МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИКА ПРОГНОЗУВАННЯ ІНЦИДЕНТІВ У ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

_____ Альбіна АЛЕКСЕЄНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Альбіна АЛЕКСЕЄНКО
Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ
Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

1.

1. Кафедра Управління інформаційною та кібернетичною безпекою
2. Ступінь вищої освіти магістр
3. Спеціальність 125 Кібербезпека
4. Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Алексеєнко Альбіні Вікторівні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: " Методика прогнозування інцидентів у інформаційних системах військового призначення "

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *управління кібербезпекою, інформаційні системи, управління інцидентами*,

4. Перелік питань, які потрібно розробити:
   1. Здійснити аналіз наукової літератури та публікацій, пов'язаних із прогнозуванням інцидентів у інформаційних системах військового призначення.
   2. Дослідити сучасний стан управління інцидентами у інформаційних системах.
   3. Розробити методику прогнозування інцидентів у інформаційних системах військового призначення.
   4. Здійснити моніторинг та оцінку ефективності нової методики прогнозування інцидентів у інформаційних системах.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Аналіз інцидентів у інформаційних системах військового призначення	27.10.2023	
4.	Розроблення методики прогнозування інцидентів у інформаційних системах військового призначення.	10.11.2023	
5.	Визначення рекомендацій застосування розробленої методики	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	18.01.2024	

Здобувачка вищої освіти _____ Альбіна АЛЕКСЕЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Алексеєнко А.В.. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

Освітньо-професійної програми Управління інформаційною безпекою
(назва)

на тему: “ Методика прогнозування інцидентів у інформаційних системах військового призначення ”
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка **АЛЕКСЕЄНКО Альбіна** у кваліфікаційній роботі дослідила сучасний стан управління інцидентами інформаційної безпеки у системах військового призначення, що дало змогу зробити правильний висновок про необхідність застосування сучасних технологій при відпрацюванні нових підходів до розроблення способів і методів прогнозування інцидентів. Розроблена у роботі методика включає практичні рекомендації керівникам структурних підрозділів кібербезпеки, які орієнтовані на вдосконалення стратегій прогнозування інцидентів та підвищення рівня захисту в інформаційних системах. Розроблені критерії оцінки ефективності можуть слугувати інструментом практичного оцінювання заходів інформаційної безпеки в системах військового призначення.

На основі отриманих результатів розроблено конкретні рекомендації для практичного впровадження в області безпеки інформаційних систем. Рекомендації орієнтовані на вдосконалення стратегій прогнозування інцидентів та підвищення рівня захисту в інформаційних системах. Зокрема, важливо активно використовувати розроблені методики в системах моніторингу безпеки та забезпечити їхню взаємодію з існуючими інструментами управління ризиками. Однак, розвиток нових методик, які базуються на штучному інтелекті, квантових технологіях та кіберфізичній безпеці, може стати новими перспективними напрямками для поліпшення безпеки військових інформаційних систем.

АЛЕКСЕЄНКО Альбіна показала розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довела уміння самостійного застосування методів наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачки **АЛЕКСЕЄНКО Альбіни** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Алексеєнко А.В. допускається до захисту роботи в екзаменаційній комісії

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Алексеєнко Альбіни Вікторівни
на тему “ МЕТОДИКА ПРОГНОЗУВАННЯ ІНЦИДЕНТІВ У ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ ”

Актуальність

Сучасний стан інформаційної безпеки у інформаційних системах військового призначення у зв’язку з розв’язанням агресії проти України та посилення кібератак вимагає удосконалених заходів та наукових досліджень сучасних методів прогнозування інцидентів.

Позитивні сторони

Здійснений аналіз наукової літератури та публікацій, пов'язаних із прогнозуванням інцидентів у інформаційних системах військового призначення, визначив потребу у пошуку та відпрацюванні методики прогнозування з урахуванням досягнень у галузі інформаційних технологій На основі аналізу розроблена методика та конкретні рекомендації для практичного впровадження в області безпеки інформаційних систем військового призначення. Рекомендації орієнтовані на вдосконалення стратегій прогнозування інцидентів та підвищення рівня захисту в інформаційних системах.

Вказане дослідження слугує наріжним каменем для прийняття рішень керівним складом підрозділів кібербезпеки, формування політики та розвитку практик захисту інформації.

Недоліки

Недостатньо приділено уваги застосуванню штучного інтелекту при відпрацюванні методики прогнозування інцидентів. Однак, зазначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її авторка Алексеєнко Альбіна Вікторівна - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАЙДУР
підпис *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 65 стор., 16 рис., 52 джерела.

Метою роботи є розробка методики прогнозування інцидентів у інформаційних системах військового призначення для забезпечення їхньої безпеки та надійності.

Об'єктом дослідження є управління інцидентами в інформаційних системах.

Предмет дослідження – є методи прогнозування інцидентів у військових інформаційних системах.

Методи дослідження. Для вирішення завдань та процесів управління персоналом використовуються методи системного аналізу, теорії управління, Для моделювання об'єктів та суб'єктів кібербезпеки, їх характеристик та стратегій поведінки використовувалися методи соціальної психології.

Короткий зміст роботи. Робота спрямована на розробку методики прогнозування інцидентів у військових інформаційних системах з метою підвищення їхньої безпеки та надійності. Здійснений аналіз наукової літератури та публікацій, пов'язаних із прогнозуванням інцидентів у інформаційних системах військового призначення. Проведено дослідження сучасного стану управління інцидентами у інформаційних системах. Розроблена методика прогнозування інцидентів у інформаційних системах військового призначення. Визначені критерії оцінки ефективності нової методики прогнозування інцидентів у інформаційних системах.

Галузь застосування. Застосування методики прогнозування інцидентів у військових системах інформаційної безпеки забезпечить підвищення ефективності захисту інформації.

КЛЮЧОВІ СЛОВА: УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ, ІНФОРМАЦІЙНІ ЗАГРОЗИ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, ВІЙСЬКОВІ ІНФОРМАЦІЙНІ СИСТЕМИ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 65 pages, 16 figures, 52 sources.

The purpose of the work is to develop a methodology for predicting incidents in military information systems to ensure their safety and reliability.

The object of research is incident management in information systems.

The subject of research is methods of forecasting incidents in military information systems.

Research methods. Methods of system analysis, management theory are used to solve the tasks and processes of personnel management. The foundations of social psychology were used to model cyber security objects and subjects, their characteristics and behavioral strategies.

Brief content of the work. The work is aimed at developing a methodology for predicting incidents in military information systems in order to increase their security and reliability. An analysis of scientific literature and publications related to the forecasting of incidents in military information systems was carried out. A study of the current state of incident management in information systems was conducted. A methodology for forecasting incidents in military information systems has been developed. The criteria for evaluating the effectiveness of the new method of forecasting incidents in information systems have been determined.

Field of application. The application of incident forecasting techniques in military information security systems will ensure an increase in the effectiveness of information protection.

KEY WORDS: CYBER SECURITY MANAGEMENT, INFORMATION THREATS, INCIDENT MANAGEMENT, MILITARY INFORMATION SYSTEMS.

ЗМІСТ

ВСТУП 10

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ 13

1.1 Аналіз понять і теоретичних засад безпеки інформаційних систем 13

1.2 Методи прогнозування інцидентів 22

1.3 Особливості забезпечення безпеки у військових інформаційних системах 28

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ПРОГНОЗУВАННЯ ІНЦИДЕНТІВ 41

2.1 Вибір параметрів інцидентів 41

2.2 Розробка методики прогнозування інцидентів 46

РОЗДІЛ 3. ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ПРОГНОЗУВАННЯ 58

3.1 Валідація та тестування методики 58

3.2 Оцінка точності та надійності методики 63

РОЗДІЛ 4. РЕКОМЕНДАЦІЇ ПРАКТИЧНОГО ЗАСТОСУВАННЯ 65

4.1 Відпрацювання пропозицій для удосконалення рівня захисту інформації у військових системах 65

4.2 Практичні рекомендації керівникам структурних підроздлів 69

ВИСНОВКИ 73

ПЕРЕЛІК ПОСИЛАНЬ ..... **Ошибка! Закладка не определена.**

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 80

ВСТУП

У військовій сфері інформаційна безпека відіграє критичну роль у забезпеченні ефективності та функціонування різноманітних систем. Швидкість змін у цифровому середовищі та постійна загроза кібератак вимагають постійного розвитку та вдосконалення методів прогнозування інцидентів у військових інформаційних системах.

Важливо досліджувати та розробляти методики, які дозволяють виявляти потенційні загрози, ідентифікувати вразливості та передбачати можливі інциденти забезпеки. Це сприятиме зменшенню ризику атак, покращенню реагування та встановленню більш ефективних заходів захисту.

В цьому контексті важливо розглянути та проаналізувати різноманітні методи та інструменти прогнозування інцидентів, їхні переваги та обмеження, а також розробити ефективну методику прогнозування, яка б враховувала специфіку військових інформаційних систем.

Актуальність теми потребує детального розгляду сучасних тенденцій щодо інцидентів у інформаційних системах та розроблення методики їх прогнозування. Тому в даному дослідженні розглянуто сучасні тенденції в цій області та розроблена методика прогнозування інцидентів, яка враховує специфіку військових систем, з метою покращення їхньої безпеки та стійкості до можливих кіберзагроз.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки інформаційних систем військового призначення.

Об’єктом дослідження є процес управління інцидентами в інформаційних системах.

Предмет дослідження – є методики прогнозування інцидентів у військових інформаційних системах.

Метою роботи є розробка методики прогнозування інцидентів у інформаційних системах військового призначення для забезпечення їхньої безпеки та надійності.

Для досягнення цієї мети в роботі виконано наступні завдання:

1. Здійснений аналіз наукової літератури та публікацій, пов'язаних із прогнозуванням інцидентів у інформаційних системах військового призначення.

2. Проведено дослідження сучасного стану управління інциндентами у інформаційних системах.

3. Розроблена методика прогнозування інцидентів у інформаційних системах військового призначення.

4. Визначені критерії оцінки ефективності нової методики прогнозування інцидентів у інформаційних системах.

Методи дослідження. При вирішенні визначених наукових завдань в роботі при дослідженні способів планування використані аналіз, синтез, моделювання, кейс-стаді, як метод активного проблемно-ситуаційного аналізу при створенні методики прогнозування інцидентів у інформаційних системах, методи теорії управління: імперативний та диспозитивний - при формуванні рекомендацій для відпрацювання пропозицій.

Наукова новизна одержаних результатів.

1. В магістерській роботі вперше розроблена методика прогнозування інцидентів, яка враховує комплексність і динаміку сучасних загроз, і дозволяє забезпечити організації засобами для активного виявлення та ефективного реагування на потенційні інциденти.

Отримані результати вказують на те, що розроблена методика є перспективною у контексті покращення відповіді на інциденти і забезпечення високого рівня безпеки інформаційних систем.

2. Дістали подальшого розвитку способи визначення критеріїв оцінки точності та валідації методик прогнозування інцидентів в інформаційних системах.

Подальші вдосконалення та розширення методики можуть ще більше підвищити її ефективність у змінних умовах сучасного інформаційного середовища.

Практичне значення одержаних результатів. Отримані результати підтверджують ефективність розробленої методики прогнозування інцидентів, що робить її потенційно корисною для впровадження в реальні умови для підвищення рівня безпеки інформаційних систем.

Апробація результатів кваліфікаційної роботи. Результати дослідження було оприлюднено на Всеукраїнській науково-практичної Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (м. Київ, 23 лютого 2023 року), яка проведена в Навчально-науковому інституті захисту інформації ДУІКТ.

РОЗДІЛ 1

ТЕОРЕТИЧНІ АСПЕКТИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Аналіз понять і теоретичних засад безпеки інформаційних систем

Інформаційна безпека – це стан захищеності систем оброблення та зберігання даних, що гарантує конфіденційність, доступність і цілісність інформації, її використання та розвиток в інтересах громадян, або забезпечує захист персональної, соціальної та національної інформації від несанкціонованого доступу, використання, розкриття, знищення, зміни, перевірки, перевірки записів, руйнування. Це комплекс заходів, спрямованих на (у цьому сенсі частіше використовують термін "захист інформації") [1].

Інформаційна безпека держави характеризується ступенем захищеності від впливу небезпечної (дестабілізуючої, руйнівної, такої, що суперечить національним інтересам, тощо) інформації, як до її впровадження, так і до видалення, а отже, і стабільністю ключових сфер життєдіяльності (економічної, науково-технічної, управлінської, військової, інформаційно-просвітницької тощо) [2].

Концепція інформаційної безпеки не обмежується безпекою технічних інформаційних систем або інформації в числовому чи електронному вигляді, а стосується всіх аспектів захисту даних та інформації, незалежно від форми, в якій вони зберігаються.

Об'єктивно категорія "інформаційна безпека" виникла з появою інформаційного спілкування між людьми, з наявністю та розвитком інформаційної комунікації, що гарантує та налагоджує обмін інформацією між усіма елементами суспільства, при цьому люди та їхні спільноти мають інтереси, яким може бути завдано шкоди внаслідок впливу інформаційної комунікації. Це виникло в результаті визнання того факту, що розглядаючи

вплив ідеї інформаційної безпеки на зміни, можна виділити кілька етапів у розвитку інформації та комунікації [3]:

- перший етап (до 1816 року) характеризується стихійним використанням засобів інформації та комунікації. У цей період основним завданням інформаційної безпеки був захист інформації про події, факти, майно, місцезнаходження та інші дані, що мали життєво важливе значення для окремих людей і спільнот, до яких вони належали.

- другий етап пов'язаний із початком використання штучних технічних засобів телекомунікацій і бездротового зв'язку, що розпочалося 1816 року. Для забезпечення конфіденційності та завадостійкості радіозв'язку необхідно було використати досвід першого етапу інформаційної безпеки на вищому технічному рівні, а саме завадостійке кодування повідомлень (сигналів) і подальше декодування прийнятих повідомлень (сигналів).

- третій етап (починаючи з 1935 року) був пов'язаний з появою радіолокації та підводних акустичних засобів. Основним методом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, спрямованих на посилення захисту від впливу активних маскувальних і пасивних імітаційних електронних перешкод на приймальне радіолокаційне обладнання.

- четвертий етап (почався 1946 року) – винахід і практичне застосування електронних обчислювачів (ЕОМ). Проблеми інформаційної безпеки розв'язували здебільшого методами та засобами обмеження фізичного доступу до обладнання для отримання, оброблення та передавання інформації.

- п'ятий етап, починаючи з 1965 року, характеризується створенням і розвитком локальних інформаційно-комунікаційних мереж. Проблему інформаційної безпеки також розв'язували здебільшого способами і засобами фізичного захисту обладнання для збирання, оброблення та передавання інформації, інтегрованого в локальну мережу, шляхом управління і контролю

доступу до мережевих ресурсів.

- етап шостий (розпочався 1973 року) пов'язаний із використанням ультрамобільних комунікаційних пристроїв із широким спектром завдань. Загрози інформаційній безпеці стали серйознішими. Необхідно було розробити нові стандарти безпеки для забезпечення інформаційної безпеки комп'ютерних систем з бездротовими мережами передачі даних. З'явилися хакерські угруповання, які прагнуть завдати шкоди інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційні ресурси стали найважливішим ресурсом держави, а забезпечення їхньої безпеки – найважливішим і невід'ємним елементом національної безпеки. Інформаційне право формується як нова галузь міжнародної правової системи.

- етап сьомий (розпочатий 1985 року) пов'язаний зі створенням і розвитком глобальної інформаційно-комунікаційної мережі з використанням космічних засобів забезпечення. Можна припустити, що наступний етап розвитку інформаційної безпеки, найімовірніше, буде пов'язаний із поширенням надмобільних засобів зв'язку з широким спектром завдань і глобальним охопленням у просторі та часі, що забезпечується космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідно створити макросистему інформаційної безпеки людства під егідою великих міжнародних форумів.

З розвитком нових інформаційних технологій поняття інформаційної безпеки значно розширилося. Деякі експерти зазначають, що було б правильніше повністю замінити концепцію інформаційної безпеки концепцією кібербезпеки. Це пов'язано з тим, що сьогодні більше, ніж на втрату інформації, ми розраховуємо на захист процесів, інформації та діяльності в кіберпросторі. Іншими словами, втрата інформації супроводжується безліччю інших складних ускладнень.

Кібербезпека – це захист від вірусів, хакерських атак і шахрайства з даними. Віруси, наприклад, можуть не тільки видалити або вкрасти дані, а й

вплинути на роботу і продуктивність співробітників або навіть зупинити виробництво. Інформація також може бути використана не за призначенням як проти окремих осіб, так і проти організацій. Сьогодні за кібербезпеку відповідають три елементи: системи, процеси та люди. Ба більше, з огляду на повсюдну інтеграцію цифрових технологій у життя і тіло людини, питання інформаційної безпеки іноді стають питаннями безпеки життя. Таким чином, стара концепція інформаційної безпеки не може розв'язати різноманітні проблеми, що виникають у кіберпросторі в XXI столітті. Навпаки, інформаційна безпека еволюціонувала до такої міри, що стала частиною кібербезпеки [4].

Наведені нижче терміни можуть мати різне тлумачення в різних авторів і в різних контекстах.

Термін "інформаційні технології" (IT) охоплює широкий спектр дисциплін і видів діяльності та відноситься до технічних засобів оброблення і передавання даних (або інформації).

В англійській мові термін IT-безпека має два значення. Концепція функціональної безпеки означає, що система коректно і повністю реалізує лише ті цілі, які відповідають намірам її власника [5], тобто функціонує відповідно до існуючих вимог. Саме поняття інформаційної безпеки відноситься до безпеки процесу обробки технічної інформації та є характеристикою функціонально безпечної системи. Такі системи мають запобігати несанкціонованому доступу до даних і запобігати їхній втраті в разі збою.

Під інформаційною безпекою зазвичай розуміють комплекс заходів, спрямованих на зниження кількості потенційно небезпечних сценаріїв і розміру збитків, яких може зазнати компанія в разі витоку конфіденційної інформації. З цього погляду інформаційна безпека - це економічний параметр, який необхідно враховувати в діяльності компанії, де інформацію (або дані) можна розглядати як особливий товар або цінність, що підлягає захисту, і тому має бути доступною лише для авторизованих користувачів або програм.

Інформаційна безпека – це підтримання конфіденційності, цілісності та доступності інформації, на додаток до інших характеристик, таких як автентичність, відстежуваність, безвідмовність і надійність [6].

Інформаційні системи можна розділити на три частини - програмну, апаратну та комунікаційну – для цілеспрямованого застосування стандартів інформаційної безпеки (як механізмів захисту та запобігання). Самі механізми захисту реалізуються на трьох рівнях або ієрархіях: фізичному, персональному та організаційному. По суті, впровадження політик і процедур безпеки спрямоване на надання менеджерам, користувачам і операторам інформації про те, як правильно використовувати готові рішення щодо забезпечення безпеки.[7]

Інформаційна безпека за сферами застосування

Державна інформаційна безпека - це стан захищеності життєво важливих інтересів особи, суспільства і держави, запобігання шкоді від неповноти, своєчасності та недостовірності використовуваної інформації, негативного впливу інформації, негативних наслідків використання інформаційних технологій, несанкціонованого розповсюдження, використання або порушення цілісності, конфіденційності та доступності інформації (рис.1.1).

Рис. 1.1. Складові національної та міжнародної безпеки

Інформаційна безпека організації – це цілеспрямована діяльність організації та її співробітників, які використовують уповноважені сили і засоби, щодо досягнення такого стану захищеності інформаційного середовища організації, який гарантує нормальне функціонування і динамічний розвиток організації. Часто її здійснюють служби інформаційної безпеки.

Під інформаційною безпекою особистості розуміють стан захищеності цієї особистості, різних соціальних груп та об'єднань людей від впливів, що змінюють психічний стан або психологічні характеристики особистості проти її волі чи бажання, модифікують її поведінку або обмежують свободу вибору [8].

Характеристики інформації

Модель CIA (рис. 1.2) часто використовують для характеристики основних характеристик інформації як об'єкта захисту [9-12]:

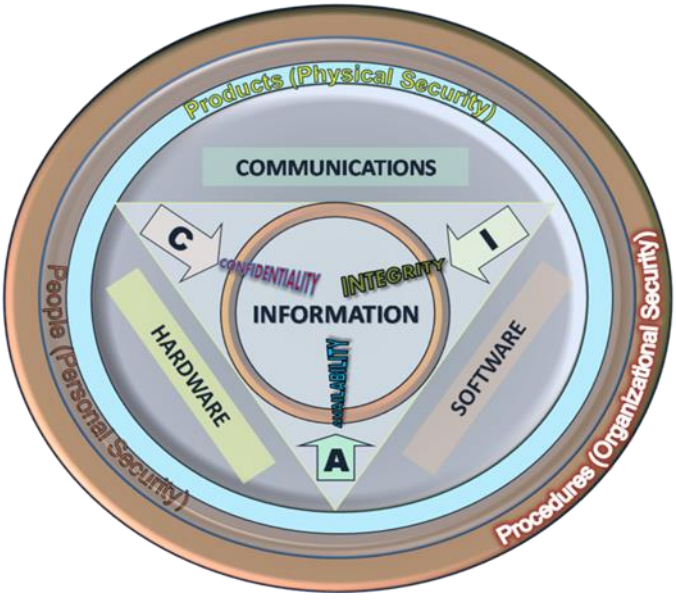

Рис. 1.2. Модель CIA

- Конфіденційність (англ. *confidentiality*) (C, рис. 1.2) – це характеристика інформації, яка означає, що інформація недоступна для

неавторизованих користувачів. Під конфіденційністю розуміють стан, при якому інформація повинна бути захищена від несанкціонованого доступу, використання та розголошення. Конфіденційність даних означає, що дані мають бути доступні лише тим, хто має авторизований доступ.

- Цілісність (англ. *integrity*) – означає, що інформація не може бути змінена неавторизованими користувачами. Цілісність (I, рис.1.2) означає, що інформація повинна бути захищена від несанкціонованого змінення і повинна бути цілісною, повною і точною. Наприклад, в дослідженнях [14-17] виявлені класифікаційні характеристики інформаційних ресурсів та взаємозв'язки між досконалістю системи управління та інформаційною системою і окреслено зовнішні та внутрішні інформаційні ресурси, цілісність яких потрібно захищати. Щоб забезпечити цілісність даних, організації можуть підтримувати та оптимізувати свою IT-інфраструктуру, створювати резервні копії даних і створювати план запобігання втраті даних, який захистить їх у разі серйозного витоку даних.

- Доступність (англ. *availability*) – можливість авторизованих користувачів отримати необхідну їм інформацію в потрібний момент за наявності відповідних повноважень. Доступність (A, рис. 1.2) означає, що інформація повинна бути доступна для користувачів, які мають на це право. Це означає, що мережа, система та необхідні пристрої готові до використання за призначенням уповноваженого персоналу [18-19]. По суті, доступність даних означає здатність співробітників отримати доступ до потрібних їм даних у будь-який момент без затримок. Є кілька факторів, які можуть перешкоджати доступу до даних навіть авторизованим користувачам, особливо в епоху хмарних технологій, коли так багато даних розміщується за межами офісу. Кібератаки, витоки даних і навіть нехтування стеками IT-технологій можуть призвести до затримок у доступі до даних або, що ще гірше, до простоїв у неробочому стані. Надаючи пріоритет інформаційній безпеці як ключовому аспекту стратегії кібербезпеки, підприємство може значно покращити досвід

співробітників і загальну безпеку вашої мережі.

Інформаційна безпека організації має кілька принципів, які визначені в дослідженнях [20-24]. Основні з них включають універсальність, надійність, постійність, модернізованість та комплексність (рис. 1.3).

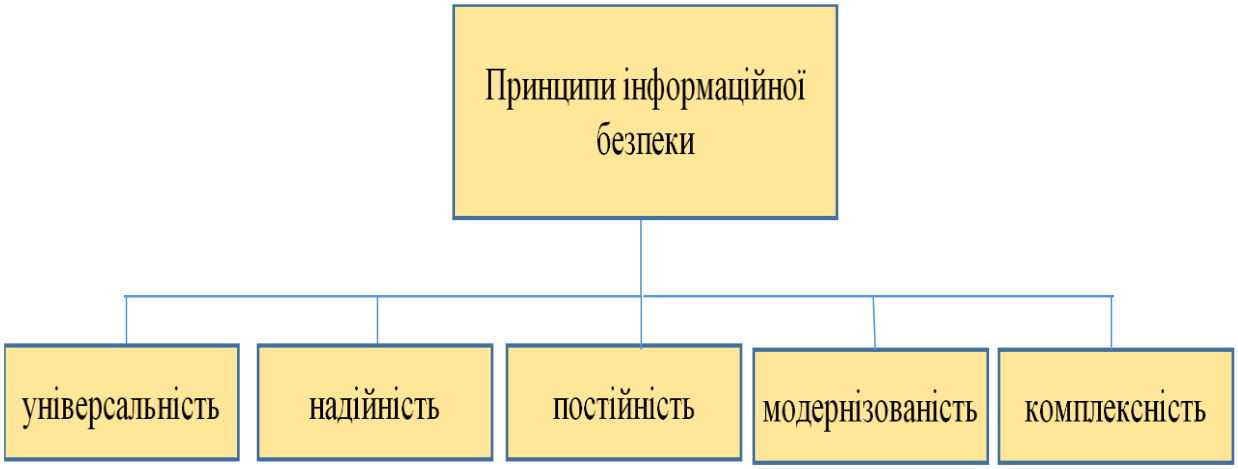

Рис. 1.3 Принципи інформаційної безпеки організації

Неможливо побудувати систему, захисні функції якої неможливо було б зламати, тому основним принципом є створення таких механізмів захисту, вартість зламу яких перевищує вартість отриманої інформації [9]. Тому необхідно впроваджувати захисне програмне забезпечення, яке вбудовується в програмне забезпечення системи і необхідне для виконання функції захисту. На думку експерта з кібербезпеки Дмитра Ганжело: "Усунення наслідків кібератаки часто обходиться в кілька разів дорожче, ніж їх запобігання. У сучасних умовах неможливо забезпечити стабільний економічний розвиток як окремих компаній, так і держав без забезпечення адекватного захисту інформації" [10].

Забезпечення національної інформаційної безпеки

Згідно з українським законодавством [7], проблему інформаційної безпеки слід розв'язувати в такі способи:

- забезпечення повноцінного функціонування інформаційної інфраструктури держави та захист її критичних елементів;
- виявлення, оцінка та прогнозування загроз інформаційній безпеці; підвищення рівня координації діяльності державних органів щодо запобігання таким загрозам та забезпечення усунення їх наслідків; здійснення міжнародного співробітництва з цих питань;
- удосконалення нормативно-правової бази в галузі інформаційної безпеки, включно із захистом інформаційних ресурсів, протидією кіберзлочинності, захистом персональних даних та правозастосуванням в інформаційній сфері;
- розгортання і розвиток національної системи засекреченого зв'язку як сучасної захищеної комунікаційної інфраструктури, здатної інтегрувати територіально розподілені інформаційні системи, що обробляють конфіденційну інформацію [10] .

Забезпечення безпеки підприємств та організацій

В Україні ІБ забезпечується захистом інформації, де необхідність захисту інформації визначається законодавством у сфері захисту інформації. Для реалізації захисту інформації створюється комплексна система захисту інформації (КСЗІ).

Як альтернативу суб'єкт захисту інформації припускає розроблення та впровадження політики інформаційної безпеки, яка може бути реалізована без порушення вимог законодавства.

Функцій забезпечення ІБ підприємств:

- розробка методів аналізу загроз, оцінки рівня інформаційної безпеки підприємства і систем її забезпечення;
- організація і здійснення діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;

- аудит і контроль функціонування системи інформаційної безпеки підприємства.

Методи забезпечення ІБ підприємств

- резервне копіювання;
- політика прав доступу (обмеження кола людей, які мають права доступу до важливих даних підприємства);
- двофакторна аутентифікація.

Органи (підрозділи) забезпечення ІБ

- відділи спецслужб держави;
- державні органи;
- спеціально уповноважений орган держави з питань захисту інформації (зараз в Україні – це Державна служба спеціального зв'язку та захисту інформації).

Підрозділи підприємства

В організації функцію забезпечення ІБ може виконувати як окремий відділ Служби безпеки підприємства, так і окрема Служба (Служба захисту інформації).

Для контролю за КСЗІ в обов'язковому порядку створюється Служба захисту інформації в інформаційно-телекомунікаційній системі.

Функції з контролю за СУІБ покладаються на певний відділ підприємства, зокрема на операційні центри безпеки.

1.2 Методи прогнозування інцидентів

Прогнозування інцидентів у сфері інформаційної безпеки - це процес

передбачення можливих загроз, вразливостей або атак на інформаційні системи, мережі чи дані. Це важлива складова управління безпекою, яка дозволяє попередити можливі проблеми та підготуватися до їх усунення або зменшення наслідків. Існує кілька кроків для прогнозування інцидентів у сфері інформаційної безпеки:

1. Аналіз історичних даних: Вивчення минулих інцидентів, їхніх причин, викликів та наслідків допомагає виявити закономірності та потенційні ризики.

2. Використання систем моніторингу та аналізу: Застосування спеціальних програмних засобів для виявлення підозрілих дій або вразливостей у мережах і системах.

3. Оцінка потенційних загроз: Аналіз сучасних тенденцій у кібербезпеці, включаючи нові види загроз та вразливості.

4. Розробка сценаріїв та планів дій: На основі прогнозів розробляються плани реагування на можливі інциденти, які включають кроки з усунення проблеми та відновлення роботи системи.

5. Навчання персоналу: Школи кібербезпеки для персоналу допомагають усвідомити загрози та прийняти заходи для запобігання інцидентам.

Ці методи дозволяють здійснювати більш об'єктивні передбачення щодо можливих ризиків та інцидентів у сфері інформаційної безпеки.[11, 12]

Прогнозування інцидентів у сфері інформаційної безпеки базується на декількох методах, що включають в себе (рис. 1.4).

1. Аналіз вразливостей: цей метод полягає у виявленні вразливостей в інформаційних системах та програмах. Шляхом аналізу цих вразливостей можна передбачити, які атаки можуть бути використані для їх використання.

2. Моніторинг і виявлення загроз: використання спеціальних систем моніторингу, які стежать за нещасними випадками або надзвичайними

ситуаціями, що можуть вказувати на можливий інцидент.

Рис. 1.4. Методи прогнозування вразливостей

3. Аналіз активності інцидентів: це включає в себе вивчення попередніх інцидентів, їхніх обставин, наслідків та причин. Аналізуючи минулі інциденти, можна виявити патерни та тенденції, які можуть допомогти прогнозувати майбутні.

4. Використання інтелектуальних систем: застосування штучного інтелекту та машинного навчання для аналізу великої кількості даних з метою виявлення аномалій, попередження можливих атак та інших інцидентів.

5. Експертні оцінки: залучення експертів у сфері кібербезпеки для оцінки ризиків та прогнозування можливих інцидентів на основі їх досвіду та знань.[12, 15]

Ці методи часто використовуються в поєднанні для більш точного прогнозування потенційних інцидентів у сфері інформаційної безпеки.

Прогнозування інцидентів у сфері інформаційної безпеки є складним завданням, і для цього використовуються різноманітні методи та інструменти. Ось кілька ключових методів та інструментів, які використовуються у цій сфері:

Детальніше про методи прогнозування:

1. Аналіз вразливостей: Виявлення та аналіз вразливостей у програмному забезпеченні, операційних системах та мережах для передбачення можливих шляхів атак.

2. Моніторинг поведінки: Системи моніторингу, які аналізують поведінку користувачів та систем, шукають аномальні дії, що можуть вказувати на потенційні загрози.

3. Прогностичні моделі на основі данних: Використання алгоритмів машинного навчання для аналізу великих обсягів даних та передбачення майбутніх інцидентів на основі попередніх патернів.

4. Аналіз інформаційних загроз: Вивчення та аналіз потенційних загроз безпеці для інформаційних систем з урахуванням сучасних тенденцій у кібербезпеці.

Інструментами прогнозування є:

1. SIEM (Security Information and Event Management): Платформи, які збирають, аналізують та інтерпретують дані з різних джерел для виявлення потенційних інцидентів безпеки.

2. IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Системи виявлення та запобігання вторгненням, які моніторять мережевий трафік на предмет підозрілих або шкідливих дій.

3. Аналітика поведінки користувачів: Інструменти, які аналізують

поведінку користувачів для виявлення аномальних дій або неавторизованого доступу.

4. Threat Intelligence Platforms: Платформи, які забезпечують доступ до інформації про потенційні загрози та нові види кібератак, що дозволяє передбачати можливі інциденти.

Ці інструменти та методи зазвичай використовуються в комплексі, дозволяючи організаціям отримувати більш повний прогноз можливих інцидентів у сфері інформаційної безпеки та готуватися до їхнього запобігання або вирішення.[13]

Різні методи та інструменти прогнозування інцидентів у сфері інформаційної безпеки мають свої переваги та обмеження, які варто враховувати при їхньому використанні:

Переваги:

1. Аналіз вразливостей:

- *Переваги:* Дозволяє виявити конкретні вразливості та шляхи потенційних атак.
- *Обмеження:* Може бути часо- та ресурсоємким, оскільки потребує систематичного оновлення та аналізу.

2. Моніторинг поведінки:

- *Переваги:* Виявляє аномальні патерни, які можуть вказувати на атаку або порушення безпеки.
- *Обмеження:* Може створити багато ложнопозитивів або потребує додаткового аналізу для підтвердження загроз.

3. Прогностичні моделі на основі даних:

- *Переваги:* Допомагають передбачати майбутні атаки на основі аналізу великої кількості історичних даних.
- *Обмеження:* Моделі можуть бути нестабільними через зміну умов

або нових типів загроз.

4. Аналіз інформаційних загроз:

- *Переваги:* Надає контекст для розуміння потенційних загроз та вразливостей у сучасному кіберпросторі.
- *Обмеження:* Інформація може бути неповною або застарілою, оскільки кіберзлочинці постійно розвивають нові методи.

Інструменти:

1. SIEM:

- *Переваги:* Централізоване управління та аналіз подій з різних джерел для виявлення загроз.
- *Обмеження:* Може генерувати великий обсяг ложнопозитивів, вимагає налаштування та підтримки.

2. IDS/IPS:

- *Переваги:* Виявлення та запобігання вторгнень у реальному часі.
- *Обмеження:* Може бути обмеженим у виявленні нових атак або тих, що використовують нові методи.

3. Аналітика поведінки користувачів:

- *Переваги:* Виявлення аномальної поведінки, що може вказувати на порушення безпеки.
- *Обмеження:* Вимагає точного налаштування для відокремлення звичайної поведінки від потенційних загроз.

4. Threat Intelligence Platforms:

- *Переваги:* Надає доступ до актуальної інформації про потенційні загрози.
- *Обмеження:* Може бути складним у використанні без адекватного аналізу та інтеграції з іншими системами.

Враховуючи ці переваги та обмеження, організації вибирають комбінацію методів та інструментів для більш ефективного прогнозування інцидентів у сфері інформаційної безпеки.

1.3 Особливості забезпечення безпеки у військових інформаційних системах

Прогнозування інцидентів у військових інформаційних системах є складним завданням, яке вимагає глибокого розуміння базової технології та потенційних загроз. Згідно з нещодавньою статтею Automatic Control and Computer Sciences, можна налаштувати традиційно визначені моделі прогнозування стрибків індикаторів шкоди від інцидентів інформаційної безпеки за умови виконання певних умов.

Дослідники повідомляють, що США Армія працює над системою, яка може швидко аналізувати величезні масиви даних для прогнозування дій противника та постійно оновлювати цей прогноз, коли супротивники змінюють свою тактику.

Україна, як і багато інших країн, має розвинуту систему військових інформаційних систем, які використовуються для різноманітних цілей, включаючи стратегічне планування, оперативне управління, збір та обробку інформації, а також забезпечення безпеки.

У статті [25] запропоновано модель максимізації інформаційної безпеки військових організацій, що впроваджується в середовище інформаційної війни. Вона намагається відповісти на три фундаментальні питання: що робити, чому і як? для захисту інформації та інформаційних систем від можливих інцидентів, пов'язаних з інформаційною безпекою, які можуть вплинути на конфіденційність, цілісність і доступність інформації. Визначено основні

змінні, що підлягають розгляду, та запропоновано їх можливі значення. Ці змінні отримують за допомогою інтерпретативного епістемологічного підходу, за допомогою огляду літератури, використання дослідницьких методів аналізу змісту, фокус-групи та методу загального морфологічного аналізу. Для комплексного реагування на три вищезазначені питання модель розглядає можливі інциденти інформаційної безпеки в інформаційних системах, беручи до уваги, перш за все, основні складові ризиків безпеки інформаційних систем, які збирають, зберігають, обробляють, передають і поширюють інформацію. Його діяльність керується військовими концепціями інформаційної війни, інформаційного забезпечення, найважливішими принципами війни, що застосовуються до оборонних операцій, та військовою доктриною інформаційних операцій. З огляду на тип проблеми, виявленої в дослідженні, орієнтуючись насамперед на аналіз сценаріїв інцидентів інформаційної безпеки та взаємозв'язок з плануванням і вибором засобів контролю безпеки, використовується метод загального морфологічного аналізу. Цей метод дозволяє прогнозувати можливі сценарії виникнення інцидентів, пов'язаних з інформаційною безпекою, на організаційному рівні, що призводить до вибору найбільш ефективного рішення засобів контролю безпеки, для максимального забезпечення безпеки інформації. Інформаційна безпека повинна гарантувати конфіденційність, цілісність і доступність інформації і прагне сприяти шляхом оперативної реалізації військової концепції інформаційного забезпечення досягненню інформаційної переваги.

Системи повідомлення про інциденти та аварії можуть бути використані для виявлення закономірностей поведінки операторів у причинах та пом'якшенні несприятливих подій. Однак найбільша увага в цій сфері зосереджена на цивільному процесі, охороні здоров'я та транспортній галузі. На противагу цьому, ця стаття зосереджується на питаннях людського фактору у звітуванні про військові інциденти. Ми виявляємо важливі відмінності як в інцидентах, про які повідомляють, так і у ставленні до людської «помилки». Наприклад, військові системи містять набагато більше невдач, пов'язаних з

навчанням, ніж можна було б очікувати в цивільних системах. Ці інциденти часто пов'язані з напругою між необхідністю підготовки персоналу до оперативних ситуацій і необхідністю контролювати небезпеки, які є необхідною частиною складних сценаріїв військових навчань. Подальші відмінності пов'язані з необхідністю для військовослужбовців проводити комплексну оцінку ризиків у невизначених умовах у суворо обмежені періоди часу. Наприклад, лідерам, можливо, доведеться вибирати між короткочасним впливом ситуації відносно високого ризику і тривалим впливом меншого ризику. Одним із наслідків цього є те, що військові системи звітності часто більше зосереджені на процесі прийняття рішень щодо ризиків, ніж на негайних діях, які призводять до несприятливої події. Також можна виявити сильну форму ретроспективного упередження, в якій люди можуть бути звинувачені незалежно від ризику, який вони приймають.

Згідно зі звітом Управління підзвітності уряду (GAO), Міністерство оборони (DOD) США зазнало понад 12 000 кіберінцидентів з 2015 року. Посилена увага необхідна для забезпечення належного повідомлення про кіберінциденти та їх поширення, зазначається у звіті. Міністерство оборони (MO) і оборонно-промислова база нашої країни (DIB), до якої входять організації за межами федерального уряду, які надають товари або послуги, критично важливі для задоволення військових потреб США, залежать від інформаційних систем для виконання своїх операцій. Ці системи продовжують бути об'єктом кібератак, оскільки з 12 року Міністерство оборони США пережило понад 12 000 2015 кіберінцидентів (Рис. 1.5). Для боротьби з цими інцидентами Міністерство оборони США розробило два процеси управління кіберінцидентами – один для всіх інцидентів і один для критичних інцидентів. Однак Міністерство оборони США не повністю реалізувало жоден із цих процесів.

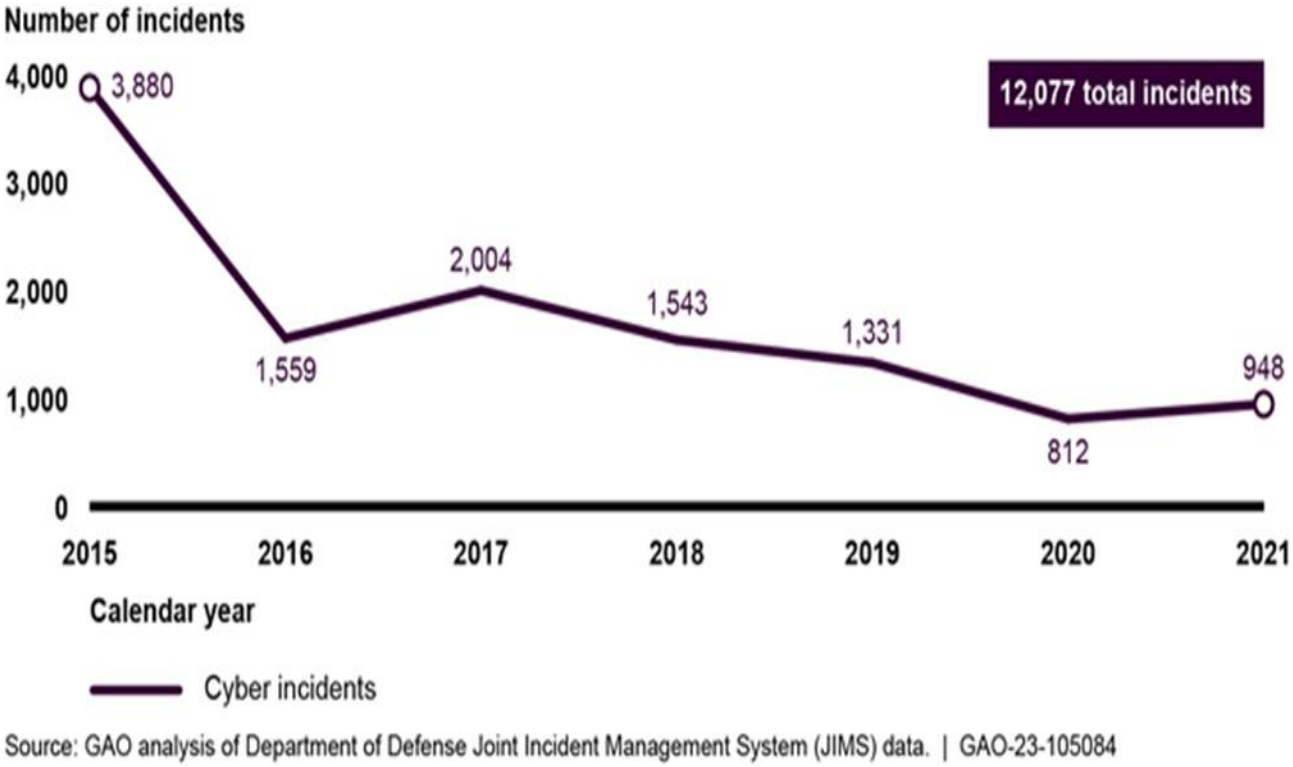

Рис. 1.5 Кіберінциденти, про які повідомляли постачальники послуг кібербезпеки Міністерства оборони США з 2015 по 2021 календарні роки

Незважаючи на зменшення кількості інцидентів завдяки зусиллям Міністерства оборони США, недоліки у повідомленні про ці інциденти залишаються. Наприклад, система повідомлення про всі інциденти Міністерства оборони США часто містила неповну інформацію, і Міністерство оборони не завжди могло продемонструвати, що вони повідомили відповідне керівництво про відповідні критичні інциденти. Слабкі місця в реалізації цих двох процесів пов'язані з тим, що Міністерство оборони США не призначило організацію, відповідальну за забезпечення належного повідомлення про інциденти та дотримання інструкцій, серед інших причин. До тих пір, поки Міністерство оборони не покладе на себе таку відповідальність, Міністерство оборони не має впевненості в тому, що його керівництво має точну картину стану кібербезпеки департаменту.

Крім того, Міністерство оборони ще не вирішило, чи слід повідомляти про кіберінциденти, виявлені постачальниками послуг кібербезпеки, всім

відповідним зацікавленим сторонам, за словами офіційних осіб. У керівництві Міністерства оборони США зазначено, що для захисту інтересів національної безпеки кіберінциденти повинні координуватися між організаціями Міністерства оборони та зовнішніми джерелами, такими як партнери DIB. До тих пір, поки Міністерство оборони США не вивчить, чи слід передавати цю інформацію всім відповідним сторонам, можуть бути втрачені можливості для виявлення системних загроз і усунення слабких місць системи.

Міністерство оборони США встановило процедуру визначення того, чи слід повідомляти осіб про порушення їхньої особистої інформації (PII). Цей процес включає в себе проведення оцінки ризиків, яка враховує три фактори – характер і чутливість особистої інформації, ймовірність доступу до неї та її використання, а також тип порушення. Однак Міністерство оборони США не послідовно документує повідомлення постраждалих осіб, оскільки офіційні особи заявили, що повідомлення часто робляться усно або електронною поштою, і жодних записів не зберігається. Без документування повідомлення Міністерство оборони США не може перевірити, чи були люди поінформовані про порушення.

У звіті також підкреслюється, що комп’ютерні системи DOD містять величезні обсяги конфіденційних даних, у тому числі контрольовану несекретну інформацію (CUI).), які можуть бути вразливими до кіберінцидентів.

Інформаційно-технологічні системи Міністерства оборони та DIB продовжують бути вразливими до кіберінцидентів, оскільки загрози кібербезпеці еволюціонують і стають все більш складними. Федеральні закони та вказівки Міністерства оборони США наголошують на важливості належного звітування та обміну інформацією про кіберінциденти, оскільки обидва є життєво важливими для виявлення слабких місць системи та підвищення безпеки систем.

Програма стратегічних технологій Центру стратегічних і міжнародних

досліджень (CSIS) веде хронологію значних кіберінцидентів з 2006 року. Хронологія фіксує кібератаки на державні установи, оборонні та високотехнологічні компанії або економічні злочини зі збитками понад мільйон доларів. Деякі з останніх інцидентів включають:

У листопаді 2023 року китайські хакери скомпрометували урядові мережі Філіппін за допомогою фішингових електронних листів для впровадження шкідливого коду в системи своїх цілей, щоб встановити командно-контрольний режим і шпигувати за діяльністю своїх цілей.

У серпні 2023 року китайські хакери атакували систему військових закупівель США для розвідки разом із кількома тайванськими організаціями. Зловмисники націлювалися на маршрутизатори з високою пропускною здатністю, щоб викрадати дані та створювати приховані проксі-мережі в цільових системах.

Квітень 2022. Хакери націлилися на український енергетичний об'єкт, але CERT-UA та допомога приватного сектору значною мірою запобігли спробам зупинити електричні підстанції в Україні. Дослідники вважають, що атака була здійснена тією ж групою, пов'язаною з російським ГРУ, яка була націлена на електромережу України в 2016 році, використовуючи оновлену форму того ж шкідливого програмного забезпечення.

Квітень 2022. Хакери націлилися на облікові записи українських урядовців у Telegram за допомогою фішингової атаки, намагаючись отримати доступ до облікових записів.

Червень 2022. Фішингова кампанія була націлена на американські організації у військовому секторі, програмному забезпеченні, ланцюжках поставок, охороні здоров'я та фармацевтиці, щоб скомпрометувати облікові записи Microsoft Office 365 і Outlook.

Вересень 2023 року: Російські кіберзлочинці отримали доступ до конфіденційної інформації Міністерства оборони Південної Африка,

включаючи військові контракти та інформацію про особовий склад. Департамент скасував свою попередню заяву, заперечуючи витік даних.

Вересень 2023 року: Російські хакери викрали тисячі документів з Міністерства оборони Великої Британії та завантажили їх у даркнет. Документи містили подробиці доступності ядерної бази в Шотландії, в'язниць суворого режиму та інші деталі національної безпеки. Хакери отримали документи, зламавши британського розробника огорож і отримавши бекдор-доступ до файлів міністерства.

Вересень 2023 року: Новий звіт Microsoft вказує на збільшення китайських кібероперацій у Південно-Китайському морі, а також на посилення атак на оборонно-промислову базу США та критично важливу інфраструктуру США. Підвищення відбувається на тлі зростання напруженості між Китаєм і США.

Вересень 2023 року: Російські війська в окупованому Криму повідомили про кібератаку на кримських інтернет-провайдерів. Атака сталася приблизно в той самий час, коли український ракетний удар був спрямований на російський військово-морський штаб у цьому районі.

Вересень 2023 року: Індійські хактивісти націлилися на військові та парламентські веб-сайти Канади за допомогою DDoS-атак, які сповільнили роботу системи на кілька годин. Хактивісти посилалися на публічне звинувачення прем'єр-міністра Канади Джастіна Трюдо на адресу Індії у вбивстві активіста за незалежність сикхів Хардіпа Сінгха Ніджара як мотивацію для злому.

Жовтень 2023 року: Хактивісти викрали 3 документів з НАТО, що стало другим випадком за три місяці, коли хактивісти зламали систему кібербезпеки НАТО. Хакери назвали себе "пухнастими хакерами-геями" і оголосили, що їхня атака була помстою за порушення прав людини країнами НАТО. У НАТО стверджують, що напад не вплинув на місії, операції чи військове розгортання сил НАТО.

Далеко не всі перераховані інциденти інформаційної безпеки у військовому секторі визначають необхідність детального розгляду та удосконалення структури військових інформаційних систем з метою їх захисту.

Структура військових інформаційних систем на рис.1.6.

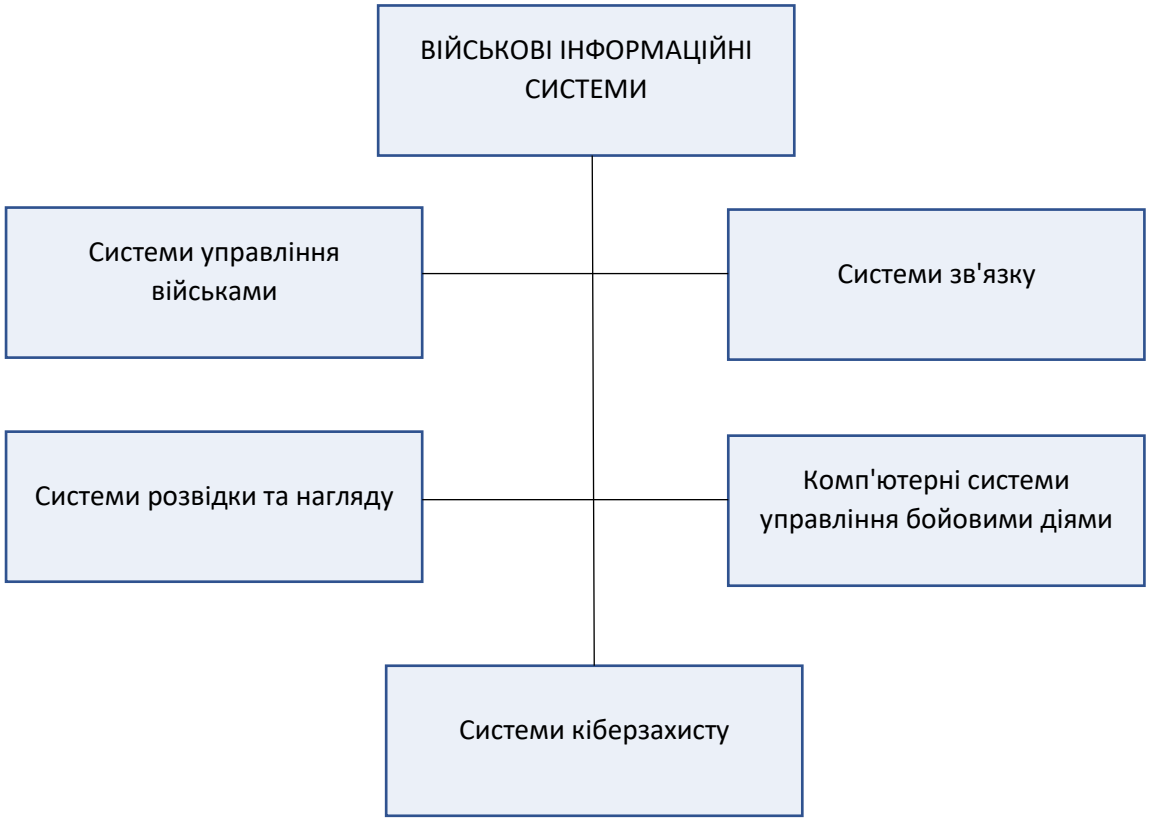

Рис. 1.6. Структура військових інформаційних систем

Основні аспекти військових інформаційних систем в Україні:

1. Системи управління військами: ці системи включають в себе програмне забезпечення та технічне обладнання, яке допомагає забезпечувати керівництво, планування та ведення військових операцій.

2. Системи зв'язку: це включає в себе широкий спектр засобів зв'язку - від радіо та супутникових зв'язків до систем кіберзахисту та шифрування.

3. Системи розвідки та нагляду: військові системи спостереження,

дрони, супутникові засоби та інші засоби для збору інформації про дії противника.

4. Комп'ютерні системи управління бойовими діями: інформаційні системи, які допомагають у веденні бойових операцій, управлінні вогнем, координації дій військ і тактичному прийнятті рішень.

5. Системи кіберзахисту: технології та системи, спрямовані на захист військових інформаційних систем від кібератак та забезпечення цілісності, конфіденційності та доступності даних.

Ці системи використовуються для покращення ефективності та безпеки військових операцій та забезпечення обороноздатності країни. З розвитком технологій вони постійно модернізуються та адаптуються до змін у загрозах та вимогах.[14]

Військові інформаційні системи мають свої особливості, оскільки вони призначені для специфічних потреб у сфері оборони та військових операцій. Особливості військових інформаційних систем наступні (рис.1.7):

1. Надійність та стійкість

- Стійкість до впливу: Військові системи повинні залишатися функціональними під час стрес-ситуацій, таких як кібератаки або фізичні пошкодження.
- Резервування та відновлення: Можливість швидкого відновлення роботи системи в разі відмови чи атаки.

2. Конфіденційність та безпека

- Криптографічний захист: Використання потужних шифрувальних методів для захисту конфіденційної інформації.
- Аутентифікація та авторизація: Суворі процедури перевірки особистості та доступу до системи для запобігання несанкціонованому використанню.

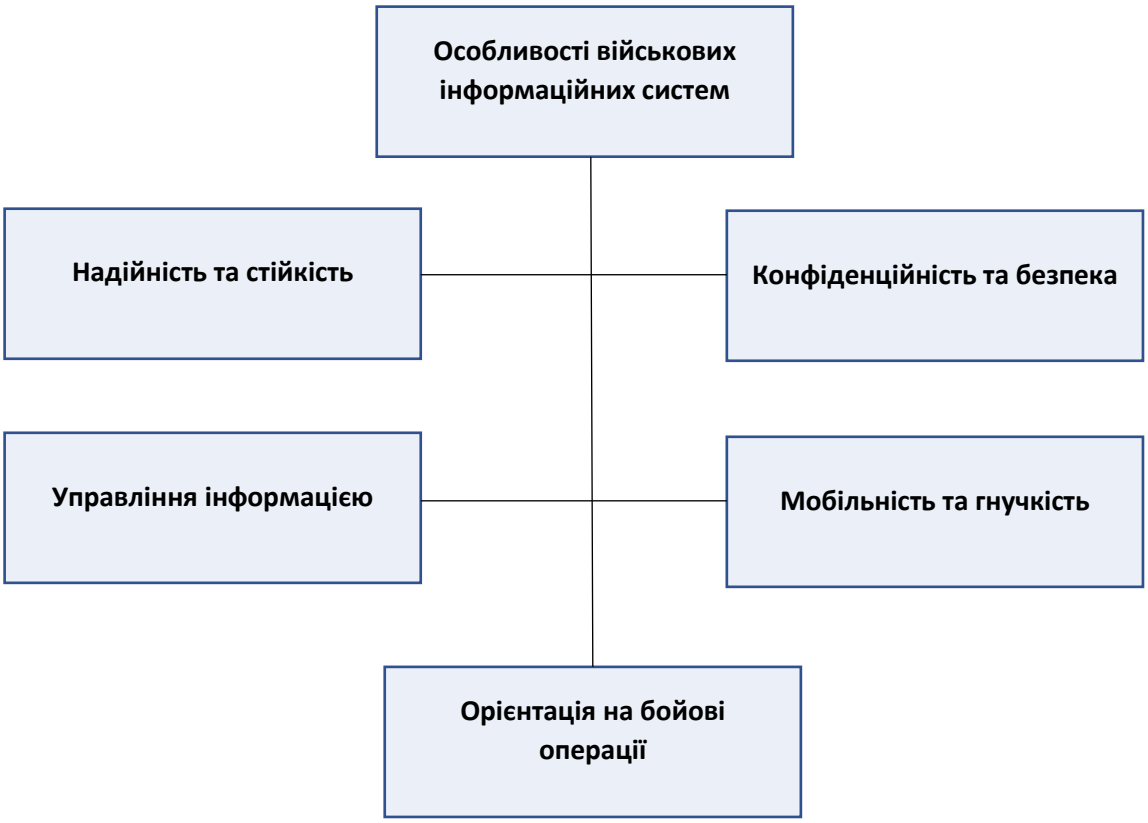

Рис.1.7. Особливості військових інформаційних систем

3. Управління інформацією

- Інтеграція даних: Здатність об'єднувати та аналізувати великі обсяги різноманітної інформації для прийняття важливих стратегічних рішень.
- Точність та актуальність: Забезпечення швидкого доступу до актуальної інформації для прийняття рішень в реальному часі.

4. Мобільність та гнучкість

- Мобільність даних: Здатність оперативно переносити та обробляти інформацію на різних театрах війни або місцевостях.
- Сумісність та інтеграція: Можливість спільно працювати з різними системами та платформами для забезпечення спільної діяльності.

5. Орієнтація на бойові операції

- Підтримка прийняття рішень: Забезпечення інформацією та

аналітикою для стратегічного та тактичного прийняття рішень.

- Керівництво бойовими діями: Системи управління, які дозволяють ефективно керувати бойовими операціями та ресурсами.

Ці особливості дозволяють військовим інформаційним системам ефективно функціонувати в умовах стресу, забезпечуючи важливість та безпеку даних для військових операцій та стратегічного планування [15].

Вимоги до безпеки та надійності військових інформаційних систем вкрай важливі через їхнє призначення у сфері оборони та військових операцій. Ось ключові вимоги до безпеки та надійності таких систем:

Безпека:

1. Конфіденційність:

- Вимагається захист від несанкціонованого доступу до конфіденційної інформації, що може бути важливою для національної безпеки.

2. Цілісність:

- Забезпечення захисту від несанкціонованих змін або втрати цілісності даних чи функціональності системи.

3. Доступність:

- Забезпечення доступності до системи та її функцій навіть у випадках намагань атаки або виникнення аварій.

4. Ідентифікація та аутентифікація:

- Ефективна система перевірки ідентичності та автентифікації користувачів, щоб уникнути несанкціонованого доступу.

5. Шифрування:

- Вимагається використання потужних шифрувальних методів для захисту інформації в транспортуванні та зберіганні.

Надійність:

1. Стійкість до впливу:

- Здатність системи залишатися функціональною під час стрес-ситуацій, таких як кібератаки або фізичні пошкодження.

2. Відновлення після відмов:

- Можливість швидкого відновлення роботи системи в разі відмови чи атаки.

3. Резервування та резервування даних:

- Здатність забезпечити резервні копії даних та систем для відновлення у разі втрати.

4. Управління виключеннями та помилками:

- Механізми для виявлення помилок та відновлення роботи від них.

5. Спротивлення злому:

- Використання заходів для запобігання несанкціонованому доступу та втручанню в систему.

Ці вимоги до безпеки та надійності враховуються при проектуванні, впровадженні та експлуатації військових інформаційних систем для забезпечення їхньої ефективності, захищеності та стійкості у важливих військових сценаріях та умовах.[15]

Висновок до розділу 1. У даному розділі магістерської роботи проведено глибокий аналіз теоретичних аспектів безпеки інформаційних систем, що включає розгляд понять і ключових теоретичних засад. Вивчено методи прогнозування інцидентів, які відіграють важливу роль у забезпеченні ефективної і розумної стратегії безпеки.

Особлива увага приділена військовим інформаційним системам, їх призначенню, особливостям і викликам, що стоять перед такими системами в контексті сучасних загроз і вимог безпеки. Результати цього дослідження

вказують на важливість розуміння контексту військових інформаційних систем для ефективного розвитку та застосування засобів захисту.

Аналізовані концепції інформаційної безпеки, представлені у цьому розділі, надають теоретичну базу для подальшого вивчення та розвитку в області безпеки інформаційних систем, а також вказують на актуальні проблеми і виклики, що виникають у сучасному інформаційному середовищі.

РОЗДІЛ 2
РОЗРОБКА МЕТОДИКИ ПРОГНОЗУВАННЯ ІНЦИДЕНТІВ

2.1 Вибір параметрів інцидентів

Розробка методики прогнозування інцидентів у сфері інформаційної безпеки включає кілька кроків, які спрямовані на створення системи аналізу та передбачення можливих загроз. Кроки, які можна включити до такої методики, які складають алгоритм самої методики:

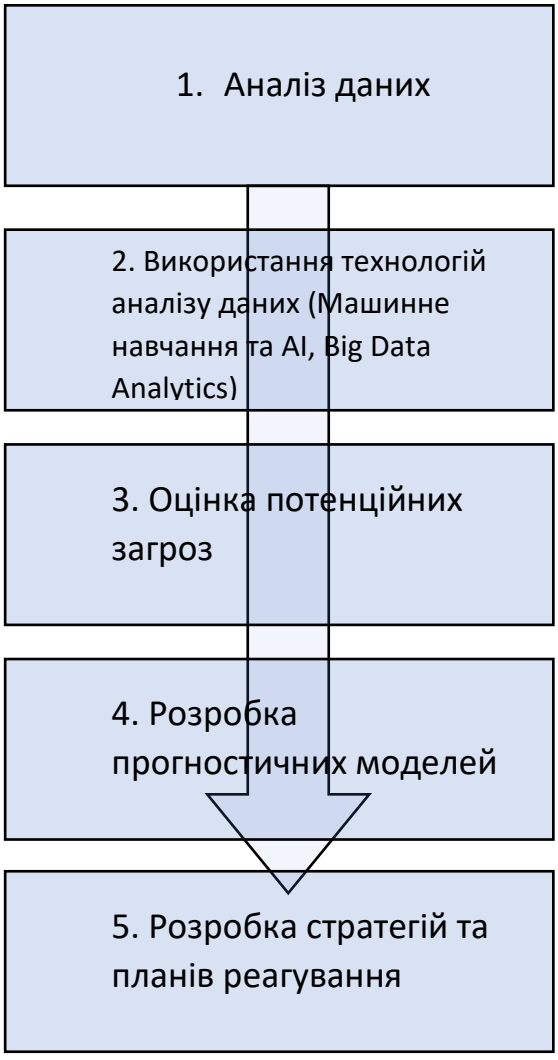

Рис.2.1. Алгоритм методики прогнозування інцидентів

1. Аналіз даних:

- Збір даних: Важливо використовувати дані про попередні інциденти та атаки, включаючи їхні обставини, наслідки та використані методи.
- Аналіз патернів: Виявлення патернів та тенденцій у минулих інцидентах для виявлення можливих сценаріїв майбутніх загроз.

2. Використання технологій аналізу даних:

- Машинне навчання та AI: Використання алгоритмів машинного навчання для аналізу великих обсягів даних та виявлення аномалій.
- Big Data Analytics: Використання технологій аналізу великих обсягів даних для виявлення тенденцій та кореляцій між різними параметрами.

3. Оцінка потенційних загроз:

- Створення сценаріїв загроз: Розробка різних сценаріїв можливих атак або інцидентів на основі аналізу даних.
- Оцінка ризиків: Визначення потенційних ризиків для системи з урахуванням різних сценаріїв загроз.

4. Розробка прогностичних моделей:

- Створення моделей прогнозування: Розробка моделей на основі аналізу даних та оцінки ризиків для передбачення можливих інцидентів.
- Перевірка та валідація моделей: Перевірка ефективності моделей на історичних даних та їхнє узгодження з реальними ситуаціями.

5. Розробка стратегій та планів реагування:

- Створення планів заходів: Розробка стратегій реагування та планів дій для випадків, коли прогнозований інцидент стає реальністю.
- Тестування та вдосконалення: Проведення симуляцій та тестувань планів реагування для їхнього вдосконалення та адаптації.

Ці кроки допомагають створити методику прогнозування інцидентів, яка базується на аналізі даних, моделях прогнозування та стратегіях реагування для ефективного управління потенційними загрозами у сфері інформаційної безпеки [17].

Параметри для прогнозування інцидентів у сфері інформаційної безпеки можна поділити на кілька категорій, які охоплюють різні аспекти технічних, поведінкових та контекстуальних чинників. Основні ключові параметри показані на рис. 2.2:

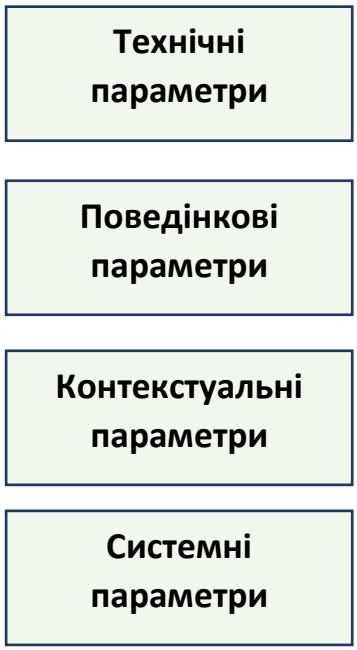

Рис. 2.2. Перелік параметрів для прогнозування інцидентів

1. Технічні параметри:

1. Вразливості системи: системні вразливості та потенційні місця для атаки, що можуть бути використані зловмисниками.

2. Логі файли та журнали подій: аналіз записів про активність для виявлення аномалій або підозрілих дій.

3. Інтенсивність трафіку: моніторинг обсягу та характеристик мережевого трафіку для виявлення аномалій.

4. Успішні та неуспішні входи: інформація про спроби входу в систему, які можуть вказувати на спроби несанкціонованого доступу.

2. Поведінкові параметри:

1. Аномальна активність користувачів: виявлення несподіваної чи нехарактерної активності у користувачів системи.

2. Зміни в звичайній поведінці: ідентифікація раптових змін у поведінці користувачів чи систем.

3. Стратегії атак: аналіз історичних даних про методи та стратегії попередніх атак.

3. Контекстуальні параметри:

1. Географічний контекст: Інформація про місце розташування користувачів або джерела трафіку.

2. Тренди та зміни в індустрії: Аналіз нових загроз та трендів у кібербезпеці.

3. Структура організації та доступи: Інформація про рівні доступу та права користувачів у системі.

4. Системні параметри:

1. Стан систем та ресурсів: Аналіз стану апаратних та програмних ресурсів системи.

2. Патерни навантаження: Виявлення несподіваних змін у навантаженні системи.

Ці параметри, коли використовуються разом або в комбінації, можуть надати цінну інформацію для прогнозування можливих інцидентів у сфері інформаційної безпеки. Комплексний аналіз цих параметрів дозволяє вчасно виявляти потенційні загрози та ефективно реагувати на них [16, 17] .

При класифікації інцидентів у сфері інформаційної безпеки важливо визначити критерії, які дозволять систематизувати та розподілити їх у відповідності до їхньої серйозності, типу та наслідків. Основних критерії для класифікації інцидентів показані на рис. 2.3:

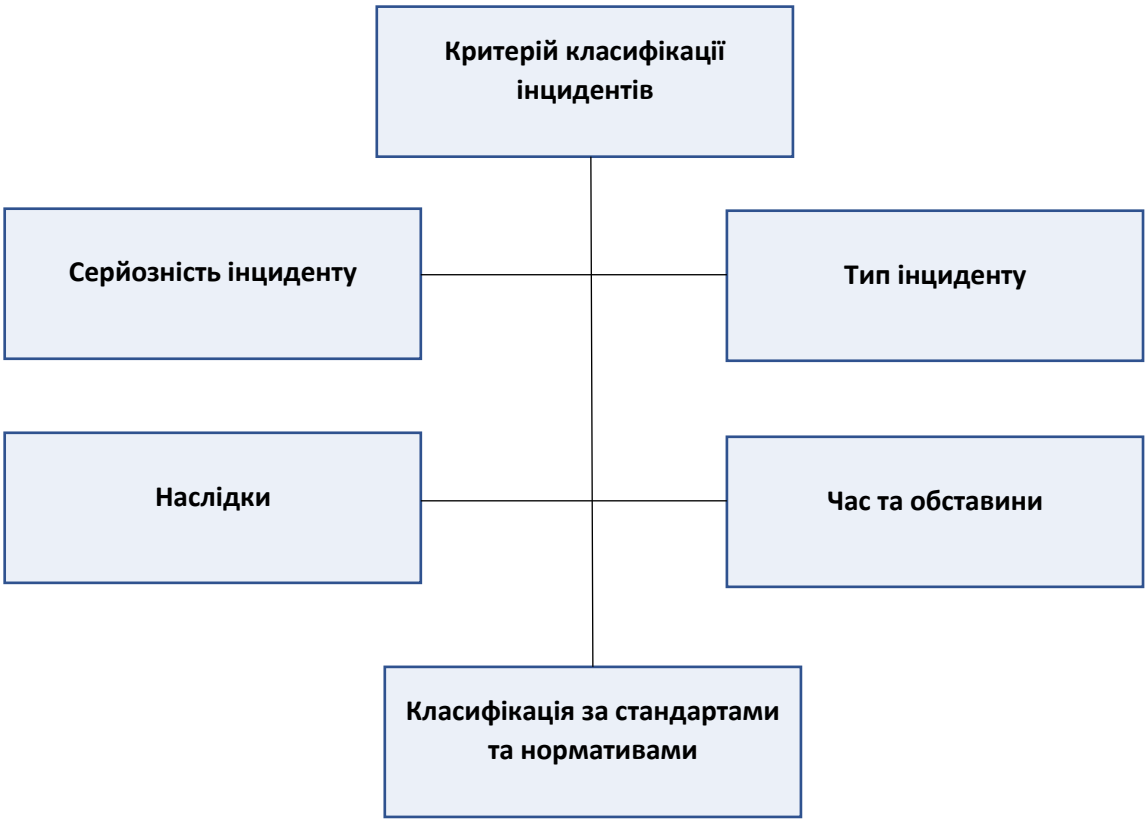

Рис. 2.3. Критерії класифікації інцидентів

1. Серйозність інциденту:

1) Критичність: Оцінка впливу на роботу системи чи організації. Чи загрожує цей інцидент безпеці системи чи користувачів?
2) Масштаб інциденту: Визначення обсягу систем, користувачів чи даних, які можуть бути пошкоджені або втрачені через інцидент.

2. Тип інциденту:

1) Категорія атаки: Наприклад, віруси, фішинг, DDoS атаки, витік інформації тощо.
2) Технічний аспект: Наприклад, атака на мережу, витік даних, вразливості програмного забезпечення тощо.

3. Наслідки:

1) Втрати: Оцінка фінансових, технічних чи репутаційних втрат через інцидент.

2) Час відновлення: Прогнозований час, необхідний для відновлення системи після інциденту.

4. Час та обставини:

1) Час виникнення: Момент виникнення інциденту та тривалість його дії.
2) Причина інциденту: Чи був інцидент результатом людської помилки, внутрішньої атаки чи зовнішньої загрози.

5. Класифікація за стандартами та нормативами:

1) Стандарти безпеки: Класифікація за визначеними стандартами, такими як NIST, ISO 27001 тощо.
2) Законодавча вимога: Чи є інцидент вимагається звітування чи відповідності до законодавства.

Ці критерії дозволяють систематизувати та оцінити інциденти у сфері інформаційної безпеки за різними аспектами, що допомагає приймати обгрунтовані рішення щодо заходів управління ризиками та реагування на інциденти.[18]

2.2 Розробка методики прогнозування інцидентів

Існують різні методи, які можна використовувати для прогнозування інцидентів. Деякі з поширених методів включають аналіз часових рядів, регресійний аналіз і алгоритми машинного навчання. Ці методи покладаються на статистичні моделі та історичні дані для прогнозування майбутніх подій.

Наприклад, регресійний аналіз – це статистичний підхід, який можна використовувати для прогнозування майбутніх значень на основі часового ряду спостережень деякої незалежної змінної. Цей підхід може бути використаний для виконання прогнозування з використанням загальноприйнятих галузевих статистичних засобів. Регресія намагається знайти «найкращу відповідну» пряму лінію між точками даних (нанесеними координатами X і Y на графіку),

щоб лінію можна було продовжити для визначення майбутніх точок на цьому графіку.

Регресійний аналіз може бути корисним для прогнозування інцидентів інформаційної безпеки, оскільки він дозволяє встановити залежність між різними факторами та інцидентами інформаційної безпеки.

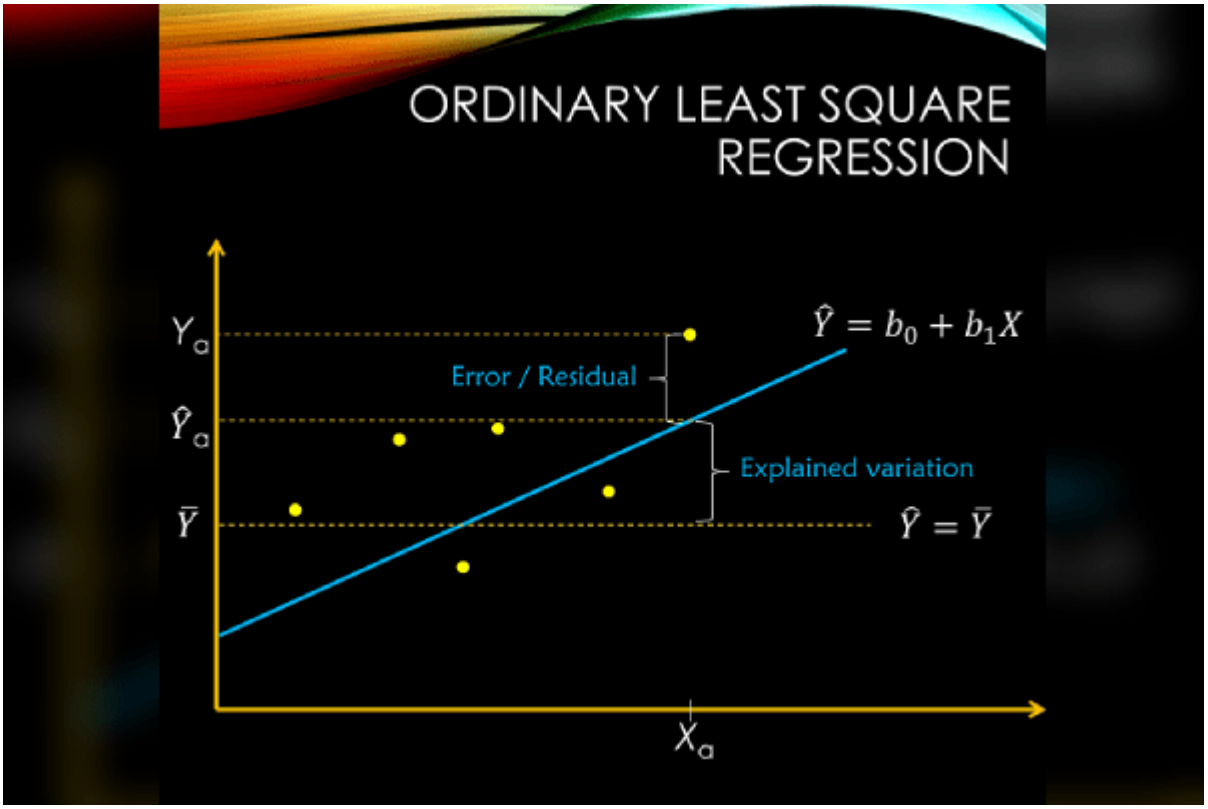

Рис. 2.4. Прогнозування кількості інцидентів за допомогою лінійної регресії

Регресійний аналіз є чудовим інструментом, оскільки він дозволяє нам вийти за рамки поточних зібраних даних. Для представлення регресійного аналізу ми використовуємо наступне рівняння

$$\hat{Y} = b_0 + b_1X$$

де X – незалежні змінні (результати інцидентів на конкретний термін);

b_0 , b_1- коефіцієнти регресії.

Наведене вище рівняння просто означає, що наша залежна змінна (Y) може бути передбачена моделлю, яка найкраще відповідає нашим даним, плюс

деяка похибка. Як правило, ми використовуємо лінійну модель в регресії. Тобто ми підсумовуємо наш набір даних прямою лінією. Модель у наведеному вище рівнянні замінюється нашими незалежними змінними або предикторами.

Пряма може бути визначена відрізком (b0) і за швидкістю зміни або нахилу (b1) між X і Y. Після того, як ми отримаємо відрізок і нахил, ми можемо підключити будь-яке значення X ($_{1,2,3...}$) і отримати відповідне значення для Y($_{1,2,3...}$). Пряма лінія, яка підсумовує дані, називається лінією регресії. Оскільки для прогнозування використовується регресійний аналіз, нам потрібна лінія, яка найкраще відповідає даним і мінімізує похибку прогнозування. Тобто, він повинен проходити через якомога більше точок даних або бути близьким до них, щоб це призводило до найменшої різниці між спостережуваною точкою даних і лінією. Проблема, однак, полягає в тому, що ми можемо знайти кілька рядків, що відповідають даним, що призводить до мінімальної похибки, коли ці помилки просто підсумовуються (позитивні та негативні помилки).

Засіб регресійного аналізу виконує лінійний аналіз регресії за допомогою методу "найменших квадратів", щоб припасувати лінію через набір спостережень. Ви можете проаналізувати, як на одну залежну змінну впливають значення однієї або кількох незалежних змінних. Наприклад, ви можете проаналізувати, як на швидкодію фахівця впливають такі фактори, як вік, висота та вага. Ви можете затверджувати акції в показниках продуктивності до кожного з цих трьох факторів, базуючись на наборі даних продуктивності, а потім використовувати результати для прогнозування продуктивності нового, незайнятого математика.

Крім лінійної регресії ще існують кілька варіантів прогнозування в табличному процесорі Excel (рис.2.5):

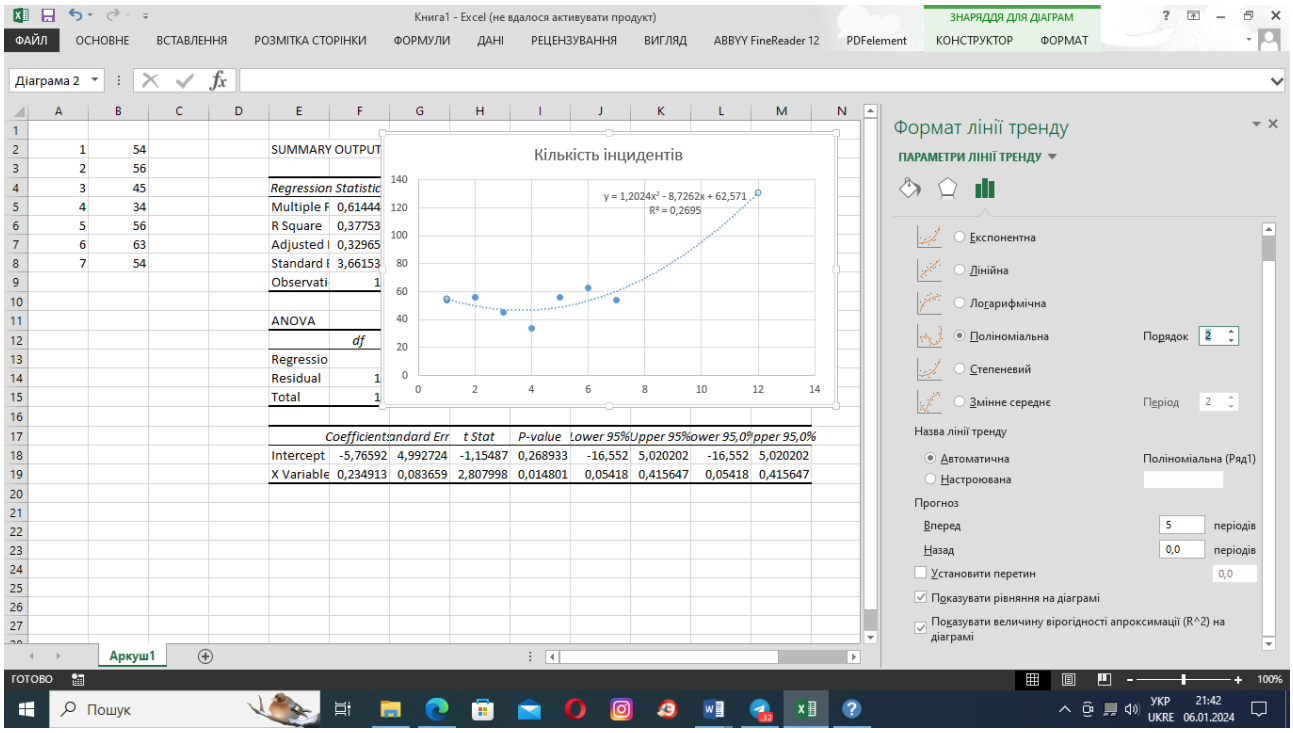

Рис.2.5. Приклад прогнозування кількості інцидентів на кінець року за допомогою поліноміальної регресії

За допомогою графіка функції регресії можна графічно спрогнозувати кількість інцидентів на конкретну дату (рис. 2.6)

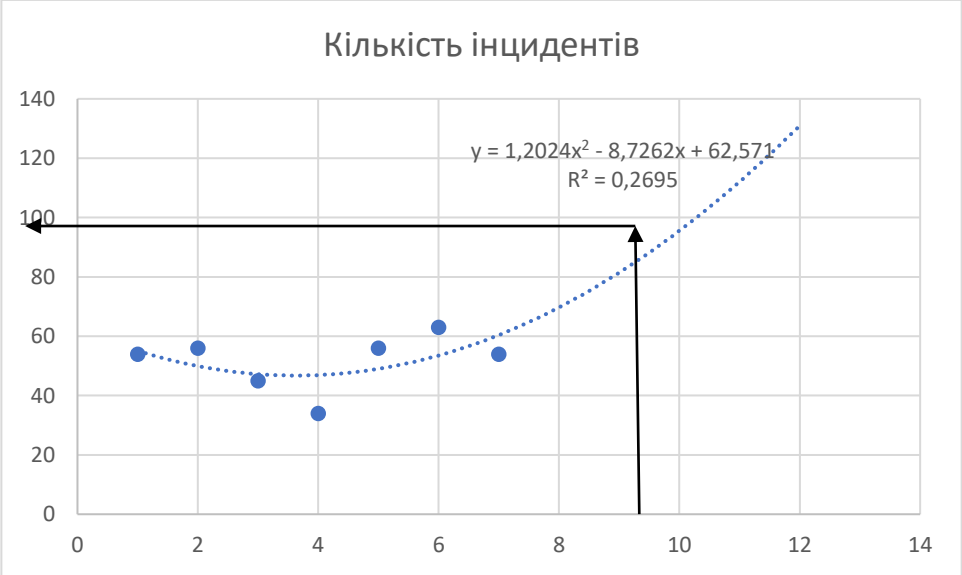

Рис.2.6. Графічне прогнозування результатів.

Крім графічного прогнозування можна використати функцію регресії з її коефіцієнтами, яка визначена на рис.2.6

$$y = 1{,}2024x^2 - 8{,}7262x + 62{,}571$$
$$R^2 = 0{,}2695$$

При цьому необхідно звернути увагу на можливість застосування кількох варіантів прогнозування (рис.2.5). Найкращий спосіб визначають за коефіцієнтом детермінації R^2, який тез визначається на діаграмі (рис.2.5, 2.6)

Перевіряємо валідність моделі за допомогою F-критерію. F-критерій - це статистика, яка говорить нам, чи може модель (наша незалежна змінна) краще передбачити змінну результату, ніж відсутність моделі взагалі. Значущий ($p<0{,}05$) F-критерій вказує на те, що наша незалежна змінна (або змінні в множинній регресії) краще прогнозує залежну змінну. Тобто, ваша лінія регресії відповідає даним краще, ніж відсутність незалежної змінної. Також ми можемо розрахувати R^2, що показує частку поліпшення за рахунок моделі. R^2 інтерпретується як частка дисперсії в Y, що пояснюється моделлю. У простій регресії, взявши квадратний корінь з цього значення, ми отримаємо коефіцієнт кореляції Пірсона r.

Іншим методом є аналіз часових рядів, який використовується для аналізу даних часових рядів і отримання з них значущих статистичних даних і характеристик. Цей метод корисний для прогнозування майбутніх цінностей на основі минулих тенденцій і моделей.

Нарешті, алгоритми машинного навчання можна використовувати для прогнозування інцидентів, навчаючи моделі на історичних даних і використовуючи їх для прогнозування майбутніх подій. Ці алгоритми можна використовувати для виявлення закономірностей і тенденцій у даних, які можуть бути не відразу очевидними для людини.

Важливо зазначити, що вибір методу залежить від типу доступних даних,

характеру прогнозованого інциденту та необхідної точності.

Раннє виявлення інцидентів безпеки та правильне прогнозування розвитку атаки є основою ефективного та своєчасного реагування на кіберзагрози. Розвиток атаки залежить від майбутніх кроків, доступних зловмисникам, їхніх цілей та мотивації, тобто «профілю» зловмисника, який визначає поведінку зловмисника в системі. Зазвичай «профіль зловмисника» – це набір атрибутів зловмисника – як внутрішніх, таких як мотиви та навички, так і зовнішніх, таких як наявна фінансова підтримка та інструменти, що використовуються. Визначення профілю зловмисника дозволяє визначити тип зловмисника та складність контрзаходів, а також може значно спростити процес атрибуції зловмисника при розслідуванні інцидентів безпеки. аналіз існуючих методів поведінки зловмисника, специфікацій профілю зловмисника є основою для прогнозування майбутніх кроків атаки. Проведений аналіз дозволяє окреслити основні переваги та обмеження підходів до прогнозування атак та побудови профілю зловмисника, існуючі виклики та перспективи у цій сфері. Потрібно визначити підхід, який конкретизує подальші етапи досліджень і є основою для розробки методики прогнозування поведінки зловмисника.

Розробка методики прогнозування в інформаційній безпеці вимагає кількох етапів, починаючи від збору даних і закінчуючи оцінкою результатів та постійним вдосконаленням процесу прогнозування. Загальні кроки, позначені на рис. 2.7.

1. Збір та підготовка даних:

- Вибір джерел даних: Визначення джерел, з яких будуть збиратися дані про інциденти, вразливості, логи подій, статистика попередніх атак тощо.
- Обробка даних: Очищення, структурування та підготовка даних для подальшого аналізу.

2. Аналіз та моделювання:

- Вибір методів аналізу: Використання статистичних аналізів,

машинного навчання, алгоритмів прогнозування тощо для виявлення патернів та тенденцій у даних.

- Розробка прогностичних моделей: Створення моделей на основі аналізу даних для передбачення майбутніх інцидентів.

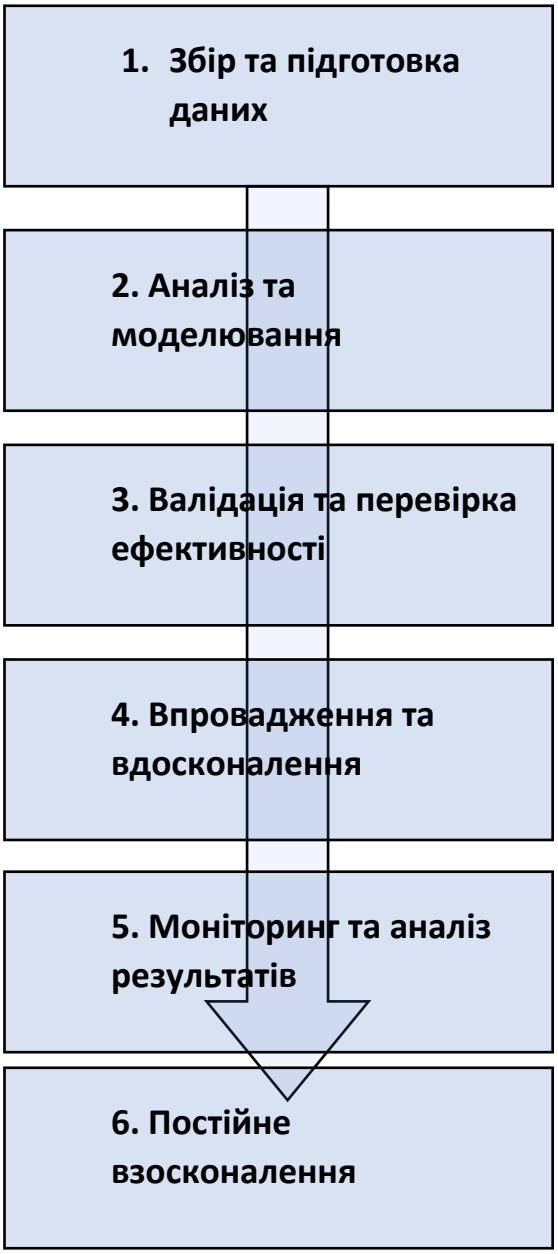

Рис. 2.7. Алгоритм методики прогнозування

3. Валідація та перевірка ефективності:

- Тестування моделей: Перевірка моделей на тестових даних для оцінки їхньої точності та ефективності.
- Оцінка результатів: Аналіз результатів прогнозування, виявлення помилок чи недоліків, визначення показників ефективності моделі.

4. Впровадження та вдосконалення:

- Впровадження моделі: Інтеграція розробленої методики в робочий процес безпеки, можливо, через систему моніторингу чи автоматизовану систему реагування.
- Постійне вдосконалення: Оновлення моделей на основі нових даних, врахування змін у загрозах та вразливостях.

5. Моніторинг та аналіз результатів:

- Слідкування за ефективністю: Постійний моніторинг роботи методики прогнозування та її точності.
- Звітність та аналіз: Аналіз отриманих результатів для виявлення закономірностей та вдосконалення методології.

Цей процес вимагає систематичного підходу, постійного оновлення та аналізу результатів для того, щоб забезпечити ефективне прогнозування інцидентів в сфері інформаційної безпеки [19-22] .

Розробка методики прогнозування інцидентів у сфері інформаційної безпеки – це комплексний процес, що включає в себе кілька етапів і стратегій. Загальний опис того, як можна розробити таку методику:

1. Збір та аналіз даних:

- Збір історичних даних
- Збір та систематизація інформації про минулі інциденти, включаючи їх тип, час, наслідки, використані методи та можливі вразливості

систем.

- Аналіз патернів
- Виявлення повторюваних патернів, тенденцій та кореляцій між різними інцидентами для створення бази для прогнозування майбутніх подій.

2. Використання аналітики даних

- Статистичний аналіз
- Використання статистичних методів для розуміння взаємозв'язків між різними змінними та подіями, що можуть привести до інцидентів.
- Моделювання та прогнозування
- Створення моделей на основі аналізу, які можуть передбачати можливі інциденти на основі отриманих даних.

3. Використання технологій аналізу даних

- Машинне навчання та штучний інтелект
- Використання алгоритмів машинного навчання для автоматизованого аналізу та прогнозування на основі виявлених патернів та залежностей.
- Великі дані
- Використання технологій аналізу великих обсягів даних для виявлення складних залежностей та тенденцій.

4. Розробка стратегій та планів реагування

- Створення планів дій
- Розробка стратегій та планів дій для випадків, коли прогнозований інцидент стає реальністю.
- Тестування та вдосконалення
- Проведення симуляцій та тестувань планів реагування для їхнього

вдосконалення та адаптації до різних сценаріїв.

5. Оновлення та адаптація методики

- Континуальне оновлення методики на основі нових даних, технологій та вдосконалення стратегій реагування.

Цей процес дозволяє створити систему, яка базується на аналізі даних, моделях прогнозування та стратегіях реагування для ефективного управління потенційними загрозами у сфері інформаційної безпеки.

Розробка методики прогнозування інцидентів у військових системах інформаційної безпеки вимагає специфічного підходу, оскільки вони мають особливості, пов'язані з високою конфіденційністю та важливістю інформації. Ось деякі кроки, які можна врахувати [23-24]:

Крок 1: Розуміння особливостей військових систем.

1) Аналіз потенційних загроз: Ретельний огляд типових загроз, які можуть вплинути на військові інформаційні системи.
2) Ідентифікація вразливостей: Виявлення слабких місць у системах, що можуть бути використані для атак.

Крок 2: Збір даних та ресурсів.

1) Збір військових даних: Отримання історичних даних про атаки, інциденти, логи подій в рамках військових мереж і систем.
2) Використання конфіденційних джерел: Робота з класифікованою інформацією для врахування найбільш критичних аспектів безпеки.

Крок 3: Аналіз та моделювання.

1) Статистичний аналіз: Використання статистичних методів для виявлення патернів інцидентів та аномалій.
2) Моделювання за допомогою класифікаційних алгоритмів: Використання методів машинного навчання для прогнозування можливих атак на основі

історичних даних.

Крок 4: Розробка стратегій та заходів.

1) Створення планів заходів: Розробка стратегій реагування на конкретні типи інцидентів у військових системах.

2) Симуляції та тестування: Проведення симуляційних вправ для перевірки ефективності планів реагування.

Крок 5: Оновлення та адаптація

1) Оновлення на основі нових загроз: Постійне оновлення методики на основі нових даних про загрози та інциденти.

2) Підвищення кваліфікації персоналу: Постійне навчання та оновлення знань персоналу для відповіді на нові виклики.

Цей алгоритм надає загальну структуру для розробки методики прогнозування інцидентів у військових системах. Оскільки військові системи мають високу ступінь конфіденційності та важливості, важливо враховувати ці особливості при розробці та застосуванні методики.[25-30]

Висновки до розділу 2. У даному розділі магістерської роботи була виконана значуща робота з розробки методики прогнозування інцидентів в інформаційних системах. Проаналізовано і обґрунтовано вибір параметрів інцидентів, які визначаються як ключові для ефективного прогнозування та запобігання можливим загрозам.

Вибір параметрів був виконаний на основі обширного огляду літератури та аналізу існуючих підходів до прогнозування інцидентів. Особлива увага була приділена важливості обрання параметрів, які є чутливими до змін у сучасному інформаційному середовищі.

Розроблена методика прогнозування інцидентів враховує комплексність і динаміку сучасних загроз, і дозволяє забезпечити організації засобами для активного виявлення та ефективного реагування на потенційні інциденти.

Отримані результати вказують на те, що розроблена методика є

перспективною у контексті покращення відповіді на інциденти і забезпечення високого рівня безпеки інформаційних систем. Подальші дослідження та вдосконалення методики можуть призвести до її більш широкого застосування в різних галузях та сценаріях застосування.

РОЗДІЛ 3

ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ПРОГНОЗУВАННЯ

3.1 Валідація та тестування методики

Перевірка ефективності методики прогнозування інцидентів у військових системах інформаційної безпеки включає кілька специфічних аспектів, оскільки ці системи мають особливі вимоги до безпеки, конфіденційності та надійності. Ключові елементи для перевірки ефективності наступні (рис. 3.1):

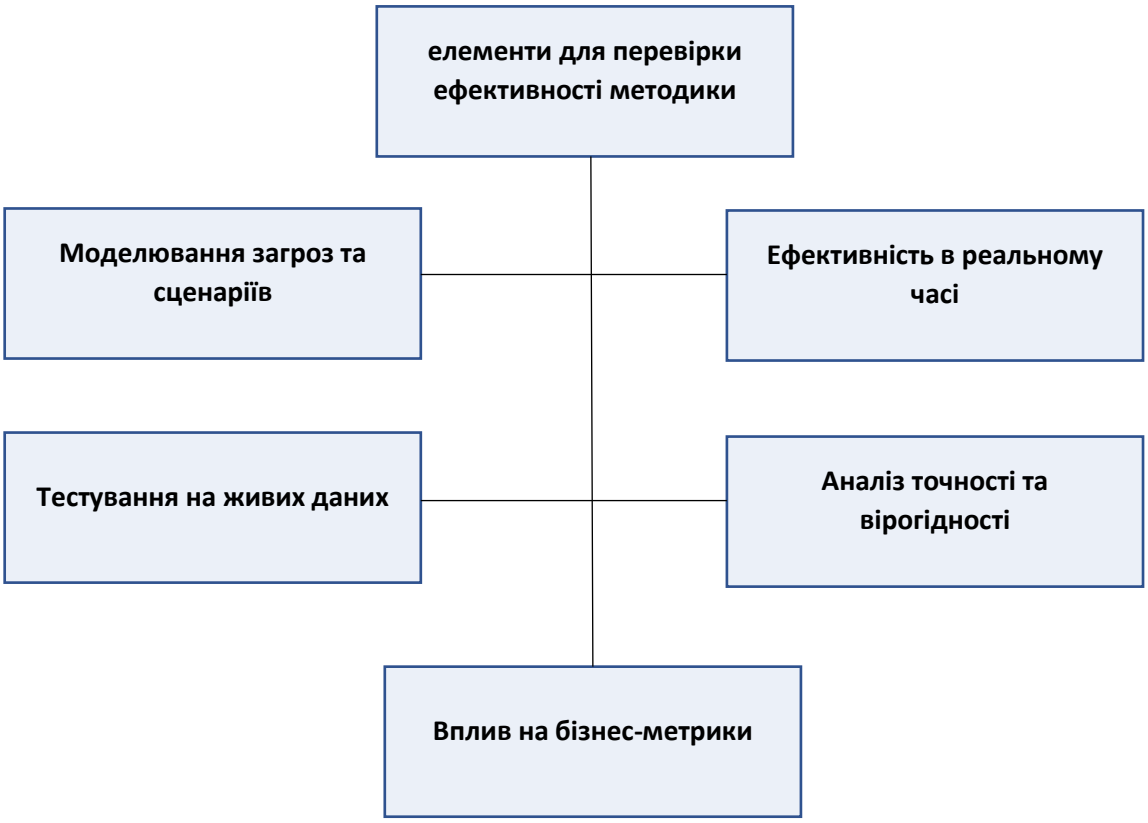

Рис. 3.1. Ключові елементи для перевірки ефективності методики [31]

Ключові елементи включають наступні пункти.

1. Моделювання загроз та сценаріїв

- Створення сценаріїв: створення реалістичних сценаріїв атак та інцидентів, що можуть статися у військових системах.

- Тестування реакції: тестування методики прогнозування на здатність передбачати ці сценарії.

2. Ефективність в реальному часі

- Час реагування: оцінка часу між прогнозом і реальною реакцією на інцидент.
- Адаптабельність: здатність методики швидко адаптуватися до нових загроз та атак.

3. Тестування на живих даних

- Тестування на реальних даних: використання реальних журналів подій інцидентів для перевірки точності та передбачуваності методики.
- Тестові сценарії: застосування методики до тестових сценаріїв на живих системах для оцінки реальної ефективності.

4. Аналіз точності та вірогідності

- Метрики ефективності: використання метрик, таких як точність, чутливість, специфічність та AUC-ROC для оцінки прогностичної здатності методики [32].
- Перевірка вірогідності: оцінка того, наскільки точні та достовірні прогнози методики.

5. Вплив на бізнес-метрики

- Вартість інцидентів: оцінка вартості втрат у разі неспрогнозованих або неефективно передбачених інцидентів.
- Час відновлення: визначення, наскільки швидко можна відновити роботу після інциденту, передбаченого методикою.

Перевірка ефективності методики прогнозування у військових системах вимагає інтенсивного тестування та оцінки на реальних умовах, з урахуванням специфіки військової безпеки, критичної важливості інформації та вимог до надійності та конфіденційності.

Валідація методик (Analytical Validation, AV) - документоване підтвердження того, що затверджена методика контролю придатна для застосування при виробництві та контролі якості лікарських засобів [33-38].

Верифікація програмного забезпечення - це процес визначення відповідності розроблюваного програмного забезпечення очікуванням, потребам і системним вимогам користувачів. Верифікація є одним з основних етапів тестування програмного забезпечення.

Метою процесу верифікації є забезпечення виконання певних вимог до програмного продукту, і це робиться за допомогою [39]:

- стратегій і критеріїв, розроблених для перевірки всіх робочих продуктів;
- узгодженої діяльності з верифікації.
- доказів того, що розроблений програмний продукт відповідає вимогам замовника та правилам використання;
- узгодження результатів перевірки продукту із замовником.

Процес валідації може виконуватися виконавцем або іншою стороною, наприклад, замовником. Виконавець реалізує цей процес відповідно до плану, який відображає елементи та завдання валідації, і вживає заходів для його виконання. Методи, інструменти та процедури використовуються для виконання завдань процесу, забезпечення відповідності вимогам тестів та створення специфікацій для правильної реалізації вимог за допомогою програмного продукту проекту [40-46] .

Верифікація та валідація передбачає перевірку специфікації та правильності виконання програми відповідно до заданих вимог та формального опису програми.

Верифікація програмного коду допомагає зробити висновки про коректність програмної системи, створеної під час проектування та після розробки. Верифікація передбачає перегляд, вивчення та оцінку результатів проектування протягом усього життєвого циклу, щоб визначити застосовність заданих вимог, переконатися, що вимоги реалізовані правильно і що умови та обмеження, визначені для системи, виконані. Верифікація та валідація перевіряють повноту, узгодженість та невизначеність специфікацій, а також

правильність виконання функцій системи.

Верифікація та валідація охоплює наступне [45]:

- компоненти системи, їх інтерфейси (програмні, апаратні, інформаційні) та взаємодію об'єктів у розподіленому середовищі (протоколи, повідомлення);
- визначення доступу до бази даних, заходи захисту від несанкціонованого доступу до даних різними користувачами;
- документація системи;
- тести, тестові процедури, набори вхідних даних.

Інші процеси життєвого циклу виконують додаткові дії:

Верифікація і контроль проектних рішень з використанням методів і процедур перегляду процесу розробки, доступ до CASE-систем, включаючи процедури перевірки вимог до продукту перегляд проміжних результатів та аудит відповідності вимогам для забезпечення того, що програмна система правильно реалізує та виконує вимоги та перегляд проміжних результатів та аудит відповідності вимогам, щоб гарантувати, що програмна система правильно реалізує вимоги та відповідає умовам функціонування.

Таким чином, основна мета процесу верифікації та валідації полягає у перевірці та підтвердженні того, що кінцевий програмний продукт відповідає своєму призначенню та вимогам замовника. Ці процеси взаємозалежні і часто описуються загальними термінами "верифікація та валідація" або "верифікація та валідація" (V&V).

V&V - це обробка і перевірка найважливіших елементів проекту: компонентів, інтерфейсів (програмних, апаратних, інформаційних), взаємодії об'єктів (протоколів, повідомлень), передачі даних між компонентами та їх захисту, а також розробка тестів і тестових процедур. Він ґрунтується на плануванні обох етапів.

Після перевірки окремих компонентів системи вони інтегруються як

цілісна система, повторно перевіряються і валідуються, а за результатами перевірки і тестування створюється комплект документів, що відображає правильність виконання вимог [47-48] .

У військових системах інформаційної безпеки експерименти з реальними даними для перевірки методологій вимагають системного підходу і дотримання певних принципів. Кроки для досягнення цього є наступними:

1) Отримання реальних даних:

2) Конфіденційність та дозволи: Забезпечити доступ до реальних даних, які є конфіденційними та відповідають усім необхідним дозволам і правилам безпеки;

3) Інтеграція даних: збір, обробка та інтеграція реальних журналів подій, записів та іншої інформації з військових систем;

4) Створення тестових кейсів, сценарії атак: створення сценаріїв, що моделюють можливі атаки або інциденти для використання в експериментах.

5) Реалістичність: забезпечення того, щоб тестові сценарії відображали реальні загрози та можливі ситуації.

6) Проведення експерименту

7) Реалізація методології: використання методів прогнозування на підготовлених тестових кейсах і реальних даних

8) Збір результатів: збір результатів прогнозування для подальшого аналізу.

9) Аналіз та оцінка ефективності:

10) Оцінка точності: визначення точності прогнозів на основі порівняння з реальними подіями та виявлення закономірностей.

11) Визначення критичних моментів: виявлення та аналіз ситуацій, коли методологія не спрацьовує або недопрогнозує події.

12) коригування та доопрацювання:

13) Вдосконалення методології: аналіз експериментальних результатів і внесення змін для підвищення ефективності методології.

14) Постійна підтримка: підтримка та оновлення методології на основі

даних і висновків.

Ці кроки допомагають оцінити ефективність методології на реальних даних і переконатися, що вона придатна для використання у військових системах інформаційної безпеки [49] .

3.2 Оцінка точності та надійності методики

Оцінка точності та надійності методики прогнозування інцидентів у військових системах інформаційної безпеки важлива для визначення її ефективності. Ключові моменти для цієї оцінки:

1. Точність:

- Confusion Matrix: Створення матриці помилок, яка відображає True Positives, True Negatives, False Positives та False Negatives.
- Accuracy (Точність): Визначення відсотка правильних прогнозів у загальній кількості прогнозів.
- Precision (Точність): Розрахунок відсотка правильно передбачених позитивних випадків серед усіх передбачених позитивних випадків.
- Recall (Повнота): Визначення відсотка правильно передбачених позитивних випадків серед усіх фактичних позитивних випадків.

2. Надійність:

- Cross-validation: Використання крос-валідації для перевірки стабільності та універсальності методики на різних підвибірках даних.
- Bootstrapping: Використання методу бутстрепа для оцінки стабільності прогнозів шляхом повторного випадкового вибору та оцінки результатів.

3. ROC та AUC:

- Receiver Operating Characteristic (ROC) Curve: Побудова графіка залежності між чутливістю та специфічністю методики.
- Area Under the Curve (AUC): Вимірює область під кривою ROC та

вказує на загальну ефективність методики.

4. Валідація на реальних даних:

- тестування на реальних сценаріях: Використання методики на реальних або симулюваних сценаріях для оцінки її прогностичної здатності;
- аналіз результатів: Оцінка прогнозів на реальних даних та порівняння їх з фактичними подіями;
- ці метрики та методи допоможуть визначити точність та надійність методики прогнозування інцидентів у військових системах інформаційної безпеки та підтвердити її ефективність [51] .

Висновок до розділу 3. У даному розділі магістерської роботи було проведено перевірку ефективності розробленої методики прогнозування інцидентів в інформаційних системах. Досягнуті результати вказують на важливі аспекти щодо валідації та тестування методики, а також на оцінку її точності та надійності.

Процес валідації та тестування методики був ретельно спланований та виконаний відповідно до визначених критеріїв. Використання реальних даних та сценаріїв допомогло визначити, наскільки добре методика працює в умовах, аналогічних реальному інформаційному середовищу.

Результати оцінки точності та надійності методики підтверджують його ефективність у прогнозуванні інцидентів. Порівняння прогнозів методики з реальними інцидентами свідчить про те, що вона здатна вчасно виявляти потенційні загрози та надавати підстави для прийняття заходів щодо їх запобігання чи обмеження наслідків.

Отже, отримані результати підтверджують ефективність розробленої методики прогнозування інцидентів, що робить її потенційно корисною для впровадження в реальні умови для підвищення рівня безпеки інформаційних систем. Подальші вдосконалення та розширення методики можуть ще більше підвищити її ефективність у змінних умовах сучасного інформаційного середовища.

РОЗДІЛ 4
РЕКОМЕНДАЦІЇ ПРАКТИЧНОГО ЗАСТОСУВАННЯ

4.1 Відпрацювання пропозицій для удосконалення рівня захисту інформації у військових системах

Застосування методики прогнозування інцидентів у військових системах інформаційної безпеки може бути корисним для забезпечення високого рівня захисту важливої інформації та реагування на можливі загрози. Ось кілька рекомендацій щодо її практичного застосування:

1. Підготовка даних та інтеграція:

- Очищення та підготовка даних: перед застосуванням методики переконайтеся, що дані належним чином очищені та готові до аналізу.
- Інтеграція з військовими системами: інтегруйте методику у військові інформаційні системи для безперервного моніторингу та аналізу потенційних інцидентів.

2. Тестування та оцінка ефективності:

- Проведення експериментів: тестуйте методику на реальних та симульованих сценаріях для оцінки її точності та надійності.
- Оцінка метрик: спостерігайте за метриками точності, чутливості, специфічності та іншими ключовими показниками для перевірки роботи методики.

3. Адаптація та постійне вдосконалення:

- Аналіз результатів: постійно аналізуйте результати та коригуйте методику відповідно до виявлених патернів та підходів.
- Стабілізація та розвиток: забезпечте стабільність та розвиток методики з урахуванням нових тенденцій у загрозах та технологіях.

4. Підтримка та навчання персоналу:

- Тренування персоналу: забезпечте навчання персоналу з використання методики та аналізу отриманих результатів.
- Підтримка та консультування: надайте підтримку та консультування персоналу з питань застосування методики [23] .

5. Інтеграція в стратегічні процеси:

- Реакція на результати: використовуйте результати прогнозування для стратегічного планування та прийняття рішень.
- Інтеграція у системи управління ризиками: впроваджуйте методику у системи управління ризиками для попередження можливих інцидентів.

Ці практичні рекомендації допоможуть впровадити та максимально використати методику прогнозування інцидентів у військових системах інформаційної безпеки для забезпечення найвищого рівня захисту [24] .

Існують різноманітні системи та підходи до забезпечення інформаційної безпеки у військових інформаційних системах. Деякі з них включають:

1. Сегментація мережі:

- Застосування фізичних та логічних бар'єрів: розділення мережі на сегменти, які забезпечують обмежений доступ до конкретних частин системи.

2. Криптографічні заходи:

- Шифрування даних: використання криптографії для захисту конфіденційності та цілісності даних, особливо у випадку передачі чутливої інформації.

3. Управління доступом:

- Системи автентифікації та авторизації: використання систем ідентифікації та контролю доступу для забезпечення правильного доступу користувачів до системи.

4. Моніторинг та виявлення загроз:

- Системи моніторингу та аналізу подій: виявлення потенційних загроз та надання можливості реагувати на них у реальному часі.

5. Фізична безпека:

- Захист фізичного доступу: застосування фізичних заходів безпеки, таких як бар'єри, камери спостереження та обмежений доступ до приміщень.

6. Аудит та відповідність стандартам:

- Перевірка та оцінка безпеки: регулярні аудити та оцінка систем з метою визначення відповідності стандартам безпеки.

7. Захист від кібератак:

- Запобігання та реагування на кіберзагрози: використання різноманітних заходів для захисту від хакерських атак, вірусів та інших кіберзагроз.

Ці підходи і системи можуть використовуватися окремо або спільно для створення комплексної системи захисту інформації у військових інформаційних системах, що має вирішувати низку унікальних викликів та загроз у військовому середовищі.[23, 51]

Основною метою створення системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України є попередження і нейтралізація інформаційних загроз їх функціонуванню, створення умов для сталого та гарантованого виконання Міністерством оборони та Збройними Силами України завдань визначених Конституцією та законами України. Під час обґрунтування критеріїв та показників, що впливають на ефективність функціонування системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України, були враховані вимоги міжнародних та національних керівних документів та стандартів у визначеній сфері. За основу взята “модель безпеки ЦКД” (забезпечення цілісності, конфіденційності та доступності інформації). Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України на відміну від існуючої ґрунтується на удосконаленій системі критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України. Схема показана на рис.4.1.

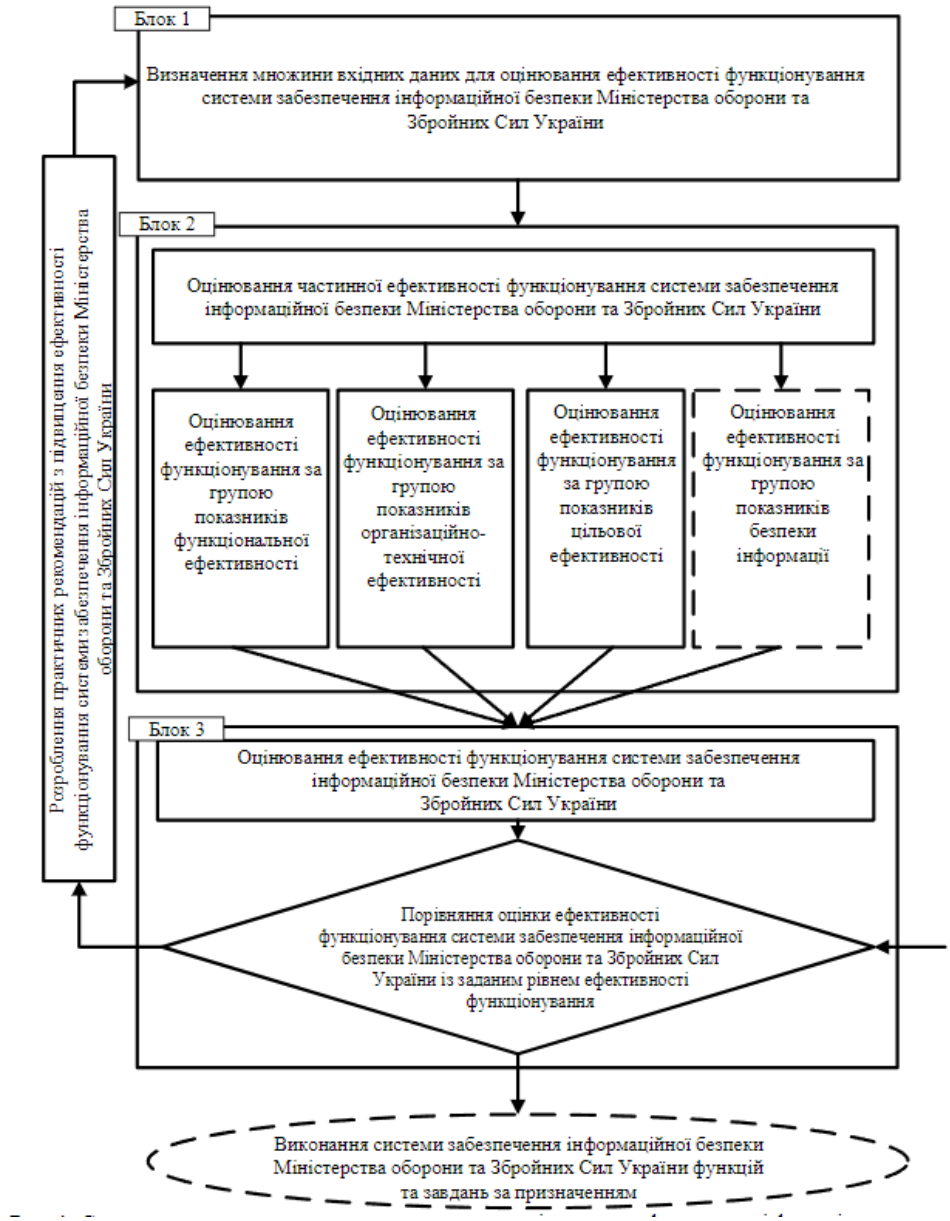

Рис.4.1. Структурна схема удосконаленої методики оцінювання ефективності функціонування системи забезпечення інформаційної безпеки Міністерства оборони та Збройних Сил України

4.2 Практичні рекомендації керівникам структурних підрозділів

З метою підвищення безпеки та надійності інформаційних систем військового призначення є кілька практичних рекомендацій:

1. Аудит та оновлення безпеки:

- Регулярні аудити безпеки: проведення систематичних оглядів та оцінок, щоб ідентифікувати потенційні слабкі місця та вразливості системи.
- Постійні оновлення: забезпечення постійних оновлень програмного забезпечення та застосунків для закриття вразливостей.

2. Захист даних:

- Шифрування даних: застосування криптографічних методів для захисту конфіденційної інформації в покращеній формі.
- Строгий контроль доступу: встановлення механізмів авторизації та автентифікації для обмеження доступу до чутливої інформації.

3. Системи виявлення загроз:

- Використання систем виявлення інцидентів: установка систем, які надають можливість виявлення відхилень у поведінці системи та потенційних атак.
- Моніторинг подій: реагування на надзвичайні події шляхом постійного моніторингу та аналізу.

4. Навчання та свідомість персоналу:

- Тренування з безпеки: проведення регулярних навчань для персоналу з питань кібербезпеки та свідомості щодо загроз.
- Створення культури безпеки: підтримка свідомості про безпеку серед усіх працівників, включаючи відповідальність за безпеку даних.

5. Резервне копіювання та відновлення:

- Регулярні резервні копії: виконання регулярних резервних копій даних для можливості відновлення після інцидентів.
- Плани відновлення після кризи: розробка планів відновлення

діяльності в разі серйозних інцидентів.

Ці рекомендації можуть покращити безпеку та надійність військових інформаційних систем, забезпечуючи кращу захищеність даних та зменшуючи ризик можливих загроз.

Для практичного використання розробленої методики прогнозування інцидентів у військових інформаційних системах рекомендую:

1. Впровадження методики:

- Тестування на обмеженому масштабі: почніть з впровадження методики на обмеженому масштабі для перевірки її ефективності та коригування перед загальним застосуванням.
- Ітеративний процес вдосконалення: розвивайте методику через ітеративний процес, враховуючи нові дані та висновки.

2. Інтеграція з існуючими системами:

- Синтез з існуючими інструментами безпеки: інтегруйте методику вже існуючими системами безпеки для комплексного аналізу та реагування на загрози.
- Автоматизація процесу: розгляньте можливість автоматизації процесу прогнозування через підключення до систем моніторингу та виявлення загроз.

3. Підготовка персоналу:

- Навчання персоналу: проведіть навчання персоналу щодо використання методики, її особливостей та принципів роботи.
- Підтримка та консультації: забезпечте можливість отримання підтримки та консультацій з використання методики для ефективного застосування.

4. Моніторинг та оцінка:

- Система моніторингу результатів: створіть систему моніторингу результатів застосування методики для оцінки її ефективності в реальному часі.
- Аналіз впливу: проводьте періодичний аналіз впливу використання методики на загальну безпеку та надійність систем.

5. Постійне вдосконалення:

- Фідбек та коригування: враховуйте отриманий фідбек для постійного удосконалення методики.
- Розробка нових функцій: розвивайте методику, додавши нові функції або враховуючи нові методи та підходи у сфері кібербезпеки.

Ці рекомендації допоможуть забезпечити успішне та ефективне впровадження розробленої методики прогнозування інцидентів у практичній діяльності військових систем.[15, 50, 52]

У цій області існує безліч напрямків для подальших досліджень, спрямованих на покращення безпеки та надійності військових інформаційних систем:

1. Розробка нових алгоритмів прогнозування:

- Удосконалення методів машинного навчання: розвиток нових моделей та алгоритмів, які б краще враховували специфіку загроз у військових системах.
- Глибше використання штучного інтелекту: дослідження можливостей використання AI для виявлення вразливостей та прогнозування нових типів атак.

2. Аналіз нових типів загроз:

- Стратегії кіберзахисту: вивчення нових методів атак та виявлення потенційних слабких місць у системах безпеки.
- Кібервійна та кіберстратегії: дослідження впливу кіберзагроз на військові операції та розробка стратегій відповіді на них.

3. Використання квантових технологій:

- Безпека квантових систем: дослідження та розробка методів квантової криптографії для захисту від квантових обчислювальних атак.
- Квантове виявлення загроз: використання квантових принципів для виявлення та передбачення кіберзагроз.

4. Кіберфізична безпека:

- Інтеграція фізичних та кіберзагроз: дослідження заходів безпеки

для кіберфізичних систем, які поєднують технології та фізичні компоненти.

- Моделювання вразливостей: аналіз впливу кібератак на фізичні системи та розробка заходів захисту.

5. Покращення відповіді на інциденти:

- Системи реагування на інциденти: розробка ефективних систем реагування та відновлення після кіберінцидентів.
- Аналіз та вдосконалення планів бізнес-контингентності: Дослідження та вдосконалення стратегій для швидкого відновлення діяльності після атак.

Ці напрямки досліджень спрямовані на розвиток більш ефективних та інноваційних методів забезпечення безпеки військових інформаційних систем у змінному кіберпросторі .

Висновки до розділу 4. У ході дослідження було проведено обґрунтований аналіз та вивчення актуальних проблем в області безпеки інформаційних систем. Відповідно до поставлених завдань, були розроблені методики прогнозування інцидентів, вивчені та аналізовані параметри безпеки, і враховані ключові аспекти, такі як військові інформаційні системи.

На основі отриманих результатів розроблено конкретні рекомендації для практичного впровадження в області безпеки інформаційних систем. Рекомендації орієнтовані на вдосконалення стратегій прогнозування інцидентів та підвищення рівня захисту в інформаційних системах. Зокрема, важливо активно використовувати розроблені методики в системах моніторингу безпеки та забезпечити їхню взаємодію з існуючими інструментами управління ризиками.

Отримані рекомендації стануть підґрунтям для подальших практичних застосувань у сфері інформаційної безпеки та можуть служити орієнтиром для фахівців, що зацікавлені у підвищенні рівня захисту інформаційних систем.

ВИСНОВКИ

У висновках можна відзначити, що безпека військових інформаційних систем є критично важливою для забезпечення національної безпеки та ефективності військових операцій. Розробка та застосування методик прогнозування інцидентів є важливим етапом для попередження кібератак, виявлення вразливостей та підвищення рівня захисту систем.

Дослідження в цій області вимагає постійного вдосконалення та адаптації до нових загроз, оскільки кібератаки постійно еволюціонують. Важливо підкреслити значення поєднання технічних рішень, які використовують передові технології, з вдосконаленням стратегій та процесів управління кібербезпекою.

На основі отриманих результатів розроблено конкретні рекомендації для практичного впровадження в області безпеки інформаційних систем. Рекомендації орієнтовані на вдосконалення стратегій прогнозування інцидентів та підвищення рівня захисту в інформаційних системах. Зокрема, важливо активно використовувати розроблені методики в системах моніторингу безпеки та забезпечити їхню взаємодію з існуючими інструментами управління ризиками. Однак, розвиток нових методик, які базуються на штучному інтелекті, квантових технологіях та кіберфізичній безпеці, може стати новими перспективними напрямками для поліпшення безпеки військових інформаційних систем.

Загальний висновок полягає в тому, що розуміння поточних тенденцій у кібербезпеці, використання передових технологій та постійне вдосконалення методик прогнозування інцидентів є ключовими для забезпечення безпеки та надійності військових інформаційних систем у сучасному цифровому світі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Pavlenko, E.Y., Yarmak, A.V. & Moskvin, D.A. Hierarchical approach to analyzing security breaches in information systems. Aut. Control Comp. Sci. 51, 829–834 2017. URL: https://doi.org/10.3103/S0146411617080144.

2. Коваленко, Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. № (3). с. 123–129. Архів оригіналу за 21 січня 2022. Процитовано 16 листопада 2019.

3. Інформаційна безпека (2-а книга соціально-політичного проекту «Актуальні проблеми безпеки соціума»). К.: «Зброя і технології», 2009. 112 с.

4. ДСТУ СУІБ 1.0/ISO/IEC 27001:2010 [Архівовано 21 серпня 2011 у Wayback Machine.], Інформаційні технології-методи захисту-система управління інформаційною безпекою, офіційний переклад, ст.3. URL: https://s-byte.com/useful/27001.pdf (дата звернення 13.10.2023 р.).

5. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 № 537-V. Архів оригіналу за 8 листопада 2018. URL: https://zakon.rada.gov.ua/go/537-16. (дата звернення 13.10.2023 р.)

6. Г. Сащук . Інформаційна безпека в системі забезпечення національної безпеки. Архів оригіналу за 10 листопада 2015.

7. Про основні засади забезпечення кібербезпеки України: Закон України Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/2163-19. (дата звернення 13.10.2023 р.)

8. Baboş, Alexandru, Iacob, Corneliu-George and Ene, Cristian. Use of Forecasting Systems in the Military Decision Making Process. Land Forces Academy Review, vol.27, no.4, 2022, pp.316-322. URL: https://doi.org/10.2478/raft-2022-0040

9. CIA Triad - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/ (дата звернення 13.10.2023 р.).

10. Chai W. What is the CIA triad? Definition, explanation, examples | techtarget. WhatIs. URL: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA (дата звернення 13.10.2023 р.).

11. What is the CIA triad and why is it important? | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/cia-triad (date of access: 03.10.2023).

12. Архипов О.Є., Муратов О.Є. Про зміст та взаємозв'язок понять "інформаційна безпека" та "безпека інформації. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., 17 березня 2010 р., м. Київ. – К.: Наук.-вид. Відділ НА СБ України, 2010. – С.185-187.

13. Архипов О.Є, Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах. Інформаційна безпека людини, суспільства, держави: науково-практ.журнал / Національна академія Служби безпеки України. – 2010. – №2(4).– С.62-65.

14. Фостолович В.А. Інформаційно-аналітична база в інтегрованій системі управління підприємством. Проблеми економічного, облікового, контрольного і аналітичного забезпечення управління підприємством: матеріали II Всеукр. наук.-практич. конф. молод. учених, 8 грудня 2016 року − Вінниця. − «Едельвейс і К». С.179-181.

15. Бурик З.М., Огірко О.І. Інформаційні технології забезпечення сталого розвитку в контексті формування нової науково-технічної парадигми. Міжнародний науковий журнал «Інтернаука». 2017. № 1(2). С. 24–28. URL: http://nbuv.gov.ua/UJRN/mnj_2017_1%282%29__8 (дата звернення: 03.10.2023).

16. Правдюк А. Л., Прутська Т. Ю., Правдюк М. В. Інформаційне забезпечення управління підприємницькою діяльністю на засадах інституціоналізму: монографія. Київ: «Центр учбової літератури». 2019. – 360 с.

17. Sepideh Yeganegi, André O. Laplume, Parshotam Dass, The role of information availability: A longitudinal analysis of technology entrepreneurship,

Technological Forecasting and Social Change, Vol. 170, 2021, 120910, URL: https://doi.org/10.1016/j.techfore.2021.120910.

18. Laplume A. O., Pathak S., Xavier-Oliveira E. The politics of intellectual property rights regimes: An empirical study of new technology use in entrepreneurship. Technovation. – 2014. – Т. 34. – №. 12. – С. 807-816. URL: https://doi.org/10.1016/j.technovation.2014.07.006.

19. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological forecasting and social change. – 2020. – Vol.. 150. – p. 119791. URL: https://doi.org/10.1016/j.techfore.2019.119791.

20. Menzel M., Thomas I., Meinel C. Security requirements specification in service-oriented business process management //2009 International Conference on Availability, Reliability and Security. – IEEE, 2009. – pp. 41-48. URL: https://doi.org/10.1109/ARES.2009.90.

21. Stephenson P. S-TRAIS: A Method for Security Requirements Engineering Using a Standards Based Network Security Reference Model. Conference Proceedings from SREIS. – 2005. С. 44-51.

22. К. Волтер, М. Менцель, А. Шаад, Ф. Місельдін, К. Майнель. Специфікація вимог безпеки бізнес-процесів на основі моделі. Журнал системної архітектури 55, № 4. 2009. С. 211-223. URL: https://doi.org/10.1016/j.sysarc.2008.10.002 .

23. Lakomaa E., Kallberg J. Open data as a foundation for innovation: The enabling effect of free public sector information for entrepreneurs. IEEE Access. – 2013. – Vol. 1. – pp. 558-563. URL: https://doi.org/10.1109/ACCESS.2013.2279164.

24. S. Kondakci, Analysis of information security reliability: A tutorial, Reliability Engineering & System Safety, Volume 133, 2015, Pages 275-299, URL: https://doi.org/10.1016/j.ress.2014.09.021.

25. Martins, J. & Santos, Henrique & Nunes, Paulo & Silva, Rui. Information Security Model to Military Organizations in Environment of Information

Warfare. 11th European Conference on Information Warfare and Security 2012, ECIW 2012. 172-179. URL: https://doi.org/10.2316/j.sysarc.2012.10.42.

26. Erkan, B.; Mehmet, D.; Koh, S.C.L.; Tatoglu, E.; Zaim, H. A causal analysis of the impact of information systems and supply chain management practices on operational performance: Evidence from manufacturing SMEs in Turkey. Int. J. Prod. Econ. 2009, 122, 133–149. URL: https://doi.org/10.1016/j.ijpe.2009.05.011.

27. Habib, M. Supply Chain Management (SCM): Its future implications. Open J. Soc. Sci. 2014, 2, 238–246. URL: https://doi.org/10.4236/jss.2014.29040.

28. Matinrad, N., Roghanian, E., Rasi, Z. Supply chain network optimization: A review of classification, models, solution techniques and future research. Uncertain Supply Chain Manag. 2013, 1, pp.1–24. URL: https://doi.org/10.5267/j.uscm.2013.05.003.

29. Анісімов В.Г., Анісімов Є.Г., Зегжда П.Д., Сауренко Т.М., Присяжнюк С.П., Показники ефективності захисту інформації в системі інформаційної взаємодії для управління складними розподіленими організаційними об'єктами, Автомат. Контрольні обчислення. наук, 2017, том 51, No 8, с. 824–828. URL: https://doi.org/10.3103/S0146411617080053.

30. Анісімов В.Г., Зегжда Д.П., Анісімов Є.Г., Бажин Д.А. Ризик-орієнтований підхід до організації управління підсистемами захисту інформаційних систем Autom. Контрольні обчислення. наук, 2016, том 50, No 8, с. 717–721. URL: https://doi.org/10.3103/S0146411616080289

31. Pavlenko, E.Y., Yarmak, A.V. & Moskvin, D.A. Hierarchical approach to analyzing security breaches in information systems. Aut. Control Comp. Sci. 51, 829–834. 2017. URL: https://doi.org/10.3103/S0146411617080144.

32. Lele, A. Disruptive Technologies for the Militaries and Security, SmartInnovation, Systems and Technologies 132. 2018Available at: URL: https://doi.org/10.1007/978-981-13-3384-2_1 (accesed on 23 September 2022)

33. Mojtahedi, M., & Lanoo, B. Critical attributes for proactive engagement ofstakeholders in disaster risk management . 2017. Available at: URL: https://doi.org/10.1016/j.ijdrr.2016.10.017. (accesed on 28 September 2022).

34. Шаньгін, В.Ф. Захист комп'ютерної інформації. Ефективні методи і засоби. - М.: ДМК Пресс, 2008. - 544 с.

35. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/go/851-15. (дата звернення 13.10.2023 р.)

36. Казакова Н.Ф. Аналіз внутрішніх та зовнішніх загроз корпоративних мереж. Матер. міжвідомч. міжрегіон. семінару Наук. Ради НАН України «Технічні засоби захисту інформації», 15 лютого 2006 р., Київ-Одеса : НАН України, 2006. – С.11.

37. Казакова Н.Ф. Принципи створення систем мережного управління. Матер. наук.-практ. конф. проф.-викл. складу «Актуальні проблеми та досвід використання сучасних інформаційно-комунікаційних технологій», 10-12 травня 2005 р., Одеса : ОНЮА, 2005. – С.133-138.

38. J. Kim, H. Lee and S. Choi, Machine learning based approach for demand forecasting anti-aircraft missiles. 2018 5th International Conference on Industrial Engineering and Applications (ICIEA), Singapore, 2018, pp. 367-372, URL: https://doi.org/10.1109/IEA.2018.8387126.

39. J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, et al. Big Data: The Next Frontier for Innovation. in Competition and Productivity, New York:McKinsey Global Institute. 2011.

40. J. Kim and H. Lee, A study on forecasting spare parts demand based on data-mining. Internet Comput. Serv., vol. 18, no. 1, pp. 121-129, 2017. URL: https://doi.org/10.7472/jksii.2017.18.1.121.

41. Heckman, R.M. Attacker Classification to Aid Targeting Critical Systems for Threat Modelling and Security Review. 2005. Available online: www.rockyh.net/papers/AttackerClassification.pdf (accessed on 22 January 2020).

42. Rocchetto M., Tippenhauer N. O. On attacker models and profiles for cyber-physical systems //Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30,

2016, Proceedings, Part II 21. – Springer International Publishing, 2016. – C. 427-449. URL: https://doi.org/10.1007/978-3-319-45741-3_22.

43. Kotenko, I.; Stepashkin, M.; Doynikova, E. Security Analysis of Computer-aided Systems Taking into Account Social Engineering Attacks. In Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2011), Los Alamitos, CA, USA, 9–11 February 2011; pp. 611–618.

44. Urbina, D., Giraldo, J., Tippenhauer, N.O., Cardenas, A.: Attacking fieldbus communications in ICS: applications to the SWaT testbed. In: Proceedings of Singapore Cyber Security R&D Conference (SG-CRC), January 2016. Pp. 345-354.

45. United States Environmental Protection Agency. Epanet: Software that models the hydraulic and water quality behavior of water distribution piping systems. https://www.epa.gov/nrmrl/wswrd/dw/epanet.html. (дата звернення 13.10.2023 р.).

46. Teixeira, A., Pérez, D., Sandberg, H., Johansson, K.H.: Attack models and scenarios for networked control systems. In: Proceedings of the Conference on High Confidence Networked Systems (HiCoNS), pp. 55–64. ACM. 2012. URL: https://doi.org/10.1145/2185505.2185515.

47. Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A.: Simulation of cyber-physical attacks on water distribution systems with EPANET. In: Proceedings of Singapore Cyber Security R&D Conference (SG-CRC), January 2016

48. Salomons E., Ostfeld A. Simulation of cyber-physical attacks on water distribution systems with EPANET. Proceedings of the Singapore Cyber-Security Conference (SGCRC). – 2016. – С. 123.

49. SPaCIoS. Deliverable 3.3.2: Methodology and technology for vulnerability-driven security testing (final version). 2014. http://www.spacios.eu

50. Chang S. Y., Hu Y. C., Liu Z. Securing wireless medium access control against insider denial-of-service attackers. 2015 IEEE Conference on Communications and Network Security (CNS). – IEEE, 2015. – С. 370-378. URL: https://doi.org/10.1109/CNS.2015.7346848.

51. Denning D. E. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy //Networks and netwars: The future of terror, crime, and militancy. – 2001. – T. 239. – C. 288.

52. Mohajerin Esfahani P., Vrakopoulou M., Margellos K., Lygeros J. Andersson G. Cyber attack in a two-area power system: Impact identification using reachability. Proceedings of the 2010 American Control Conference, Baltimore, MD, USA, 2010, pp. 962-967, URL: https://doi.org/10.1109/ACC.2010.5530460.