одразу. Якщо мережа постійно атакується, то у підрозділа інформаційної безпеки немає навіть місяця задля усунення критично небезпечної вразливості, завдяки якій і проникли в перший раз. Повторний інцидент кібербезпеки відбудеться набагато раніше.

9. Оповіщення зловмисників.

У випадку, якщо було скомпрометовано поштову систему, в той час як переписку служба інформаційної безпеки веде електронною поштою, то тоді зловмисник з легкістю зможе відстежувати будь-які заходи протидії. В такому випадку він або «заляже на дно», знищивши будь-які сліди, що потім ускладнить розслідування, або здійснить якісь деструктивні дії (які описані у помилці 7 вище), та у організації вже не буде часу на розслідування. Саме це колись і сталося з експертом із розслідування інцидентів кібербезпеки, коли під час розслідування адміністратор переписувався з ним через настільну версію месенджера Telegram з комп'ютера, який було скромпрометовано. Зловмисникам вдалося спостерігати за перепискою і тому вони діяли на випередження, що значно ускладнило й без того заплутане розслідування, аж до того моменту, коли факт компрометації не було виявлено і не було змінено спосіб комунікації. Саме через подібні випадки потрібно мати додаткові способи комунікацій, які жодним чином не зв'язані з інфраструктурою компанії (наприклад, використовувати той же самий Telegram, проте виключно із довірених пристроїв). Потрібно чітко зрозуміти, що якщо була скомпрометована уся мережа, то над нею вже нема контролю, і саме тому необхідно детально розписувати кожен крок в рамках розслідування інцидентів кібербезпеки.

10. Зомбі-інциденти.

Одразу після розслідування і усунення всіх наслідків, проблеми можуть нікуди не дітися. Із резервної копії можна випадково відновити образ річної давності, що вже був скомпрометований, та хакери отримають несподіваний подарунок в вигляді відновленого доступа до внутрішньої мережі. Хоча це й буває вкрай рідко, проте це доволі влучно б'є по організації. Саме тому потрібно слідкувати не лише за поточною інфраструктурою, а також і за системами архівування і резервування. Взагалі, рекомендується певний час слідкувати за ознаками компрометації інцидентів, які сталися, навіть після того, як їх було усунено та досліджено. Зомбі-інцидент може

виникнути не тільки в зв'язку з системами резервного копіювання, але і з появою активу, що був відсутній в період розслідування інциденту кібербезпеки. До прикладу, співробітник пішов у відпустку, а його комп'ютер не перевірявся чи був у ремонті. На комп'ютері віддалено активується бекдор, що ніхто не усунув. В подібних випадках вчасно відреагувати вдається тільки в разі наявності розвиненої системи моніторингу і виконання усіх рекомендацій після завершення розслідування. Головними завданнями розслідування інцидентів кібербезпеки є «докопатися» до суті, відновити хронологію інциденту, віднайти джерело, а також нейтралізувати загрозу. Проте в тому випадку, якщо організація заздалегідь не створила мінімальної інфраструктури для виявлення і усунення інцидентів, чи починає реагувати, не маючи при цьому потрібного досвіду, то допомогти не завжди представляється можливим, і тому до можливої зустрічі із кіберзлочинцями краще за все готуватися заздалегідь [2].

1.2. Аналіз загроз корпоративним інформаційним системам

Корпоративною інформаційною системою (КІС) є інформаційна система, що підтримує автоматизацію управлінських функцій в організації та надає інформацію задля прийняття рішень. У КІС реалізовано ідеологію управління, що поєднує в собі бізнес-стратегію організації разом із прогресивними інформаційними технологіями.

Сучасні КІС мають такі основні характеристики, як-от масштабність, багатоплатформні обчислення, робота у неоднорідному обчислювальному середовищі, а також розподілені обчислення.

Масштабність. Масштабність є однією з найважливіших характеристик інформаційних систем (ІС) подібного класу, особливо враховуючи масштаби діяльності організації. Масштабна ІС має функціонувати на масштабній програмно-апаратній платформі, що в свою чергу вимагає доволі значних зусиль фахівців із

розробки та реалізації подібних систем. Так як варіантів конфігурації базового устаткування і програмного забезпечення може бути доволі багато, то КІС повинна бути багатоплатформною.

Багатоплатформні обчислення. КІС необхідна, аби прикладна програма могла працювати на декількох програмно-апаратних платформах, але одночасно із цим повинні бути впроваджені однакові інтерфейс та логіка роботи на усіх платформах (схожі схеми екрана, елементів меню та діалогової інформації, яка надається користувачу на різних платформах; інтеграція із операційним середовищем користувача; одна й та ж сама поведінка на різних платформах; узгоджена підтримка незалежно від платформи та інше). Розробити прикладну програму одночасно у декількох середовищах не є легкою задачею, і тому з'явилися інтегровані програмні середовища розробки, які дуже полегшують процес перенесення прикладних програм між декількома різними середовищами. До них можна віднести, наприклад, Windows Open Systems Architecture.

Робота у неоднорідному обчислювальному середовищі. До однієї з найважливіших переваг КІС можна віднести наявність можливості роботи у мережах, до яких входять комп'ютери, які працюють на різних операційних системах або які були побудовані на різних обчислювальних платформах. При цьому повинно бути забезпечено взаємодію усіх робочих обчислювальних платформ та операційних систем, що використовуються.

Розподілені обчислення. Розподілені обчислення є одним із типів роботи у клієнт-серверній архітектурі, при якому дані або запити, які надходять із клієнтських машин, рівномірно розподіляються між декількома серверами, що в свою чергу збільшує пропускну здатність для користувача та робить можливою багатозадачну роботу, а це в свою чергу сприяє максимально ефективному використанню обчислювальних ресурсів, суттєвому зниженню витрат, а також підвищенню загальної ефективності системи. Можливість розподіленої роботи та наявність

віддаленого доступу до документів є обов'язковою вимогою до ІС корпоративного рівня. Останнім часом невід'ємною складовою цієї вимоги стала також можливість роботи в архітектурі Internet/Intranet.

КІС дає користувачу можливість вирішити такі задачі:

1. зробити для керівництва організації використання вкладених у бізнес коштів прозорим;
2. надати повну інформацію задля економічної доцільності стратегічного планування;
3. професійно керувати витратами, наочно та своєчасно показувати, яким чином можна суттєво мінімізувати ці витрати;
4. впровадити оперативне управління організацією згідно з обраними ключовими показниками;
5. гарантувати прибутковість організації шляхом оптимізування та прискорення таких процесів, як дотримання строків виконання нових замовлень та перерозподіл наявних ресурсів.

Повноцінна КІС має забезпечити інформаційну прозорість організації, сформувати єдиний інформаційний простір, що об'єднав би інформаційні потоки, які йдуть від виробництва до нього, із даними фінансово-господарських служб та видавав би необхідні повідомлення для усіх рівнів управління організацією.

КІС поділяються на Enterprise Resource Planning System (ERP), Customer Relationship Management System (CRM), Manufacturing Execution System (MES), Warehouse Management System (WMS), Enterprise Asset Management (EAM), а також Human Resource Management (HRM).

ERP (Планування ресурсів підприємства). Сучасні ERP виникли у результаті майже 40-літньої еволюції управлінських та інформаційних технологій. Загалом, вони використовуються задля створення єдиного інформаційного простору організації,

ефективного управління усіма наявними в організації ресурсами, які пов'язані з продажами, виробництвом та обліком замовлень. Реалізується ERP-система за модульним принципом і зазвичай має в наявності в своєму складі модуль безпеки задля запобігання внутрішніх і зовнішніх крадіжок інформації. Проблеми зазвичай виникають через помилки експлуатації чи початкового плану впровадження системи. Наприклад, недостатні інвестиції у навчання персоналу роботі із системою доволі суттєво знижують подальшу ефективність, і тому зазвичай ERP-системи впроваджують не відразу і в повному обсязі, а окремими модулями [10]. Функціональний склад ERP-системи зображено на рис. 1.1.

Рис. 1.1. Функціональний склад ERP

До українських ERP-систем можна віднести Універсал ERP та Дебет Плюс.

CRM (Управління відносинами з клієнтами). Управління відносинами з клієнтами є поняттям, яке охоплює концепції, які використовуються організаціями

для управління їхніми відносинами з клієнтами, у тому числі збір, зберігання та аналіз інформації про клієнтів, постачальників, партнерів, а також інформації про взаємовідносини із ними. Сучасна CRM-система спрямована на вивчення і аналіз ринку та конкретних потреб клієнтів. Завдяки цим знанням розробляються нові товари та послуги, і таким чином організація досягає поставлених цілей та покращує свої фінансові показники.

Налічують 3 CRM-підходи, кожний з яких може бути впроваджений окремо від інших:

1. оперативний — автоматизація споживчих бізнес-процесів, яка допомагає персоналу з роботи з клієнтами ефективно виконувати свої обов'язки;
2. співробітницький — програма взаємодіє з клієнтами без участі відповідного персоналу;
3. аналітичний — аналіз інформації про клієнтів з різними цілями.

Принципами CRM-систем є наявність єдиного сховища інформації, де в будь-яку мить доступні всі наявні відомості про взаємодію з клієнтами, синхронізація управління множинними каналами взаємодії, а також постійне аналізування отриманої інформації про клієнтів і прийняття відповідних організаційних рішень (наприклад, сортування клієнтів в залежності від їхньої значимості для організації) [11].

Можливості CRM-систем:

- наявність швидкого доступу до актуальної інформації про клієнтів;
- можливість оперативного обслуговування клієнтів і проведення операцій;
- чітка формалізація схеми взаємодії з клієнтами, автоматизований документообіг;
- можливість швидкого отримання усіх потрібних звітних даних і аналітики;

- відчутне зниження операційних витрат менеджерів;
- контроль за роботою менеджерів;
- налагоджена взаємодія між співробітниками та підрозділами;
- управління бізнес-процесами;
- управління контрагентами, історія взаємодій із клієнтами;
- складання планів за різними показниками;
- планування заходів, здійснення угод, отримання потрібних звітних документів;
- планування й управління закупівлями та доставками;
- управління процесом маркетингу;
- наявність можливості роботи по мережі;
- можливість імпорту контрагентів із інших баз.

MES (Керування виробництвом). MES-системи направлені на виробниче середовище організації. Такі системи відслідковують та фіксують увесь процес виробництва, а також відображають цикл виробництва у реальному часі. Порівнюючи її з ERP-системою, у якої немає прямого впливу на процес, MES дозволяє змінювати (або повністю перероблювати) процес стільки разів, скільки це буде необхідно. Іншими словами, MES-системи потрібні задля оптимізації виробництва й підвищення його рентабельності. Отримуючи та оброблюючи дані, які були отримані, наприклад, від технологічних ліній, вони надають більш повне уявлення про виробничу діяльності організації, одночасно з цим покращуючи й фінансові показники. Всі головні показники, що входять до основного курсу економіки галузі більш ніж детально відображаються у ході виробництва. Досвідчені фахівці називають MES «мостом між фінансовими операціями ERP-систем та оперативною діяльністю організації на рівні цеху, ділянки чи лінії [12]. Функціональний склад MES зображено на рис. 1.2.

Рис 1.2. Функціональний склад MES

WMS (Система управління складом). WMS є системою управління, яка забезпечує автоматизацію й оптимізацію усіх процесів складської роботи профільної організації [13].

Архітектуру WMS побудовано за трирівневим принципом:

1. перший компонент є видимою для користувача частиною (інтерфейсом типу «людина-машина») — клієнтським додатком, завдяки якому користувач вводить, змінює і видаляє дані, відправляє запити на виконання операцій та одерження звітів;
2. другий компонент, який є прихованою від користувачів частиною системи, є сервер бази даних (БД), який здійснює зберігання даних. Користувач через клієнтський додаток здійснює процедуру запиту на вибірку, введення, зміну чи видалення даних у БД;

3. третій компонент здійснює ініційовану користувачем обробку даних, а потім повертає оброблені дані в БД, повідомляючи користувача через екран додатку про завершення операції.

Загалом виділяють 6 цілей впровадження:

- активне складське управління;
- збільшення швидкості набору товарів;
- отримання точної інформації щодо місцезнаходження товару на складі;
- ефективне управління товарами, що мають обмежений термін придатності;
- отримання інструменту для підвищення ефективності і розвитку процесів по обробці товару на складі;
- оптимізування з використання складських площ.

EAM (Система управління фондами підприємства). EAM-система робить можливим суттєво скоротити простої устаткування, витрати на технічне обслуговування, ремонти та матеріально-технічне постачання. Вона є дуже потрібним інструментом у процесі роботі фондомістких галузей. Основні фонди є засобами праці, що по декілька разів беруть безпосередню участь у виробничому процесі, при цьому зберігаючи свою звичайну форму та поступово зношуючи, переносячи свою вартість частинами на щойно створену продукцію. У бухгалтерському і податковому обліках зображені у грошовому еквіваленті основні фонди є основними засобами. Взагалі EAM-системи виникли з CMMS-систем (система управління ремонтами). Наразі EAM-модулі також входять до складу таких великих пакетів ERP-систем, як, наприклад, Oracle E-Business Suite [14].

HRM (Система управління персоналом). HRM — це одна з найважливіших складових частин сучасного управління. Основною метою подібних систем є залучення і утримання вкрай цінних для організації працівників. HRM-системи головним чином вирішують 2 головні задачі: впорядкування усіх облікових та

розрахункових процесів, які пов'язані із персоналом, а також суттєве зниження відсотку «відходу» співробітників, тому HRM-системи певним чином можна назвати «оберненими CRM-системами», де залучаються і утримуються співробітники, а не покупці. Зрозуміло, що методи є зовсім іншими, але загальні підходи дуже схожі [3].

Функціями HRM-систем є:

- пошук потенціальних співробітників;
- підбір і відбір потенціальних співробітників;
- оцінювання персоналу;
- навчання і розвиток персоналу;
- управління корпоративною культурою;
- мотивування персоналу;
- організація робочої діяльності.

Призначення КІС, також відомої як корпоративна інформаційно-технологічна система, полягає у тому, аби керувати інформаційним потоком усередині організації та полегшувати його задля підтримки бізнес-операцій та процесів прийняття рішень в організації. Ці системи є вкрай важливими в сучасному бізнесі та слугують таким ключовим цілям, як управління даними, допомога у прийнятті рішень, зв’язок та співпраця, автоматизація процесів, управління взаємовідносинами із клієнтами, управління ланцюгом поставок, управління фінансами, звітність та відповідність, безпека і захист даних, стратегічне планування, керування знаннями, а також конкурентна перевага.

Взагалі, належним чином спроектована і реалізована КІС є вкрай важливою для сучасного бізнесу, аби управляти своїми операціями, реагувати на зміни ринку і ефективно конкурувати у динамічному і сфокусованому на даних бізнес-середовищі.

Зазвичай **структура** КІС складається із різних компонентів, що працюють у взаємодії задля підтримки інформаційних потреб та процесів організації. Точна

структура змінюється в залежності від розміру, галузі і вимог організації, проте основні компоненти, які зазвичай зустрічаються в КІС, включають в себе обладнання, програмне забезпечення, дані, людей, процедури та процеси, мережеву інфраструктуру, заходи безпеки, системи зберігання, резервне копіювання та аварійне відновлення, інтерфейси користувача, відповідність та керування, а також масштабованість та гнучкість.

Структуру КІС має бути розроблено таким чином, аби відповідати конкретним цілям та вимогам організації, в той же час забезпечуючи ефективне та безпечне управління інформацією таким чином, аби підтримувати бізнес-процеси і стратегічні цілі організації. Для організацій дуже важливо регулярно оцінювати і оновлювати свою структуру КІС, аби бути «на одній хвилі» із технологічним прогресом та постійною зміною потреб.

КІС виконують різні **функції** у організації для керування інформацією, підтримки бізнес-процесів та полегшення прийняття необхідних рішень. Конкретні функції КІС можуть змінюватися в залежності від галузі, розміру та мети організації, в той час як загальні функції включають в себе зберігання і управління інформацією, оброблення і подальший аналіз інформації, автоматизацію робочого процесу, комунікацію і співпрацю, управління документами, керування взаємовідносинами із клієнтами, управління людськими ресурсами, керування фінансами, менеджмент ланцюга поставок, безпека і захист інформації, допомога у прийнятті рішень, керування знаннями, стратегічне планування, відповідність і нормативна звітність, слідкування за ефективністю та основними показниками ефективності, резервне копіювання даних і аварійне відновлення, управління доступом користувачів, масштабування і адаптація, а також наявність інновацій і конкурентних переваг.

Усі ці функції разом сприяють ефективній діяльності і керування організацією. Належним чином спроектована КІС узгоджується зі стратегічними цілями організації

і гарантує, що інформація буде легкодоступною для підтримки у прийнятті рішень і ефективного управління бізнес-процесами.

Функціонування КІС залежить від доволі різних **умов**, які забезпечують її ефективність і надійність. Подібні умови критично важливі для злагодженої роботи системи і її спроможності до підтримувки бізнес-цілей організації. Конкретні умови можуть бути різними в залежності від індивідуальних потреб організації і складності її КІС, але загальні умови включають в себе якість даних, безпеку даних, конфіденційність даних та їх відповідність вимогам, резервне копіювання і аварійне відновлення даних, масштабування, здатність до інтеграції, легкість у використанні і навчанні користувачів, моніторинг ефективності, наявність технічної підтримки і технічного обслуговування, наявність повної документації, можливість управління змінами, наявність бюджету та розподіл ресурсів, планування безперебійності бізнесу, управління доступом користувачів, управління даними, наявність показників ефективності та KPI, менеджмент постачальників, а також наявність відгуків від користувачів та регулярне вдосконалення.

Синергія цих умов сприяє правильному функціонуванню КІС, при цьому гарантуючи, що вона забезпечує заплановані переваги і підтримує операційні і стратегічні цілі організації.

Аналізуючи загрози, ось деякі з найпоширеніших загроз для корпоративних інформаційних систем:

1. **Шкідливе ПЗ**. Шкідливе ПЗ, таке як віруси, хробаки і програми-вимагачі, може уражати корпоративні інформаційні системи, що в свою чергу може призвести до витоку даних, збоїв у роботі системи і фінансових наслідків.

2. **Фішингові атаки**. Фішингові атаки передбачають спроби шахраїв несанкціоновано отримати конфіденційні дані, такі як імена користувачів, паролі і фінансова інформація, видаючи себе за надійну особу. Фішингові атаки дуже часто

спрямовані на співробітників через електронні листи, повідомлення чи фішингові веб-сайти.

3. **Внутрішні загрози**. Співробітники чи контрагенти, у яких є доступ до корпоративних інформаційних систем, можуть бути загрозою через навмисні чи ненавмисні дії. Це включає в себе несанкціонований доступ, витік даних чи зловживання наявними ресурсами компанії.

4. **Розподілені атаки на відмову в обслуговуванні (DDoS)**. DDoS-атаки ставлть собі за мету порушення нормального функціонування мережі, служби або веб-сайту, шляхом їх перевантаження потоком трафіку. Це може призвести до простою, який може вплинути на бізнес-операції.

5. **Розширені стійкі загрози (APT)**. APT передбачають складні цілеспрямовані атаки, які використовуються для отримання несанкціонованого доступу до системи і збереження такого доступу протягом доволі тривалого періоду часу. APT часто пов’язують зі шпигунством чи крадіжкою конфіденційних даних.

6. **Атаки програм-вимагачів**. Програми-вимагачі зашифровують файли та системи, в той час як зловмисники вимагають за це плату. Такі атаки можуть призвести до втрати даних, фінансових наслідків та виникнення збоїв у роботі.

7. **Невиправлене ПЗ і вразливості**. Експлуатація вразливостей в ПЗ або системах, що не були виправлені або оновлені, може надати хакерам несанкціонований доступ. Регулярне оновлення системи має вирішальне значення задля усунення подібних вразливостей.

8. **Атаки на ланцюги поставок**. Кіберзлочинці фокусуються на ланцюгах поставок, аби опосередковано зламувати системи. Це може включати в себе атаки на постачальників або контрагентів задля отримання доступу до мережі.

9. **Людський фактор**. Такі помилки співробітників, як випадкове надсилання конфіденційних даних іншому одержувачу чи неправильне налаштування параметрів безпеки, можуть спричинити потенційний кіберінцидент.

10. **Відсутність належної поінформованості щодо безпеки**. Недостатня поінформованість та відсутність навчання працівників найкращим практикам кібербезпеки може наражати організації на ризики. Навчання персоналу потенційним загрозам має вкрай важливе значення задля підтримки безпечного середовища.

11. **Загрози через мобільні пристрої**. Через збільшення використання мобільних пристроїв загрози, що націлені на смартфони і планшети, як-от зловмисне ПЗ для мобільних пристроїв та незахищені Wi-Fi–з'єднання, можуть також становити загрозу для корпоративних інформаційних систем.

12. **Хмарні проблеми безпеки**. Через те, що організації поступово мігрують на хмарні служби, забезпечення кібербезпеки хмарних середовищ стає все дедалі важливішим. Через такі проблеми, як неправильно налаштовані параметри хмарного середовища і недостатньо захищені інтерфейси програмування додатків (API), конфіденційні дані можуть бути розкриті.

Аби залишатися стійкими до подібних загроз, організаціям потрібно запровадити комплексну стратегію кібербезпеки, яка б включала регулярні перевірки безпеки, навчання співробітників та використання передових технологій безпеки. Окрім цього, необхідно бути в курсі останніх тенденцій та загроз кібербезпеки, аби мати вирішальне значення задля відповідного адаптування заходів безпеки.

1.3. Аналіз технологій розслідування кіберінцидентів

При розслідуванні кіберінцидентів, як правило, використовується одразу декілька технологій для виявлення, аналізу і реагування на інциденти безпеки. Деякі з найвідоміших технологій розслідування кіберінцидентів включають в себе SIEM, EDR, IRP та SOAR.

SIEM. Управління інформацією про безпеку та подіями — це технологічне рішення, яке призначене для того, аби надавати комплексну аналітичну інформацію про безпеку шляхом збору і аналізу даних журналу, які були створені в технологічній інфраструктурі організації. SIEM-системи мають вирішальну роль в кібербезпеці, допомагаючи організаціям виявляти та реагувати на інциденти безпеки, а також надавати засоби для звітування щодо відповідності та судового аналізу. Ось основні компоненти і функції технології SIEM:

- **Колекція журналів**. SIEM-системи збирають дані журналу із різних джерел в організації, включаючи при цьому мережеві пристрої, сервери, програми, пристрої безпеки і кінцеві точки. Ці дані містять інформацію щодо подій та дій, які відбуваються в IT-середовищі.
- **Нормалізація і кореляція**. SIEM нормалізує дані журналу, перетворюючи їх при цьому в стандартизований формат задля полегшення подальшого аналізу. Після цього система співвідносить події із різних джерел, аби визначити шаблони і зв’язки, що можуть вказувати на інцидент безпеки. Кореляція дозволяє зрозуміти контекст подій та відокремити звичайну діяльність від можливих загроз.
- **Моніторинг та сповіщення в режимі реального часу**. SIEM-системи забезпечують моніторинг подій безпеки в режимі реального часу – коли система розпізнає шаблон чи аномалію, що відповідають попередньо

визначеним правилам чи сигнатурам, вона автоматично генерує відповідні сповіщення, які сповіщають групи безпеки щодо потенційних інцидентів безпеки, що в свою чергу дозволяє вчасно зреагувати.

- **Виявлення кіберінцидентів та подальше реагування**. SIEM-системи дозволяють виявляти інциденти безпеки і вчасно реагувати на них, спираючись на інформацію про незвичайні або ж підозрілі дії. Команди безпеки потім можуть використати інформацію, надану SIEM, задля розслідування кіберінцидентів, правильного розуміння їхнього масштабу і подальшого втілення відповідних заходів задля зменшення ризиків.
- **Історичний аналіз і криміналістика**. Завдяки технології SIEM можна аналізувати історичні дані журналу. Фахівці з кібербезпеки мають змогу відстежити хронологію подій, краще зрозуміти першопричину інциденту та визначити ступінь впливу.
- **Звіт щодо відповідності**. Багато організацій використовують SIEM, аби відповідати нормативним вимогам. У SIEM-систем є можливість створювати звіти, що наглядно демонструють дотримання політик безпеки і надають докази вжиття відповідних заходів безпеки.
- **Аналіз поведінки користувачів та суб'єктів**. Деякі рішення SIEM включають в себе аналіз поведінки користувачів та суб'єктів задля виявлення аномалій, що можуть вказувати на зламані облікові записи чи внутрішні загрози. Це покращує здатність ідентифікувати інциденти безпеки, що будь-яким чином пов'язані з діяльністю користувачів.
- **Інтеграція з іншими засобами безпеки**. SIEM-системи дуже часто інтегруються із іншими технологіями кібербезпеки, як-от системи виявлення/запобігання вторгненням (IDS/IPS), брандмауери, антивірусні рішення і засоби захисту кінцевих точок. Подібні інтеграції покращують

загальну кібербезпеку і забезпечують більш скоординовану реакцію на можливі кіберінциденти.

- **Масштабованість та гнучкість**. SIEM-системи були розроблені задля її масштабування разом із зростанням організації. Вони можуть обробляти великі обсяги даних, які були створені різними джерелами, а також можуть бути налаштованими відповідно до конкретних потреб кібербезпеки у різних галузях та секторах.
- **Хмарний SIEM**. Зі зростанням популярності хмарних служб багато рішень SIEM відтепер пропонують хмарно-сумісні чи хмарні варіанти, які дозволяють організаціям контролювати і захищати як локальне, так і хмарне середовища.

Впровадження SIEM вимагає детального планування, налаштування і регулярного керування, аби забезпечити його ефективність. Ця технологія є критично важливим компонентом комплексної стратегії кібербезпеки, яка надає організаціям засоби, потрібні для проактивного управління і реагування на кіберінциденти.

EDR. Технологія виявлення кінцевої точки і реагування — це технологія кібербезпеки, що призначена задля моніторингу і реагування на кіберзагрози на рівні кінцевої точки у мережі організації. Кінцеві точки стосуються окремих пристроїв, як-от комп’ютери, сервери, ноутбуки і мобільні пристрої. Рішення EDR базуються на виявленні у режимі реального часу, розслідуванні і реагуванні на потенційні кіберінциденти на цих кінцевих точках. Основні функції технології виявлення кінцевої точки і реагування включають:

- **Моніторинг у режимі реального часу**. Рішення EDR постійно відслідковують кінцеві пристрої на наявність будь-яких ознак шкідливої діяльності. Це включає в себе аналіз процесів, системних викликів, змін файлів та іншої поведінки, що може вказувати на потенційну загрозу безпеці.

- **Поведінковий аналіз**. EDR використовує поведінковий аналіз задля встановлення базової лінії нормальної активності на кінцевих точках. Мінімальне відхилення від цього базового рівня ініціює попередження, що допомагає командам безпеки швидше виявляти потенційно зловмисну поведінку чи несанкціоновані дії.
- **Виявлення і запобігання загрозам**. Інструменти EDR мають можливості виявлення загроз, що в свою чергу дає їм змогу ідентифікувати вже відомі та ще невідомі загрози, такі як зловмисне ПЗ, програми-вимагачі і вдосконалені постійні загрози. Деякі рішення EDR можуть використовувати машинне навчання і штучний інтелект задля покращення своїх можливостей виявлення.
- **Розслідування і криміналістика**. Коли виявляється потенційний кіберінцидент, EDR надає групам безпеки можливість проводити детальні розслідування уражених кінцевих точок, що включає у себе аналіз хронології подій, повне розуміння масштабів кіберінциденту і точне визначення джерела загрози.
- **Ізолювання і стримування**. У відповідь на підтверджений кіберінцидент, рішення EDR мають змогу ізолювати чи помістити в карантин уражені кінцеві точки, аби запобігти подальшому поширенню загрози й на інші частини мережі. Заходи стримування дозволяють обмежити вплив кіберінциденту, в той час як команда безпеки розслідує і нейтралізує загрозу.
- **Автоматизація реагування на кіберінциденти**. Багато рішень EDR пропонують автоматизацію задля оптимізації процесів реагування на кіберінциденти. Автоматичні відповіді можуть включати такі дії, як ізоляція зараженого пристрою, блокування зловмисних процесів чи запуск попередньо визначених дій із відновлення.

- **Інтеграція із аналізом загроз**. Рішення EDR доволі часто інтегруються із каналами аналізу загроз, аби бути в курсі останніх відомих загроз та індикаторів компрометації. Такі інтеграції покращують здатність системи до виявлення нових загроз і завчасного реагування.
- **Наявність централізованої консолі управління**. Рішення EDR, як правило, забезпечують наявність централізованої консолі управління, що дає групам безпеки можливість відстежувати і управляти усіма кінцевими точками із єдиного інтерфейсу. Це, в свою чергу, спрощує загальне управління і реагування на кіберінциденти.
- **Аналіз поведінки користувачів та суб'єктів**. Деякі з рішень EDR включають в себе аналіз поведінки користувачів та суб'єктів задля подальшого аналізу поведінки кінцевих точок. Це дозволяє виявити незвичні дії, що можуть вказувати на зламані облікові записи користувачів чи наявність внутрішніх загроз.
- **Моніторинг відповідності**. Інструменти EDR доволі часто включають в себе функції моніторингу і забезпечення відповідності політикам та нормам безпеки. Вони можуть генерувати звіти, що демонструють дотримання стандартів безпеки.
- **Масштабованість**. Рішення EDR були розроблені для масштабування відповідно до розмірів організацій, що дозволяє їм ефективно захищати доволі велику кількість кінцевих точок.

EDR є ключовим компонентом сучасних стратегій кібербезпеки, який надає організаціям засоби виявлення і реагування на кіберзагрози на рівні кінцевих точок.

IRP. Платформи реагування на інциденти — це технології, які були розроблені задля полегшення і оптимізації управління кіберінцидентами в організації. Ці платформи забезпечують централізований та скоординований підхід до реагування на кіберінциденти, допомагаючи при цьому командам безпеки ефективно виявляти,

аналізувати та нейтралізовувати загрози кібербезпеці. IRP мають вирішальну роль в підвищенні ефективності і результативності процесу реагування на кіберінциденти організації. Основні функції платформ реагування на інциденти включають:

- **Централізоване управління кіберінцидентами**. IRP надають централізовану платформу для управління усіма аспектами процесу реагування на кіберінциденти. Це включає в себе виявлення кіберінцидентів, їх розслідування, стримування, ліквідацію, відновлення та подальший аналіз.
- **Автоматизування робочого процесу та організація**. Однією з ключових особливостей IRP є здатність до автоматизування і організування робочих процесів під час реагування на кіберінциденти. Автоматичні відповіді можуть включати в себе ізоляцію уражених систем, блокування зловмисних дій чи запуск попередньо визначених дій в залежності від характеру кіберінциденту.
- **Агрегація і кореляція сповіщень**. IRP об’єднують сповіщення із різних інструментів кібербезпеки та джерел, що в свою чергу дозволяє командам безпеки корелювати цю інформацію і таким чином мати повне уявлення про кіберінцидент. Це дозволяє швидше визначити першопричину і зрозуміти більш широкий вплив.
- **Спілкування і співпраця**. IRP сприяють спілкуванню і співпраці між членами групи реагування на кіберінциденти. Вони доволі часто мають функції, призначені для співпраці у режимі реального часу, захищені канали зв’язку і автоматичне документування дій, які були вжиті під час реагування на кіберінцидент.
- **Інтеграція з інструментами безпеки**. IRP можуть інтегруватися із різними інструментами безпеки, включаючи вище згадані SIEM і EDR, а також каналами розвідки про загрози та іншими відповідними

технологіями. Така інтеграція гарантує, що групи реагування на кіберінциденти матимуть доступ до найактуальнішої інформації і зможуть найбільш ефективно зкоординувати відповідне реагування.

- **Аналіз та збір доказів**. IRP допомагають в проведенні криміналістичного аналізу, надаючи при цьому інструменти і можливості задля збору доказів, які пов’язані із кіберінцидентами. Це дуже важливо для повного розуміння масштабів кіберінциденту, правильної ідентифікації зловмисників та надійного забезпечення відповідної документації для юридичних чи нормативних цілей.
- **Посібники та стандартні операційні процедури**. IRP доволі часто дозволяють створювати посібники із реагування на кіберінциденти та стандартних операційних процедур. Ці попередньо визначені робочі процеси дозволяють особам, що займаються реагуванням на кіберінциденти, слідувати діям, що потрібно виконати в залежності від різних типів кіберінцидентів.
- **Звітування про кіберінциденти і документування**. IRP дозволяють групам безпеки формувати звіти та документацію, що пов’язана із кіберінцидентами. Це включає в себе детальні звіти щодо кіберінцидентів, їх часові рамки, опис вжитих дій та «винесених уроків». Документування є важливим процесом для аналізу після кіберінциденту.
- **Інтеграція аналізу загроз**. Багато IRP інтегруються із каналами аналізу загроз, аби надати контекстну інформацію щодо загроз. Це дозволяє службам реагування на кіберінциденти приймати більш обґрунтовані рішення, базуючись на останніх даних розвідки щодо загроз.
- **Постійне вдосконалення і навчання**. IRP підтримують постійне вдосконалення, допомагаючи організаціям аналізувати минулі кіберінциденти, визначати області вдосконалення і відповідним чином

покращувати процедури реагування. Цей послідовний процес дозволяє підвищити загальну кібербезпеку організації.

- **Моніторинг відповідності**. Деякі IRP включають в себе функції моніторингу і відповідності галузевим нормам та стандартам безпеки. Це вкрай важливо для організацій, що мають дотримуватися певних вимог щодо відповідності.

Платформи реагування на кіберінциденти вкрай важливі для організацій, що прагнуть покращити свої можливості з реагування на кіберінциденти. Забезпечуючи централізований та автоматизований підхід, IRP дозволяють організаціям ефективніше реагувати на кіберінциденти, мінімізувати потенційну шкоду і вчитися на кожному кіберінциденті задля покращення загальної кібербезпеки.

SOAR. Організація, автоматизація і реагування на безпеку — це технологічне рішення, що дозволяє підвищити ефективність та результативність операцій із кібербезпеки шляхом інтеграції і автоматизації різних процесів кібербезпеки. Платформи SOAR спрощують робочі процеси реагування на кіберінциденти, покращують співпрацю між різними командами безпеки і автоматизовують повторювані задачі, дозволяючи при цьому організаціям реагувати на кіберінциденти швидше і ефективніше. Ключові особливості та функції технології організації, автоматизації і реагування на безпеку включають:

- **Організація**. Платформи SOAR полегшують організацію складних робочих процесів кібербезпеки шляхом координації і автоматизації задач в різних інструментах та системах кібербезпеки. Це забезпечує безперебійну і скоординовану відповідь на кіберінциденти.
- **Автоматизація**. Можливості автоматизації на платформах SOAR допомагають виконувати заздалегідь визначені дії і реагувати на кіберінциденти. Це включає в себе автоматизацію рутинних задач, як-от

збір та аналіз даних щодо загроз, ізоляцію скомпрометованих систем та запуск посібників з реагування на кіберінциденти.

- **Посібники з реагування на кіберінциденти**. Платформи SOAR дозволяють організаціям створювати і слідувати посібникам із реагування на кіберінциденти. Ці посібники визначають серію кроків, що потрібно зробити під час різних типів кіберінцидентів. Автоматизація забезпечує послідовне і ефективне виконання цих кроків.
- **Інтеграція із інструментами кібербезпеки**. Платформи SOAR інтегруються із широким спектром інструментів та технологій кібербезпеки, включаючи зазначені вище SIEM та EDR, а також канали аналізу загроз, брандмауери тощо. Ці інтеграції гарантують, що групи безпеки зможуть використовувати можливості існуючих інструментів в рамках єдиної платформи.
- **Сортування попереджень та визначення пріоритетів**. Платформи SOAR дозволяють сортувати сповіщення завдяки автоматичному визначенню пріоритетів та категоризації сповіщень безпеки в залежності від попередньо визначених критеріїв. Це дозволяє командам безпеки зосереджуватися лише на критично важливих сповіщеннях та реагувати на кіберінциденти у порядку серйозності.
- **Співпраця і комунікація**. Платформи SOAR надають функції співпраці і комунікації задля полегшення взаємодії між членами групи безпеки. Це включає в себе наявність захищених каналів зв’язку, інструментів для співпраці у режимі реального часу і документацію дій, які були вжиті під час реагування на кіберінциденти.
- **Інтеграція аналізу загроз**. Платформи SOAR доволі часто інтегруються із каналами аналізу загроз, аби надавати релевантну інформацію щодо загроз. Такі інтеграції покращують процес прийняття рішень, при цьому

гарантуючи, що групи безпеки матимуть доступ до найактуальніших даних розвідки щодо загроз.

- **Аналіз і звітність**. Платформи SOAR мають можливості аналізу і звітності, аби надати інформацію щодо кіберінцидентів, час реагування і загальну ефективність реагування на кіберінциденти. Такі звіти дозволяють організаціям правильно визначити сфери, що потребують покращення, а також оцінити успішність своїх зусиль із реагування на кіберінциденти.
- **Постійне вдосконалення**. SOAR підтримує постійне вдосконалення, допомагаючи організаціям аналізувати минулі кіберінциденти, оновлювати посібники на основі отриманих «уроків», а також адаптувати стратегії реагування на майбутні загрози. Цей постійний процес сприяє загальній стійкості організації проти кіберзагроз.
- **Масштабованість**. Платформи SOAR були першочергово розроблені задля масштабування відповідно до розміру і складності операцій із кібербезпеки організації. Вони мають змогу ефективно обробляти велику кількість подій та кіберінцидентів.

Впровадження технології SOAR дозволить організаціям реагувати на кіберінциденти більш проактивно і ефективно, зменшуючи при цьому ручні зусилля, потрібні для виконання повторюваних задач, та дозволяючи при цьому командам безпеки зосереджуватися на більш складних та стратегічних аспектах реагування на кіберінциденти. Платформи SOAR мають вирішальну роль в модернізації операцій із кібербезпеки та покращенні загальної кібербезпеки організацій.

Підводячи підсумки, в цьому розділі було проаналізовано необхідність розслідування кіберінцидентів, проаналізовано загрози корпоративним інформаційним системам, а також проаналізовано сучасні технології розслідування кіберінцидентів.

2 МЕТОДИ ТА ЗАСОБИ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

2.1. Архітектура рішення i2 Analyst’s Notebook

i2 Analyst's Notebook — це програмний продукт від i2 Group для аналізу даних. Базуючись на методології ELP (entity-link-property), він розкриває зв’язки між об’єктами даних, щоб виявити закономірності та надати розуміння даних. Його зазвичай використовують цифрові аналітики правоохоронних, військових та інших державних розвідувальних агенцій, а також відділи боротьби з шахрайством. Це частина програми Human Terrain System, програми армії Сполучених Штатів, яка об’єднує соціологів у бойові бригади. Відомо, що кілька розслідувань, у тому числі розслідування шахрайства в армії США, використовували його. Він також використовується шведською поліцією для аналізу соціальних контактів і соціальних мереж [15].

i2 Analyst’s Notebook розроблено, щоб допомогти аналітикам отримувати та відкривати інформацію, а також створювати та публікувати розвідувальні продукти шляхом об’єднання цієї інформації. **Логічна** архітектура, **фізична** архітектура та архітектура **безпеки** i2 Analyst’s Notebook підтримують ці функції.

Логічна архітектура визначає компоненти i2 Analyst’s Notebook і те, як вони взаємодіють один з одним. Логічна архітектура i2 Analyst’s Notebook включає методи, за допомогою яких дані надходять і обробляються, надані послуги та клієнти, за допомогою яких користувачі взаємодіють з i2 Analyst’s Notebook.

У кожному розгортанні i2 Analyst’s Notebook логічна архітектура відображається у фізичній архітектурі, де компоненти розгортаються та з’єднуються один з одним. Фізична архітектура i2 Analyst’s Notebook може відрізнятися залежно від мети розгортання, вимог до продуктивності та доступності, а також будь-якої спеціальної функції, яка реалізується.

Архітектура безпеки дозволяє i2 Analyst's Notebook автентифікувати користувачів і визначати їхній рівень авторизації для кожного елемента, яким він керує. Стороння реалізація архітектури безпеки може використовувати технології, альтернативні тим, які використовуються в стандартному розгортанні i2 Analyst's Notebook, за умови, що альтернативні технології відповідають вимогам, визначеним архітектурою безпеки.

Логічна архітектура. Логічну архітектуру можна розглядати з точки зору **даних**, які обробляє i2 Analyst's Notebook, **служб**, які обробляють дані, і **клієнтів**, які отримують доступ до даних.

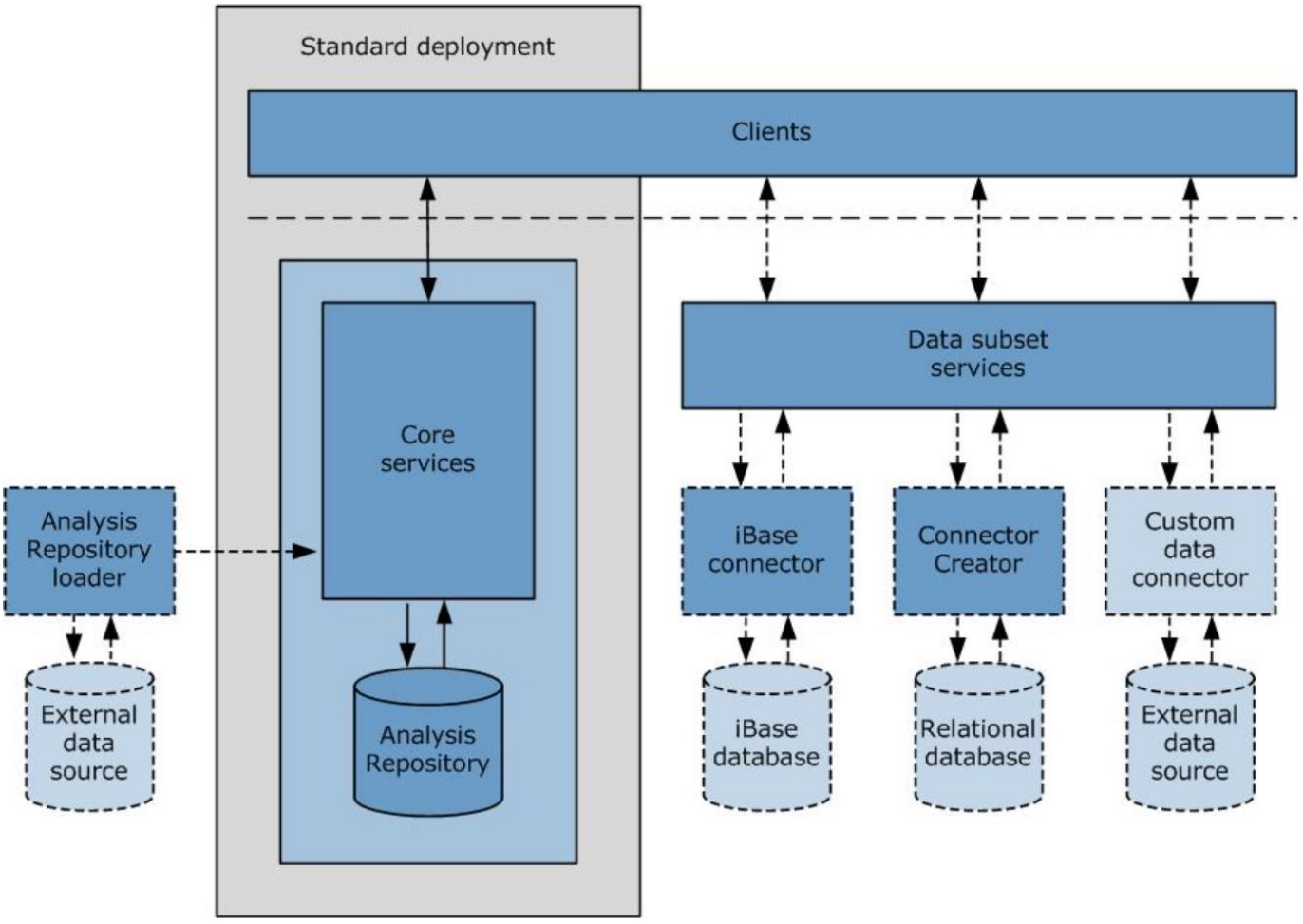

Рис. 2.1. Схема логічної архітектури i2 Analyst's Notebook

Дані. i2 Analyst's Notebook може приймати дані з різних зовнішніх джерел і

надавати їх користувачам для аналізу. Характеристики джерела даних визначають найбільш підходяще місце для зберігання або обробки даних:

- **Репозиторій аналізу**. Репозиторій аналізу – це спільний репозиторій для перевірених даних розвідки. Репозиторій аналізу містить високоцінні записи, які аналітики створили з вихідних даних, а потім помістили в репозиторій аналізу. Дані також можна розміщувати безпосередньо в репозиторії аналізу шляхом прямого завантаження даних за допомогою завантажувача репозиторія аналізу. Дані в репозиторії аналізу можна отримати для подальшого аналізу, а потім змінити за результатами аналізу.
- **Зовнішні джерела даних через з'єднувачі даних**. Доступ до даних із зовнішнього джерела даних можна отримати через з'єднувач даних, який використовує налаштовані служби для читання даних із зовнішнього джерела даних у відповідь на запит користувача. Якщо зовнішнім джерелом даних є i2 iBase або реляційна база даних із досить простою структурою, i2 Analyst's Notebook має інструменти, які полегшують створення з'єднувачів даних. Організація також може реалізувати спеціальний з'єднувач даних. З'єднувачі даних перетворюють дані у форму, готову для аналізу. Дані у вихідному джерелі даних не змінюються в результаті аналізу.

Служби. Служби i2 Analyst's Notebook дозволяють користувачам виконувати операції з даними, які зберігаються та надаються i2 Analyst's Notebook. Наступні служби дозволяють переміщувати дані на сервер i2 Analyst's Notebook і з нього:

- Для репозиторію аналізу основні служби дозволяють користувачам виявляти та отримувати елементи для подальшого аналізу, а також дозволяють користувачам виконувати операції з даними, що зберігаються в сховищі аналізу.

- Для зовнішнього джерела даних, доступ до якого здійснюється через з'єднувач даних, i2 Analyst's Notebook надає служби підмножини даних, які використовує з'єднувач даних для отримання та надання зовнішніх даних користувачам.

Інші основні служби дозволяють користувачам налаштовувати та підписуватися на сповіщення про зміни елементів, перевіряти зміни елементів, очищати елементи та адмініструвати компоненти i2 Analyst's Notebook.

Клієнти. Аналітики використовують такі клієнти для виявлення та аналізу даних, які зберігаються та надаються i2 Analyst's Notebook:

- Intelligence Portal надає можливості пошуку, виявлення та візуалізації через веб-браузери.
- Analyst's Notebook Premium забезпечує поглиблене виявлення, візуальний аналіз і можливості створення розвідки через багатофункціональний клієнт для робочого столу.

Фізична архітектура. Компоненти i2 Analyst's Notebook підтримують різні параметри фізичної архітектури. Планувати фізичну архітектуру потрібно відповідно до логічної архітектури та вимог до продуктивності та доступності організації.

Логічна архітектура розроблена для гнучкого розгортання сховища даних i2 Analyst's Notebook, служб i2 Analyst's Notebook і з'єднувачів даних для зовнішніх джерел даних. У невеликих розгортаннях багато компонентів можна розмістити разом. Для покращення масштабованості або кращої відповідності існуючій мережевій архітектурі компоненти можна розгортати окремо на кількох серверах. На рисунку нижче показано фізичну архітектуру розгортання i2 Analyst's Notebook:

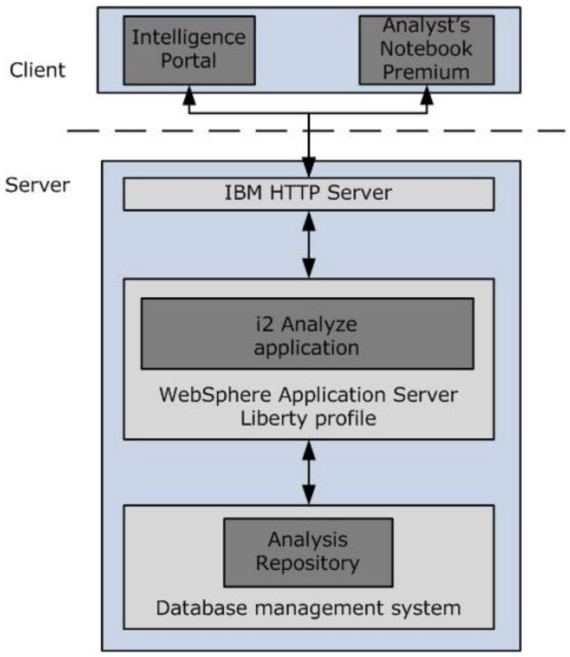

Рис. 2.2. Схема фізичної архітектури i2 Analyst's Notebook

Розгортання i2 Analyst's Notebook використовує такі компоненти фізичної архітектури, щоб забезпечити елементи логічної архітектури:

- **Компоненти для даних**. Репозиторій аналізу, розміщений у сумісній системі керування базою даних, якою може бути база даних DB2 або, альтернативно, база даних Oracle або Microsoft SQL Server.
- **Компоненти для служб**. Сервер профілів WebSphere Application Server Liberty, програма i2 Analyst's Notebook, яка надає основні служби i2 Analyst's Notebook (ця програма розміщена в профілі WebSphere Application Server Liberty), а також примірник HTTP Server, який діє як проксі-сервер для запитів клієнтів.
- **Компоненти для клієнтів**. Intelligence Portal, веб-клієнт, який доступний користувачам через веб-браузери (Intelligence Portal — це веб-клієнт Microsoft Silverlight, для якого потрібен плагін браузера), а також Analyst's Notebook Premium, багатофункціональний клієнт, який інсталюється локально на робочих станціях користувачів.

Архітектура безпеки. Архітектура безпеки i2 Analyst’s Notebook підтримує поведінку, яку вимагає модель безпеки i2 Analyst’s Notebook. Кожна служба i2 Analyst’s Notebook може взаємодіяти з архітектурою безпеки, щоб визначити, які права має поточний користувач для операції, яку він хоче виконати.

i2 Analyst’s Notebook автентифікує користувачів за допомогою вибору технологій і визначає їхній рівень авторизації для кожного елемента, яким він керує. Модель безпеки i2 Analyst’s Notebook базує свою поведінку на взаємодії між значеннями параметрів безпеки, які мають елементи, і дозволами безпеки, які мають групи користувачів.

- Користувачі класифікують елементи в репозиторії аналізу, призначаючи їм значення з параметрів безпеки. Значення, яке має елемент у певному вимірі безпеки, впливає на те, чи можуть користувачі переглядати або редагувати цей елемент (безпека доступу), або змінювати значення його виміру (надати безпеку).
- Дозволи безпеки застосовуються до груп користувачів. Для кожної групи вони пов’язують рівні доступу або надання безпеки з окремими значеннями параметрів, які можуть мати елементи. Членство в групах часто визначається назвами посад або допуском до безпеки користувачів, яких вони містять.

Компоненти розгортання i2 Analyst’s Notebook взаємодіють з архітектурою безпеки в такий спосіб:

- Під час входу профіль WebSphere Application Server Liberty вимагає від клієнтів автентифікації, перш ніж вони зможуть взаємодіяти з i2 Analyst’s Notebook. Після успішної автентифікації клієнт отримує маркер легкої сторонньої автентифікації у файлі cookie.
- Під час звичайної роботи клієнт передає файл cookie назад до i2 Analyst’s

Notebook, де кожна служба i2 Analyst's Notebook забезпечує права доступу до даних відповідно до своєї конкретної функції.

На рисунку нижче показано, як працює безпека в стандартному розгортанні i2 Analyst's Notebook:

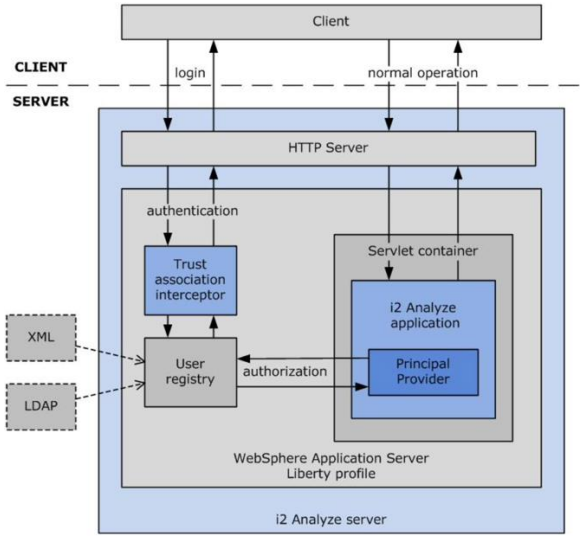

Рис. 2.3. Схема архітектури безпеки i2 Analyst's Notebook

У стандартному розгортанні i2 Analyst's Notebook, яке використовує клієнт Intelligence Portal і репозиторій аналізу, автентифікація та авторизація відбуваються наступним чином:

- Автентифікація між клієнтом Intelligence Portal і профілем WebSphere Application Server Liberty здійснюється через перехоплювач довірчих асоціацій, який надається разом із i2 Analyst's Notebook.
- Перехоплювач довірчих асоціацій взаємодіє з реєстром користувачів профілю WebSphere Application Server Liberty, щоб перевірити облікові дані, які користувач надає через клієнта. Реєстр користувачів — це служба, яка надає доступ до інформації про користувачів і групу, яка може зберігатися у файлі XML, одному чи кількох реєстрах LDAP або в будь-якому подібному сховищі, яке може використовувати профіль WebSphere

Application Server Liberty.

- Щоб авторизувати користувачів клієнта Intelligence Portal для доступу до елементів у репозиторії аналізу, програма i2 Analyst’s Notebook зв’язується з реєстром користувачів профілю WebSphere Application Server Liberty для отримання інформації про членство поточного користувача в групах. Потім основний постачальник зіставляє отриману інформацію з дозволами групи, визначеними в розділі дозволів безпеки схеми безпеки i2 Analyst’s Notebook. Це зіставлення залежить від розгортання, оскільки схема безпеки залежить від розгортання.
- Код у кожній службі i2 Analyst’s Notebook порівнює дозволи поточного користувача зі значеннями параметрів безпеки для елементів, щоб визначити, які права користувач отримує для кожного елемента.

Технології на схемі не є фіксованими. Можна надати інший перехоплювач довірчих асоціацій і використовувати будь-яке підтримуване сховище для реєстру користувачів. Вимоги такі:

- Служба i2 Analyst’s Notebook повинна мати можливість отримувати інформацію про користувача з наданих облікових даних.
- Потенційно специфічний для розгортання модуль має зіставляти інформацію користувача з членством у групах, названих у розділі дозволів безпеки схеми безпеки i2 Analyst’s Notebook.

Якщо реалізація архітектури безпеки відповідає цим вимогам, вона підходить для використання в розгортанні i2 Analyst’s Notebook.

2.2. Призначення та функції рішення i2 Analyst's Notebook

Програма i2 Analyst's Notebook надає основні служби та інфраструктуру, які дозволяють клієнтам створювати, переглядати, аналізувати та оновлювати дані, до яких i2 Analyst's Notebook має доступ.

Сервіси для репозиторія аналізу. Основні служби забезпечують взаємодію між клієнтами та репозиторієм аналізу, як показано на наступному рисунку.

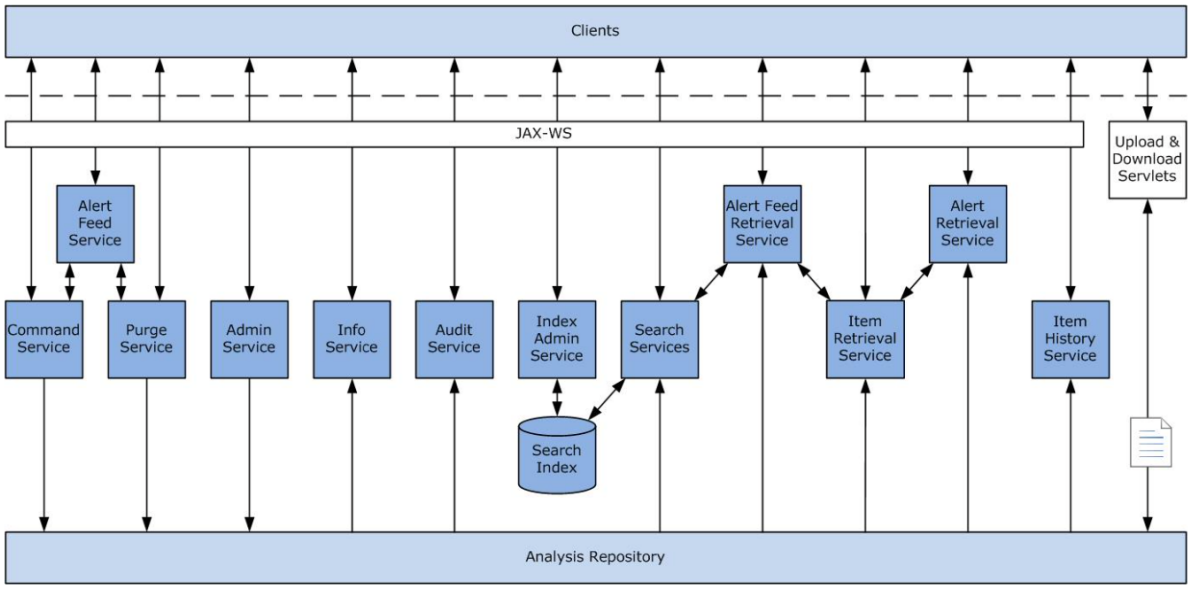

Рис. 2.4. Взаємодія між клієнтами та репозиторієм аналізу

Клієнти не користуються службами для завантаження документів у репозиторій аналізу або їх вивантаження з нього. Натомість завантаження та вивантаження документів обробляються парою сервлетів.

Сервіси для з'єднувачів даних. i2 Analyst's Notebook надає послуги для підтримки з'єднувачів даних. Клієнти використовують ці служби для запитів і отримання результатів із зовнішніх джерел даних через інтерфейс користувача Intelligence Portal.

З'єднувачі даних створюють і запитують відносно короткочасні підмножини з

більших обсягів даних. Ці операції підтримуються двома службами, які розробники повинні налаштувати для кожного з'єднувача даних відповідно до вимог зовнішнього джерела даних.

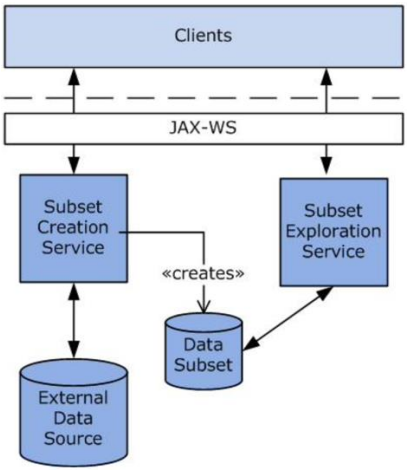

Рис. 2.5. Схема сервісів для з'єднувачів даних

Служба адміністрування. Служба адміністрування i2 Analyst's Notebook дозволяє клієнтам ініціалізувати та налаштувати i2 Analyst's Notebook і репозиторій аналізу. Служба адміністрування також забезпечує контроль над схемою безпеки.

Операції, які змінюють схему i2 Analyst's Notebook або схему безпеки, суворо обмежені після розгортання i2 Analyst's Notebook. Внесення значних змін до схеми або схеми безпеки еквівалентно запуску нового розгортання i2 Analyst's Notebook.

Сервіс сповіщень. Сервіс каналів сповіщень i2 Analyst's Notebook дозволяє клієнтам створювати, керувати та видаляти канали сповіщень у репозиторії аналізу. Служба подачі сповіщень діє як інтерфейс до служб команд і чистки.

З точки зору моделі даних i2 Analyst's Notebook, канал сповіщень є особливим типом елемента. Коли користувач підписується на канал сповіщень, i2 Analyst's Notebook створює зв'язок між елементом користувача та елементом каналу сповіщень.

Служба каналу сповіщень надає клієнтам інтерфейс для певного домену для

створення та редагування елементів каналу сповіщень у репозиторії аналізу.

Шаблон, за допомогою якого служба подачі сповіщень використовує служби команд і очищення для маніпулювання репозиторієм аналізу, є моделлю для спеціальних служб. Розробники можуть розширити i2 Analyst's Notebook, написавши власні служби, які використовують стандартні можливості i2 Analyst's Notebook.

Служба пошуку каналів сповіщень. Стандартна служба пошуку каналів сповіщень i2 Analyst's Notebook дозволяє клієнтам отримувати канали сповіщень і визначати, на які канали вони підписані. Служба пошуку каналів сповіщень має єдиний метод пошуку каналів сповіщень.

Служба отримання сповіщень. Стандартна служба отримання сповіщень i2 Analyst's Notebook дозволяє клієнтам отримувати сповіщення, створені каналами сповіщень. Служба отримання сповіщень має єдиний метод для отримання сповіщень із низкою обмежень.

Служба аудиту. Стандартна служба аудиту i2 Analyst's Notebook підтримує постійний запис усіх змін, які відбуваються з елементами в репозиторії аналізу. Служба аудиту повідомляє тип будь-якої зміни, коли вона відбулася, хто її вніс та IP-адресу, з якої вона була зроблена. Служба аудиту надає клієнтам єдиний веб-метод для виклику.

Коли елемент видаляється зі сховища аналізу, служба аудиту додає запис цієї події та зберігає свої записи всіх попередніх подій. Записи аудиту для очищених елементів не містять інформації про сам елемент; вони зберігають лише типи подій, які вплинули на елемент.

Служба команд. Служба команд i2 Analyst's Notebook дозволяє клієнтам виконувати команди, які змінюють дані в репозиторії аналізу. Служба команд також керує службою, яка допомагає визначити, які команди клієнт може виконати для певного елемента в певний час.

Служба команд дозволяє клієнтам створювати, об’єднувати, змінювати та видаляти елементи, групувати елементи в набори та змінювати дозволи безпеки для елементів. Функції, які надає служба команд, повністю задокументовані в документації i2 Analyst’s Notebook SDK API.

Щоб захистити від одночасних модифікацій, служба команд вимагає від клієнтів взяти елемент під свій контроль перед тим, як їм буде дозволено його змінювати. Клієнти беруть елементи під свій контроль неявно, коли вони їх створюють, або явно, виконуючи команду "взяти під контроль".

Лише один клієнт може мати право керування на певний предмет одночасно. Термін керування закінчується після настроюваного періоду, але клієнти, яким потрібні коротші або довші періоди керування, можуть розірвати або продовжити їх.

Щоб скористатися службою команд, клієнт створює команди, розміщує їх у списку та надсилає службі для виконання. Порядок команд у списку важливий, оскільки команда, яка керує елементом, має стояти перед командою, яка його змінює. Служба команд перевіряє список надісланих команд, який включає перевірку керування, версій і прав доступу. Потім служба команд виконує команди в списку атомарно, так що весь список повністю вдається або повністю не виконується.

Служба адміністрування індексу. Стандартна служба адміністрування індексу i2 Analyst’s Notebook надає клієнтам можливість зробити знімок індексу пошуку. Знімок, зроблений службою адміністрування індексу, може створити резервну копію, не впливаючи на нього одночасними змінами в індексі. Служба адміністрування індексу має один метод для створення знімка індексу пошуку, а інший – для випуску знімка після створення резервної копії.

Інформаційна служба. Інформаційна служба i2 Analyst’s Notebook дозволяє клієнтам знаходити інформацію про запущений екземпляр i2 Analyst’s Notebook. Інформаційна служба також надає кілька простих корисних методів. Через

інформаційну службу клієнти можуть отримати:

- Джерела даних, до яких підключено цей екземпляр i2 Analyst’s Notebook
- Схема, яка визначає типи елементів, доступні в цьому екземплярі
- Схема діаграми, яка описує, як елементи з i2 Analyst’s Notebook відображаються під час візуалізації
- Схема безпеки, яка контролює, як користувачі можуть переглядати та взаємодіяти з елементами в i2 Analyst’s Notebook
- Основне ім’я поточного користувача (наприклад для того, щоб клієнт міг відобразити його в інтерфейсі користувача)

Інформаційна служба також надає корисні методи, за допомогою яких клієнт може знайти більше інформації для поточного користувача:

- Рівні безпеки, які користувач матиме для елемента з певними дозволами
- Параметри безпеки, про які користувач має дозвіл знати
- Глобалізовані дані про часові пояси, які підтримує цей екземпляр i2 Analyst’s Notebook

Нарешті, інформаційна служба надає доступ до механізму реєстрації, який можуть використовувати інші служби, а також спосіб перевірки того, чи дійсне дане значення дати та часу.

Служба історії елементів. Стандартна служба історії елементів i2 Analyst’s Notebook надає клієнтам інформацію про те, як елементи в репозиторії аналізу змінювалися з часом. Елементи в репозиторії аналізу можуть змінюватися в результаті операцій редагування та злиття. Служба історії елементів подібна до служби пошуку елементів, але вона надає інший перегляд інформації в репозиторії аналізу.

Клієнти надають службі історії елементів ідентифікатори елементів, які вони отримали раніше. Клієнти можуть попросити службу надати детальну інформацію про

розвиток елементів, відмінності між версіями одного елемента або об'єднати інформацію.

Служба відновлення елементів. Стандартна служба відновлення елементів i2 Analyst's Notebook дозволяє клієнтам відновлювати конкретні версії конкретної інформації в репозиторії аналізу.

Клієнт i2 Analyst's Notebook надає службі відновлення елементів один або більше ідентифікаторів елементів. Клієнт отримує ідентифікатори елементів із служби пошуку або самої служби відновлення елементів. Ідентифікатори можуть бути додатково кваліфіковані номерами версій. Тоді служба відновлення елементів надає такі функції.

Результати, які служба відновлення елементів повертає клієнтам, підпадають під дію правил безпеки i2 Analyst's Notebook. Клієнти ніколи не бачать елементи, дозволи яких диктують, що користувач не має доступу до них.

Служба очищення. Служба очищення i2 Analyst's Notebook дозволяє клієнтам видаляти всі сліди зазначених елементів (окрім їхніх ідентифікаторів записів) з репозиторію аналізу. Це спеціально було розроблено таким чином, що неможливо отримати або відновити очищений елемент.

Архітектурно служба очищення схожа на службу команд. Однак функціонально служба очищення відрізняється. Через дії, яка вона виконує, можливість користувачів отримати доступ до служби очищення контролюється окремо від їхньої здатності видавати інші команди. Користувачі, які мають доступ до служби очищення, можуть очистити будь-який елемент у репозиторії аналізу, незалежно від їхніх інших дозволів. Служба очищення містить два веб-методи, які клієнти можуть визивати.

Отримавши вказівку на очищення елемента або набору з репозиторію аналізу, служба очищення виконує такі дії:

- Бере елемент в управління, при необхідності примусово.
- Він управляє будь-якими посиланнями, пов’язані з елементом, з тим самим положенням.
- Він видаляє всі дані про управляючі елементи з репозиторію аналізу.

Служба стандартного аудиту повідомляє, що чистка відбулася, але більше інформації не зберігає.

Служби пошуку. Стандартні служби пошуку i2 Analyst’s Notebook та мережевого пошуку дозволяють клієнтам переглядати, запитувати та розгортати останні версії даних у репозиторії аналізу. Клієнти служб пошуку та пошуку в мережі отримують результати, які можна сортувати, фільтрувати або оцінювати за низкою критеріїв.

Для клієнтів i2 Analyst’s Notebook пошук у репозиторії аналізу зазвичай складається з двох частин:

1. Клієнт вказує частину або всю наступну інформацію:

- Текст або інші значення властивостей, які потрібно шукати
- Набір, що містить елементи, які необхідно розглянути
- Відносини, які повинні існувати між будь-якими поверненими елементами
- Типи елементів, які має повернути пошук
- Властивості, за якими можна фільтрувати будь-які знайдені елементи

У відповідь служби пошуку повертають підсумок результатів, який містить кількість відповідних елементів і їх типи.

2. Клієнт вказує маркер для виконаного пошуку та частину або всю наступну інформацію:

- Типи результатів, які він хоче отримати

- Властивості, за якими виконується подальша фільтрація
- Критерії, за якими сортують елементи

Потім служби пошуку повертають клієнту фактичні результати щодо елементів, включаючи (за необхідності) вказівку того, наскільки добре кожен елемент відповідає початковим критеріям пошуку. Цей підхід відображено в веб-методах, які служби пошуку роблять доступними клієнтам для виклику.

Сервіси пошуку реалізують правила безпеки i2 Analyst's Notebook. Підсумок результатів містить інформацію лише про елементи, до яких має доступ користувач, який здійснював пошук.

Сервіси з'єднувача даних. i2 Analyst's Notebook визначає служби, які дозволяють отримувати дані через з'єднувачі даних. Клієнти використовують ці служби для запитів і отримання результатів із зовнішніх джерел даних через інтерфейс користувача Intelligence Portal.

З'єднувачі даних створюють і запитують відносно короткочасні підмножини з більших обсягів даних. Ці операції підтримуються службами, які розробники можуть використовувати в кожному з'єднувачі даних відповідно до вимог відповідного зовнішнього джерела даних.

1. Служба створення підмножини зовнішніх даних. В i2 Analyst's Notebook служба створення підмножини зовнішніх даних використовується як перший етап з'єднувача даних. Цей етап з'єднувача отримує дані із зовнішнього джерела даних. Служба створення підмножини дозволяє користувачам виконувати пошук із зовнішнім джерелом даних із стандартного інтерфейсу користувача Intelligence Portal. Потім він повертає ідентифікатор, який представляє підмножину даних, повернутих із запиту, за якими виконується подальший аналіз.

Служби створення підмножини зовнішніх даних можуть підтримувати 5 веб-методів. У реалізації, де зовнішнє джерело даних не підтримує певні типи запитів,

можна вимкнути деякі методи для з’єднувача даних.

2. Служба дослідження підмножини зовнішніх даних. В i2 Analyst’s Notebook служба дослідження підмножини зовнішніх даних використовується як другий етап з’єднувача даних. Цей етап з’єднувача дозволяє користувачам Intelligence Portal виконувати аналіз підмножини даних, отриманих із зовнішнього джерела даних. Служба дослідження підмножини дозволяє клієнтам переглядати отримані дані, робити запити та розгортати їх. Як правило, другий етап з’єднувача даних також відповідає за перетворення даних у підмножині у формат, сумісний зі схемою i2 Analyst’s Notebook.

Служби дослідження підмножини зовнішніх даних підтримують 8 веб-методів. Після отримання даних із зовнішнього джерела та створення підмножини всі ці методи доступні для даних у підмножині [4].

2.3. Вимоги до розгортання рішення i2 Analyst’s Notebook

Операційні системи. Для запуску продуктів i2 необхідно переконатися, що використовується підтримувана операційна система.

Підтримувані операційні системи:

- Windows 11 22H2 Enterprise/Professional
- Windows 11 21H2 Enterprise/Professional
- Windows 10 Enterprise/Professional
- Windows Server 2022/2019/2016/2012 R2 Datacenter Edition
- Windows Server 2022/2019/2016/2012 R2 Essentials Edition
- Windows Server 2022/2019/2016/2012 R2 Standard Edition

Продукти i2 підтримуються в середовищах апаратної віртуалізації, які працюють під керуванням будь-якої з операційних систем, перелічених у детальних системних вимогах. Коли користувач працює у віртуальному середовищі, будь-які проблеми, які можуть бути відтворені i2 у підтримуваній операційній системі, вирішуються за допомогою стандартної політики підтримки. Пробні версії i2 Analyst's Notebook не можна запускати у віртуалізованих середовищах.

Програмне забезпечення. Щоб запустити продукти i2, потрібно переконатися, що середовище містить перераховане нижче програмне забезпечення, що є обов'язковим. Крім того, може знадобитися інсталювати супутнє програмне забезпечення, щоб покращити робочий процес.

Остання версія i2 Analyst's Notebook (9.4.0) сумісна з:

- i2 iBase 9.1.0
- i2 iBridge 9.4.0
- i2 Analyst's Notebook Connector for Esri 9.4.0
- Ця версія Analyst's Notebook Premium використовує Chromium Embedded Framework (CEF) 94.4.20. Потрібно використовувати ту саму версію CEF для сторонніх плагінів.

Передумови середовища виконання та його мінімальної версії показано на таблиці 2.1.

Таблиця 2.1.

Передумови середовища виконання та його мінімальної версії

Середовище виконання	**Мінімальна версія**
Microsoft .NET Framework 3.5	SP1
Microsoft .NET Framework 4.7	4.7.2
Microsoft .NET Framework 4.8	4.8

Потрібні як Microsoft .NET Framework 3.5 SP1, так і Microsoft .NET Framework 4.7.2 (або новіші пакети виправлень) або Microsoft .NET Framework 4.8.

Для користувачів Analyst's Notebook Premium зі сторонніми плагінами: несумісність версії Chromium Embedded Framework (CEF) може спричинити помилки в плагінах сторонніх розробників. Так як у процесі програми компонент CEF є єдиним компонентом, його можна ініціалізувати лише один раз. У плагінах сторонніх розробників, які залежать від версії, відмінної від версії, що працює в процесі Analyst's Notebook Premium, можуть виникати помилки. Щоб уникнути цих помилок, потрібно використовувати ту саму версію CEF, що міститься в Analyst’s Notebook Premium, і перевірити, чи CEF уже запущено, перш ніж запускати плагін.

Підтримуване програмне забезпечення:

- Геоінформаційні системи
- Сервер ESRI для ArcGIS (версії 10 і майбутніх версій, випусків і пакетів виправлень)
- Звітність та аналіз (Microsoft Office 2016/2019/365 Enterprise і майбутні пакети виправлень)

Якщо необхідно імпортувати електронні таблиці Excel, то потрібно інсталювати Microsoft Access Database Engine 2010 Redistributable (32-розрядна версія).

Апаратне забезпечення. Потрібно переконатися, що апаратне забезпечення, на яке встановлюється i2 Analyst’s Notebook, відповідає мінімальним системним вимогам. Залежно від середовища можна збільшити ці значення, щоб покращити продуктивність системи:

- *Місце на диску*. Принаймні 2 ГБ вільного місця на диску для встановлення та місця для зберігання даних. Ця цифра не включає дисковий простір,

необхідний для попередніх умов. Загальні вимоги до дискового простору залежать від кількості продуктів i2, які потрібно встановити.

- *Дисплей*. Мінімум – XGA-сумісна 1152x864 висококольорова 16-розрядна відеокарта та кольоровий монітор, рекомендовано - графічна карта з підтримкою SXGA 1280x1024, 16-бітна підтримка високого кольору та кольоровий монітор.
- *Оперативна пам'ять*. Мінімум – 2 ГБ, рекомендовано – 4 ГБ.
- *Процесор*. Мінімум – 1,4 ГГц, рекомендовано – 2 ГГц.

Підтримка мов. Продукти i2 тестуються на низці різноманітних регіональних варіантів операційних систем. Крім того, вони перекладені різними мовами.

Підтримка операційної системи – i2 підтримує цей продукт на кирилиці в підтримуваних операційних системах.

Підтримка даних – продукти i2 підтримують дані Unicode.

Перекладu – нажаль, українська мова не підтримується [5].

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАСТОСУВАННЯ ЗАСОБІВ БАГАТОВИМІРНОГО ВІЗУАЛЬНОГО АНАЛІЗУ НА БАЗІ РІШЕННЯ I2 ANALYST'S NOTEBOOK

3.1. Розроблення варіанта розгортання системи застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook

Згідно з попереднім підрозділом, для розгортання системи застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook, потрібно чітко слідувати вимогам щодо операційної системи, програмного і апаратного забезпечення.

Після завантаження інсталяційного носія для i2 Analyst's Notebook, потрібно витягнути інсталяційні файли з наданого медіафайлу. Для цього можна скористатися опцією «Витягти все» в меню Windows, яке відкривається правою кнопкою миші. Вміст буде розпаковано в те саме місце, що й інсталяційний медіафайл.

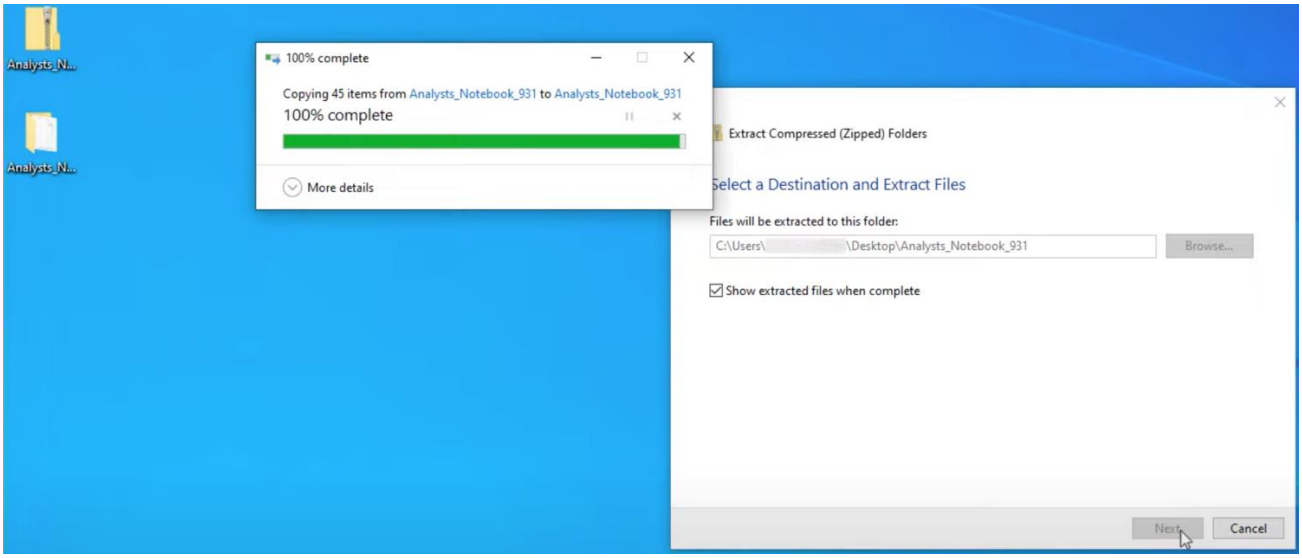

Рис 3.1. «Витягування» інсталяційних файлів з медіафайлу

Перш ніж почати інсталяцію i2 Analyst’s Notebook, спершу необхідно переконатися, що були виконані передумови щодо середовища виконання та його мінімальної версії, які були розглянуті у попередньому підрозділі. Після того, як усі передумови було виконано, потрібно відкрити папку Analyst’s Notebook, яка була створена під час вилучення інсталяційного носія. Двічі клацніть файл встановлення, щоб розпочати встановлення.

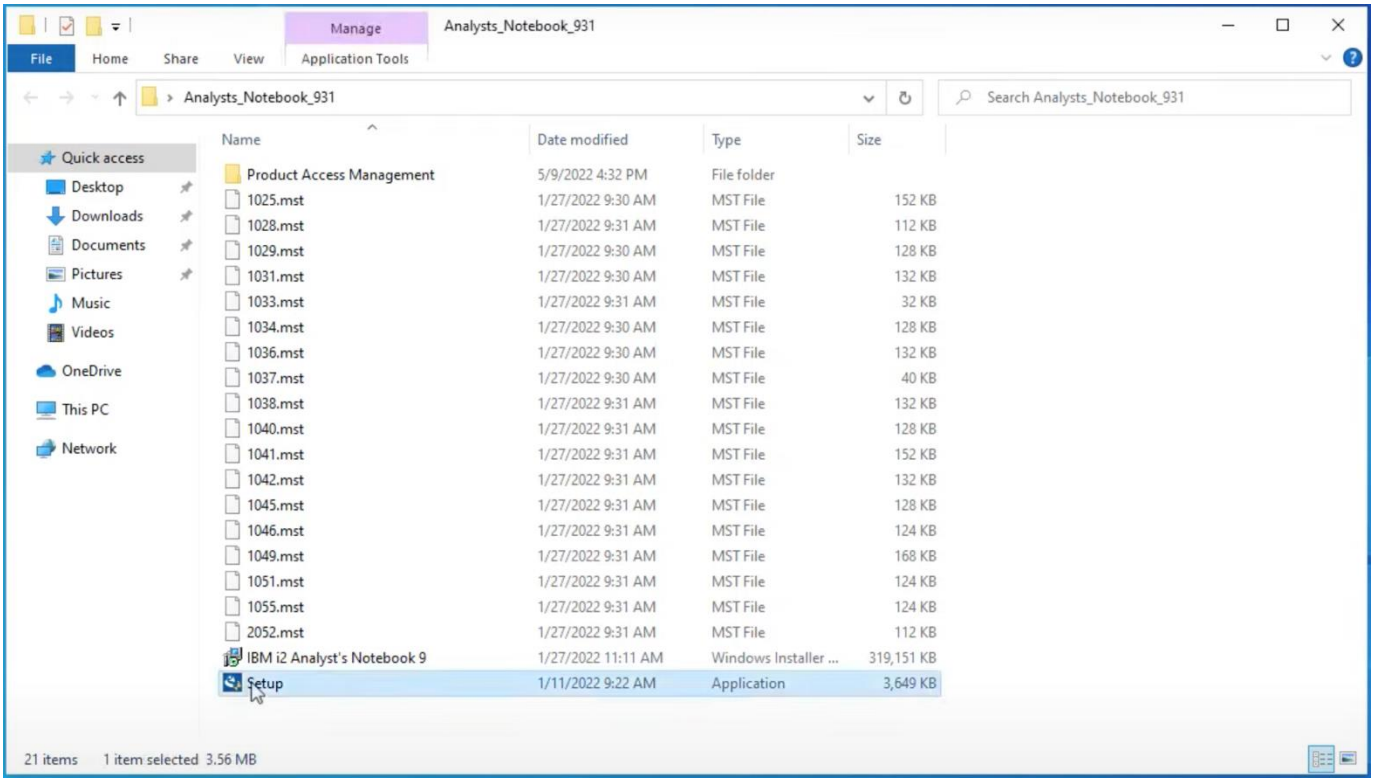

Рис 3.2. Відкриття файлу встановлення для початку інсталяції

Далі потрібно підтвердити відкриття, щоб дозволити інсталятору вносити зміни на комп’ютері.

Рис. 3.3. Надання дозволу на вносення змін на комп’ютері

Перш ніж можна буде інсталювати i2 Analyst's Notebook, потрібно прочитати та прийняти ліцензійну угоду, а потім натиснути «Далі», щоб продовжити встановлення.

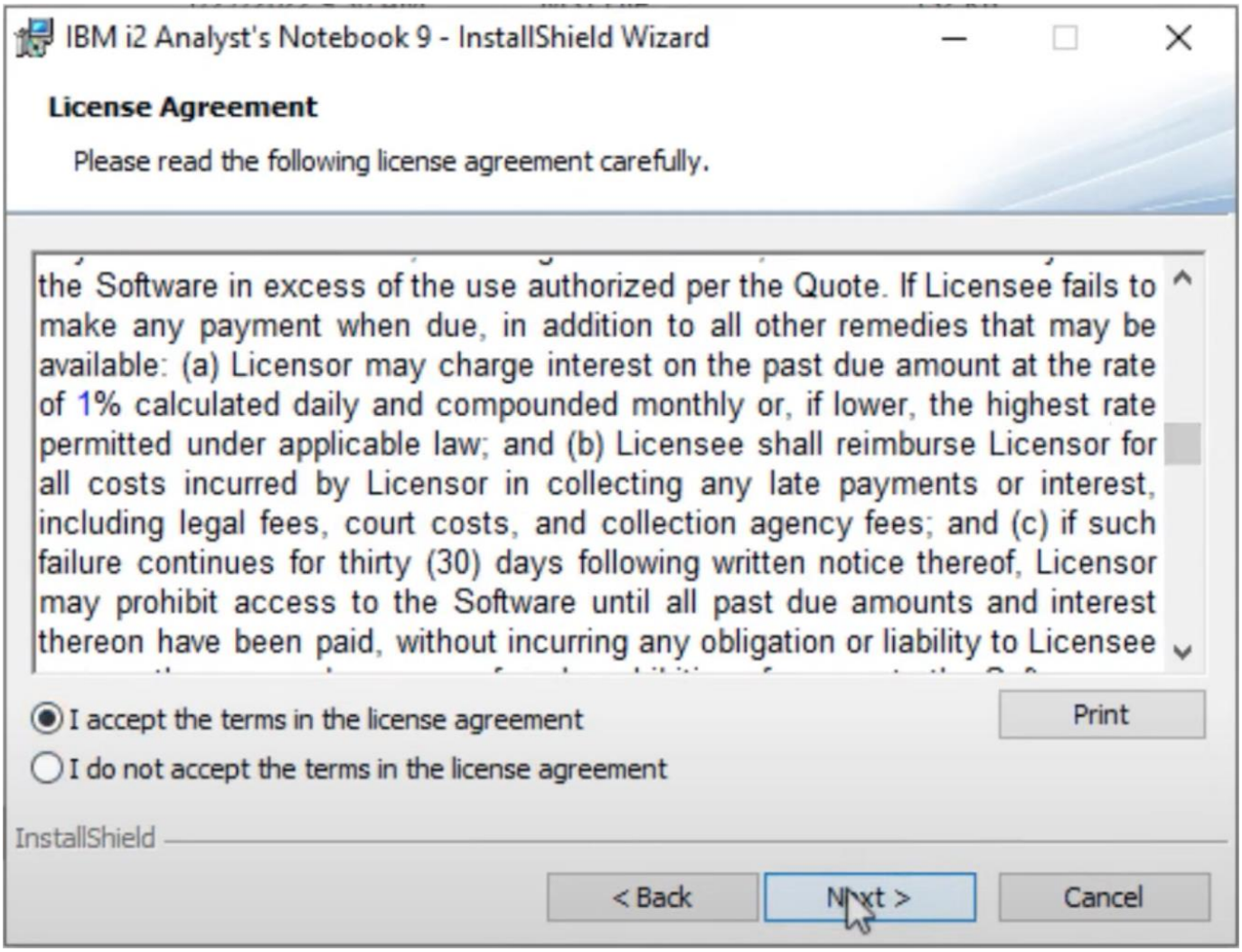

Рис. 3.4. Процес прийняття ліцензійної угоди

На наступному екрані можна встановити i2 Analyst's Notebook в іншу папку на комп’ютері, якщо ви бажаєте або повинні це зробити.

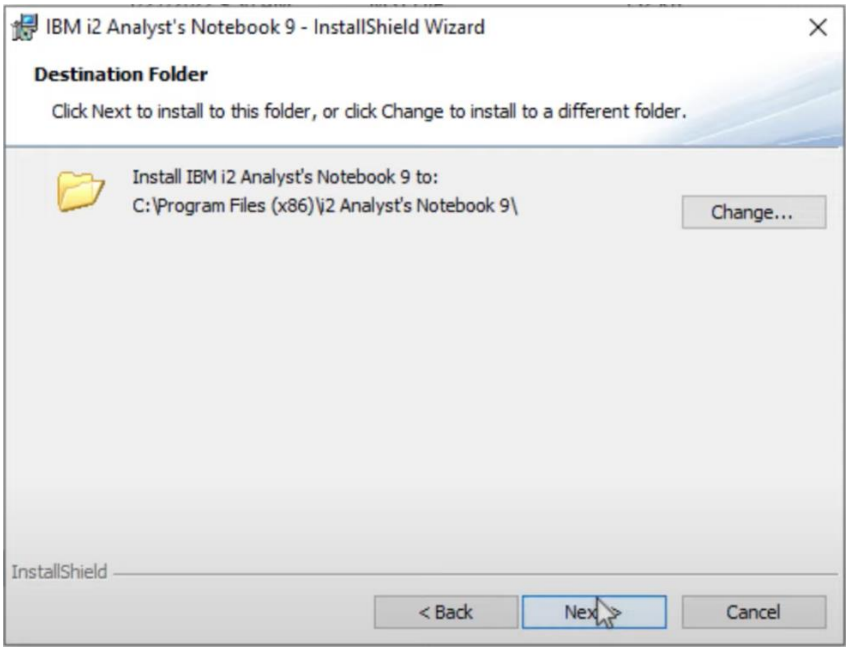

Рис. 3.5. Можливість встановити i2 Analyst's Notebook в іншу папку

На наступному екрані доступні два варіанти інсталяції – типова та індивідуальна.

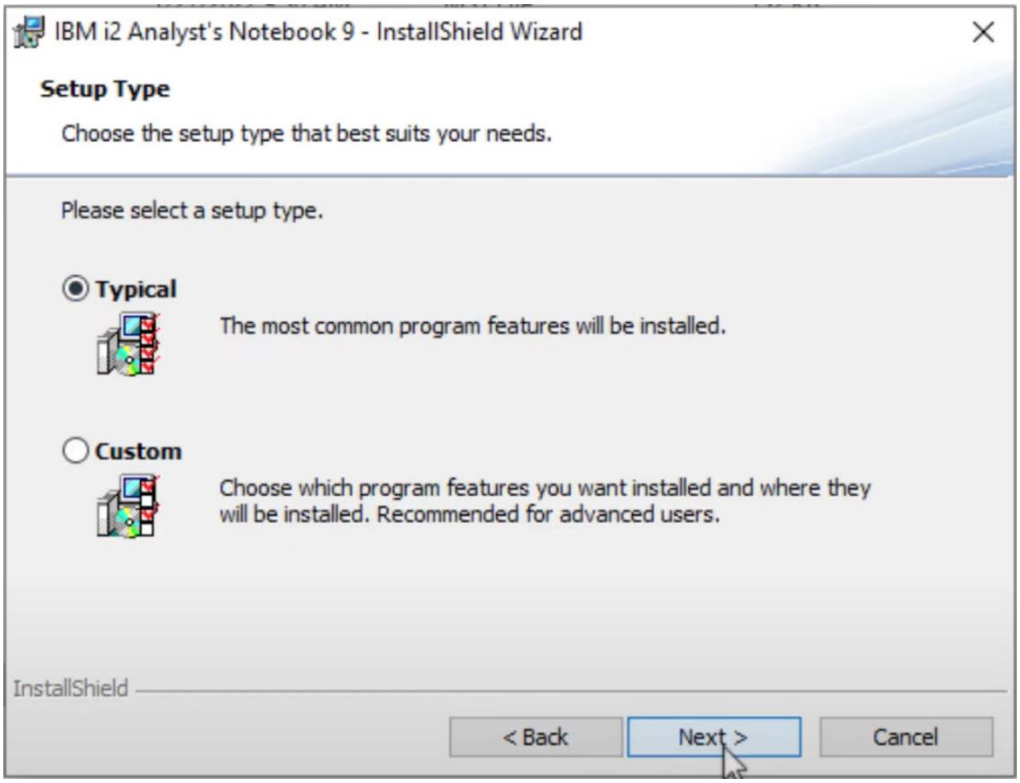

Рис. 3.6. Доступні варіанти інсталяції

Параметр індивідуальної інсталяції дозволяє вибрати окремі функції, а також мати змогу додати додаткові карти або не встановлювати ознайомлювальні матеріали.

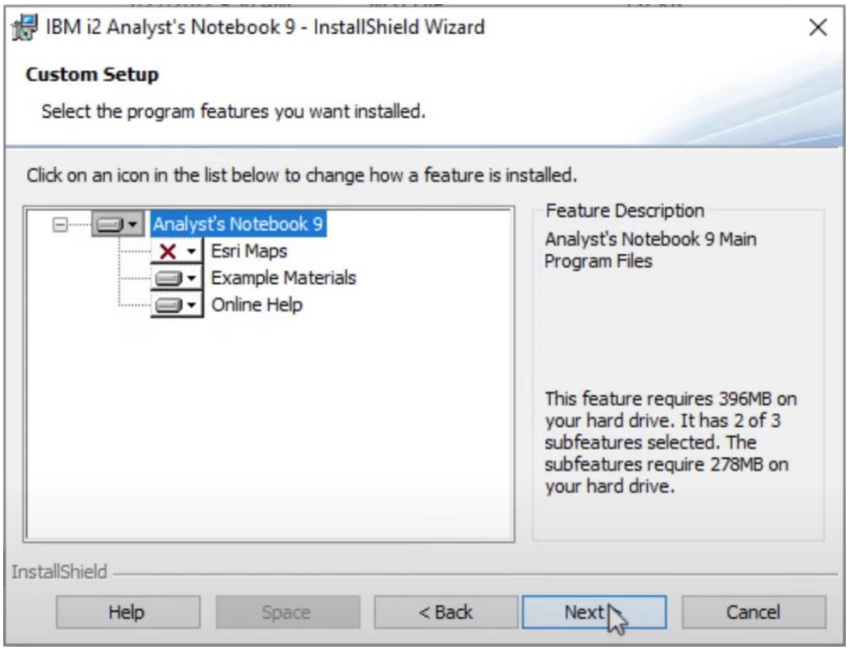

Рис 3.7. Параметри індивідуальної інсталяції

Типова інсталяція автоматично встановлює i2 Analyst’s Notebook, ознайомлювальні матеріали і онлайн-довідку. Після натискання «Встановити» почнеться процес встановлення i2 Analyst’s Notebook.

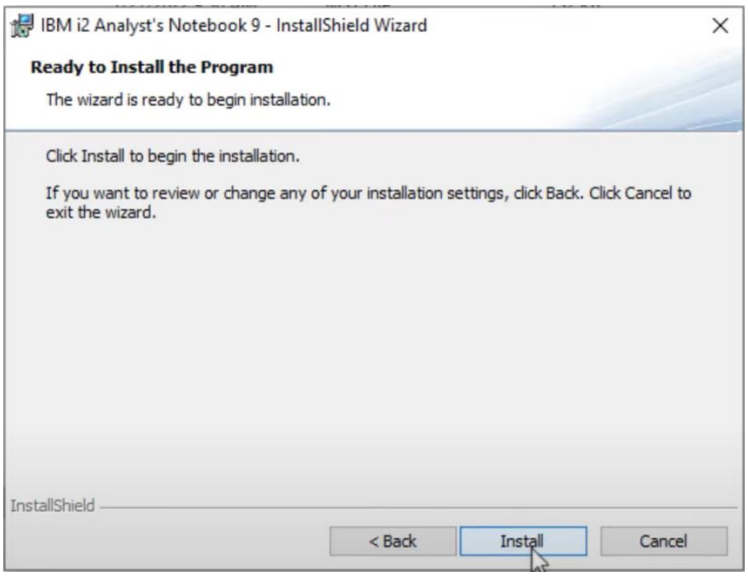

Рис. 3.8. Завершальний етап інсталяції

Завершення встановлення може зайняти деякий час.

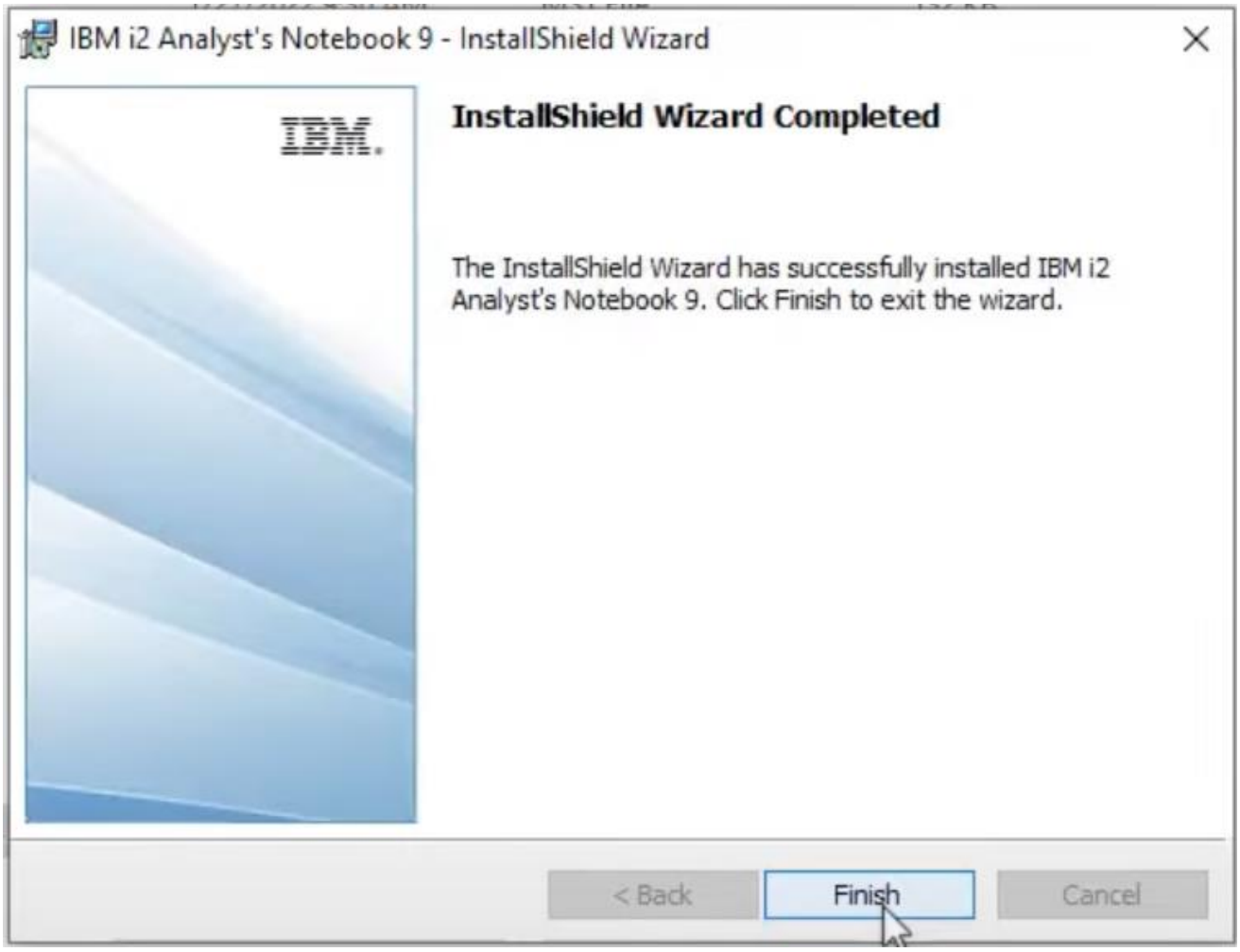

Рис. 3.9. Сповіщення про успішну інсталяцію

Якщо потрібно налаштувати i2 Analyst's Notebook іншою мовою, у меню Windows є опція для вибору потрібних параметрів мови [6].

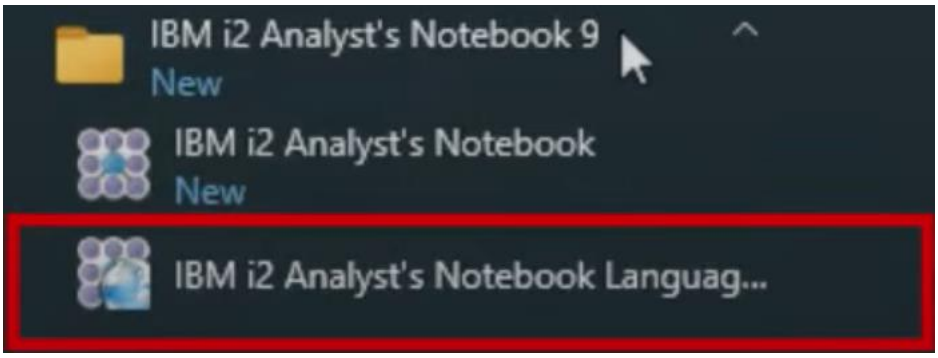

Рис. 3.10. Можливість налаштування продукту іншою мовою

3.2. Технологія застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook

Розуміння. i2 Analyst's Notebook — це багате середовище візуального аналізу, орієнтоване на дані, яке може зменшити витрати та час, пов'язані з багатовимірним аналізом.

i2 Analyst's Notebook збирає, керує та організовує інформацію та розвідку. Використовуючи i2 Analyst's Notebook, аналітики та дослідники легко виявляють мережі, закономірності та тенденції у зростаючих обсягах структурованих і неструктурованих даних.

Створення діаграм у i2 Analyst's Notebook надає користувачам широкий спектр можливостей візуального представлення даних. Відносини між такими об'єктами, як люди, майно та організації, чітко видно в цьому середовищі аналізу зв'язків. Аналітики можуть досліджувати та аналізувати мережі кількома способами, щоб зрозуміти асоціації, а також знаходити приховані зв'язки за допомогою розширених аналітичних можливостей i2 Analyst's Notebook [7].

Використання.

Дані i2 Analyst's Notebook. Щоб створити повну картину розслідування, i2 Analyst's Notebook може отримати доступ до даних із низки джерел. У i2 Analyst's Notebook дані зберігаються як сутності, посилання та властивості.

Діаграми. Діаграми відображають розвідувальні дані, які стосуються розслідування. Можна створювати діаграми як вручну, так і автоматично, використовуючи інформацію з різних джерел. Ця інформація може бути особистою інформацією, письмовими звітами, фотографіями, відеокліпами, електронними таблицями, електронною поштою, файлами обробки текстів і базами даних.

Додавання інформації до діаграми. Щоб представити інформацію, яка отримується, можна додати сутності та посилання до діаграми, а потім додати інформацію до елементів діаграми. Елементи можуть зберігати інформацію у властивостях, таких як ідентифікатор, дата й час, в атрибутах і на картках.

Робота з i2 Analyze. Якщо використовується i2 Analyst's Notebook Premium, можна підключитися до i2 Analyze і, залежно від розгортання, отримати доступ до розвідувальних даних в організації та із зовнішніх джерел.

Додавання даних з джерел даних. До діаграми можна додавати дані з таких джерел даних, як бази даних. Якщо є доступ до кількох джерел даних, то можна зіставити дані, які надає кожне джерело про цікавий елемент.

Виявлення та опрацювання дублікатів даних. Щоб переконатися, що якість аналізу не погіршується повторюваними даними, можна шукати сутності на поверхні діаграми, які можуть представляти той самий об’єкт реального світу. i2 Analyst's Notebook містить ряд інструментів, які допоможуть виявити та вирішити будь-яке дублювання без втрати критичних даних.

Макети аналітичних діаграм. Макети діаграм можуть виявити групи та шаблони в даних діаграми. На асоціативних діаграмах можна визначити тісно пов’язані сутності та групи взаємопов’язаних сутностей. На графіках шкали часу можна визначити групи подій, які відбулися близько одна до одної в часі.

Пошук інформації. Щоб знайти елементи діаграми, які можуть допомогти дослідження, можна знайти певну інформацію у властивостях елемента. Різні інструменти пошуку на вкладці «Аналіз» відповідають різним потребам.

Пошук мереж. Можна знайти зв’язки та посередників між цікавими об’єктами, дізнатися, що пов’язано з певною сутністю, а також знайти групи взаємопов’язаних сутностей. Ці мережі можуть містити сутності та зв’язки, які підтримують активність елементів, що представляють інтерес.

Виділення елементів діаграми. Щоб підкреслити вибрані об’єкти та зв’язки на діаграмі, можна скористатися функцією виділення.

Карта елементів діаграми. Щоб краще проаналізувати елементи за допомогою інформації про місцезнаходження, елементи діаграми можна візуалізувати на поверхнях карти.

Підтримка форматів координат. Координати вводяться у відповідному форматі для системи координат, яку використовує організація. Під час надсилання в Google Earth ці координати перетворюються на відповідні значення широти та довготи WGS84.

Перелічення вмісту діаграми. Перерахування елементів, карток і записів дозволяє сортувати, фільтрувати та копіювати інформацію, яку вони містять, до електронних таблиць або інших зовнішніх документів. Це дозволяє аналізувати дані, які не обов’язково видно на поверхні діаграми.

Статистичний перегляд даних діаграми. Можна переглядати розподіл даних, а також вибирати й фільтрувати дані на основі категорій і діапазонів даних. Перегляд розподілу та фільтрування допомагає визначити, наприклад, пік активності на діаграмі.

Робота з Time Wheel. Функція Time Wheel у i2 Analyst's Notebook — це надзвичайно наочний спосіб аналізу часових даних на діаграмі.

Дослідження активності елемента. Будь-які тимчасові дані, які зберігаються в елементі, можна описати як активність елемента. Можна дослідити цю інформацію, щоб виявити спільні теми чи розбіжності.

Умовне форматування. Можна використовувати умовне форматування, щоб змінити вигляд елементів на діаграмі, щоб підкреслити інформацію, яка буде цікавою для дослідження. Також можна змінити зовнішній вигляд як сутностей, так і посилань

на основі правила, які були визначені.

Аналіз соціальних мереж. Можна вивчити групові структури та комунікаційні потоки в межах мережевої діаграми, зосередившись на зв’язках, які існують між об’єктами. Цей тип аналізу називається аналізом соціальних мереж.

Зосередження на цікавих елементах. Щоб зосередити аналіз і візуалізацію на цікавих елементах, можна вибрати їх на поверхні діаграми, а потім видалити всі інші елементи з поля зору. Або, щоб зосередитися на виділенні пізніше, можна зберегти його в наборі виділення, а потім відкликати виділення, коли це буде потрібно.

Змінення зовнішнього вигляду елемента. Після додавання елемента на поверхню діаграми, можна змінити його зовнішній вигляд зі стилю за замовчуванням, указаного діаграмою. Також можна підкреслити елементи на поверхні діаграми та представити на ній лише найважливіші дані.

Розставлення елементів. Можна автоматично переміщувати елементи діаграми, щоб їхнє представлення відповідало даним і щоб елементи були рівномірно розташовані. Також можна покращити чіткість діаграми, наприклад, сформувавши зв’язки так, щоб вони не закривали інші елементи діаграми.

Підготовка схеми до публікації. Перш ніж представити або опублікувати діаграму, можна перевірити її на наявність орфографічних помилок і видалити записи даних. Щоб полегшити розуміння діаграми, можна додати легенду, яка є ключем до умов, які використовуються на діаграмі.

Презентація та публікація діаграми. Щоб ефективно представити дані на діаграмі, можна побудувати послідовність елементів діаграми для покрокового перегляду та збільшити масштаб кількох областей діаграми. Якщо потрібно опублікувати діаграму, то можна зберегти її у форматі, який підходить для одержувачів, а після чого її можна і роздрукувати.

Доступність. Функції доступності допомагають користувачам з обмеженими можливостями, такими як обмежена рухливість або обмежений зір, успішно використовувати продукти інформаційних технологій.

Налаштування i2 Analyst's Notebook. Можна налаштувати i2 Analyst's Notebook – налаштувати параметри програми, керувати файлами та плагінами, налаштувати комбінації клавіш і використовувати утиліти, такі як Series Import, щоб імпортувати більше одного файлу даних за раз [8].

Використання компаньйонного ПЗ i2. Існує ПЗ, яке доповнює і взаємодіє з i2 Analyst's Notebook.

Використання i2 Analyst's Notebook Connector for Esri. i2 Analyst's Notebook Connector for Esri додає геопросторовий аналіз до можливостей i2 Analyst's Notebook. Він повністю інтегрується з геопросторовими функціями ArcGIS Server, що означає, що можна буде проводити асоціаційний, часовий і геопросторовий аналіз в одному робочому середовищі.

Використання i2 Chart Reader. i2 Chart Reader забезпечує перегляд діаграм i2 Analyst's Notebook лише для читання. Діаграми можна розповсюджувати в електронному вигляді електронною поштою, диском або через інтернет/інтранет, а потім переглядати за допомогою i2 Chart Reader [9].

3.3. Розроблення рекомендацій щодо застосування технології застосування засобів багатовимірного візуального аналізу

Рекомендації щодо застосування технології застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook можуть суттєво підвищити ефективність досліджень і аналізу. Ось основні рекомендації:

1. **Комплексне навчання**. Переконайтеся в тому, що аналітики пройшли комплексне навчання з використання рішення i2 Analyst's Notebook. Таке навчання повинно охоплювати всі основні та розширені функції, а також найкращі практики багатовимірного візуального аналізу. Гарно підготовлені аналітики зможуть ефективніше користуватися цим рішенням під час розслідувань кіберінцидентів.

2. **Спільні семінари**. Проводьте спільні семінари для того, аби заохотити аналітиків ділитися думками, порадами і найкращими практиками з використання цього рішення. Створіть середовище для співпраці, в якому аналітики зможуть вчитися один в одного і разом покращувати свої навички з багатовимірного візуального аналізу.

3. **Встановлення стандартних операційних процедур**. Розробіть стандартизовані операційні процедури задля використання рішення i2 Analyst's Notebook під час розслідування кіберінцидентів. Вони мають охоплювати введення даних, створення діаграм, методології аналізу посилань та звітність. Послідовність у використанні рішення покращує якість та надійність аналізів.

4. **Налаштування для конкретних випадків застосування**. Заохочуйте аналітиків налаштовувати візуалізації у відповідності до конкретних вимог їхніх досліджень. Налаштовуйте діаграми і макети для розгляду унікальних аспектів різних справ, забезпечуючи, щоб i2 Analyst’s Notebook застосовувався таким чином, що був узгоджений із цілями розслідування кіберінциденту.

5. **Інтеграція із зовнішніми джерелами даних**. Закцентуйте увагу на значенні інтеграції зовнішніх джерел даних задля збагачення аналізу. Аналітики мають знати, яким чином підключати і включати відповідні дані з зовнішніх баз даних, розвідувальних даних із відкритим кодом і інших джерел, аби підвищити цінність своїх досліджень.

6. **Використання часового аналізу**. Виділіть можливості інструменту часового

аналізу. Мотивуйте аналітиків використовувати часові візуалізації для того, аби краще розуміти закономірності і тенденції із часом. Це представляє особливу цінність у тих розслідуваннях кіберінцидентів, в яких розуміння хронології подій має вирішальне значення.

7. **Регулярні заняття із підвищення кваліфікації**. Проводьте регулярні заняття із підвищення навичок для аналітиків для того, аби бути в курсі усіх нових функцій та можливостей рішення i2 Analyst's Notebook. Сфера багатовимірного візуального аналізу розвивається, і тому невпинне навчання гарантує те, що аналітики будуть використовувати найновіші інструменти і функції.

8. **Поінформованість щодо безпеки**. Закцентуйте увагу на важливості підтримки безпеки і конфіденційності під час використання i2 Analyst’s Notebook. Аналітики мають знати про конфіденційність даних, з якими вони взаємодіють, а також чітко дотримуватися заздалегідь визначених протоколів безпеки для того, аби максимально захистити секретну чи конфіденційну інформацію.

9. **Міжфункціональне співпраця**. Заохочуйте співпрацю між аналітиками й будь-якими іншими зацікавленими сторонами, як-от IT-фахівці, юридичні команди і експерти у галузі. Ефективна співпраця гарантує те, що засоби багатовимірного візуального аналізу будуть застосовуватися цілісно, враховуючи при цьому різні точки зору.

10. **Механізми зворотного зв'язку**. Встановіть механізми зворотного зв’язку, завдяки яким аналітики зможуть надавати інформацію щодо зручності використання та ефективність i2 Analyst’s Notebook. Регулярні відгуки стають у нагоді тоді, коли потрібно визначити сфери, що потребують вдосконалення, гарантуючи при цьому те, що рішення продовжує відповідати потребам слідчих груп, які регулярно змінюються.

11. **Розгляд масштабованості**. Заздалегідь плануйте масштабованість зі збільшенням обсягу даних та складності досліджень. Переконайтеся, що аналітики

знають, яким чином масштабувати свої візуалізації і аналізи задля ефективної обробки більших наборів даних.

12. **Будьте в курсі оновлень**. Регулярно перевіряйте наявність оновлень та нових версій i2 Analyst's Notebook. Залишайтеся в курсі нових функцій, вдосконалень та виправлень безпеки для того, аби продовжити забезпечувати нормальну роботу рішення.

Слідуючи цим рекомендаціям, організації матимуть змогу максимізувати переваги від використання засобів багатовимірного візуального аналізу на основі рішення i2 Analyst's Notebook, що в свою чергу покращить ефективність та результативність процесів розслідування кіберінцидентів.

ВИСНОВКИ

1. Проведено аналіз необхідності розслідування кіберінцидентів (яке полягає в тому, що розслідування інцидентів кібербезпеки – вкрай важливий процес для адекватного сприйняття масштабу, впливу і причин інциденту, а також визначення ефективних способів реагування), загроз корпоративним інформаційним системам (які включають в себе шкідливе ПЗ, фішингові атаки, внутрішні загрози, розподілені атаки на відмову в обслуговуванні, розширені стійкі загрози, атаки програм-вимагачів, невиправлене ПЗ і вразливості, атаки на ланцюги поставок, людський фактор, відсутність належної поінформованості щодо безпеки, загрози через мобільні пристрої, а також хмарні проблеми безпеки), а також технологій розслідування кіберінцидентів (які в тому числі включають в себе SIEM, EDR, IRP та SOAR).

2. Розглянуті архітектура (яка поділяється на логічну, фізичну, та архітектуру безпеки), призначення та функції (які складаються з сервісів для репозиторія аналізу, сервісів для з'єднувачів даних, служби адміністрування, сервісу сповіщень, служби пошуку каналів сповіщень, служби отримання сповіщень, служби аудиту, служби команд, служби адміністрування індексу, інформаційної служби, служби історії елементів, служби відновлення елементів, служби очищення, служби пошуку, сервісів з’єднувача даних, а також служби створення та дослідження підмножини зовнішніх даних), а також вимоги до розгортання (які залежать від операційних систем, програмного забезпечення, а також апаратного забезпечення) рішення i2 Analyst’s Notebook.

3. Розроблені варіант розгортання системи (а саме процес інсталяції рішення i2 Analyst’s Notebook) та технологія (яка складається з розуміння, використання, а також використання компаньйонного ПЗ i2, при чому використання ґрунтується на таких компонентах та функціях, як дані i2 Analyst’s Notebook, діаграми, додавання

інформації до діаграми, робота з i2 Analyze, додавання даних з джерел даних, виявлення та опрацювання дублікатів даних, макети аналітичних діаграм, пошук інформації, пошук мереж, виділення елементів діаграми, карта елементів діаграми, підтримка форматів координат, перелічення вмісту діаграми, статистичний перегляд даних діаграми, робота з Time Wheel, дослідження активності елемента, умовне форматування, аналіз соціальних мереж, зосередження на цікавих елементах, змінення зовнішнього вигляду елемента, розставлення елементів, підготовка схеми до публікації, презентація та публікація діаграми, доступність, а також налаштування i2 Analyst's Notebook) застосування засобів багатовимірного візуального аналізу на базі рішення i2 Analyst's Notebook, а також рекомендації щодо застосування технології застосування засобів багатовимірного візуального аналізу (які включають в себе комплексне навчання, спільні семінари, встановлення стандартних операційних процедур, налаштування для конкретних випадків застосування, інтеграцію із зовнішніми джерелами даних, використання часового аналізу, регулярні заняття із підвищення кваліфікації, поінформованість щодо безпеки, міжфункціональну співпрацю, механізми зворотного зв'язку, розгляд масштабованості, а також залишення в курсі оновлень).

ПЕРЕЛІК ПОСИЛАНЬ

1. Кіберінцидент URL: https://uk.wikipedia.org/wiki/Кіберінцидент (дата звернення: 10.12.2023).

2. 10 типичных ошибок при расследовании инцидентов URL: https://habr.com/ru/companies/pt/articles/685344/ (дата звернення: 10.12.2023)

3. Корпоративна інформаційна система URL: https://uk.wikipedia.org/wiki/Корпоративна_інформаційна_система (дата звернення: 10.12.2023)

4. IBM i2 Analyze Architecture and Services White Paper URL: https://www.ibm.com/support/pages/system/files/inline-files/platform_architecture_whitepaper_external_pdf.pdf (дата звернення: 10.12.2023)

5. Release notes - Analyst's Notebook 9.4.0 URL: https://docs.i2group.com/release-material/anb/9.4.0/i2-anb-9.4.0.html (дата звернення: 10.12.2023)

6. 1 - Getting Started with i2 Analyst's Notebook – Installation URL: https://www.youtube.com/watch?v=XPQrMuIxNcE (дата звернення: 10.12.2023)

7. Understanding i2 Analyst's Notebook URL: https://docs.i2group.com/anb/10.0.1/index.html (дата звернення: 10.12.2023)

8. Using i2 Analyst's Notebook URL: https://docs.i2group.com/anb/10.0.1/analysts_notebook_welcome.html (дата звернення: 10.12.2023)

9. Using companion i2 software URL: https://docs.i2group.com/anb/10.0.1/anb_using.html (дата звернення: 10.12.2023)

10. Enterprise resource planning URL:

https://en.wikipedia.org/wiki/Enterprise_resource_planning (дата звернення: 11.12.2023)

11. Customer relationship management URL: https://en.wikipedia.org/wiki/Customer_relationship_management (дата звернення: 11.12.2023)

12. Manufacturing execution system URL: https://en.wikipedia.org/wiki/Manufacturing_execution_system (дата звернення: 11.12.2023)

13. Warehouse management system URL: https://en.wikipedia.org/wiki/Warehouse_management_system (дата звернення: 11.12.2023)

14. Enterprise asset management URL: https://en.wikipedia.org/wiki/Enterprise_asset_management (дата звернення: 11.12.2023)

15. Analyst's Notebook URL: https://en.wikipedia.org/wiki/Analyst%27s_Notebook (дата звернення: 11.12.2023)