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: “ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ІНЦИДЕНТАМИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ”

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

_____ Олександр ХАРИТОНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Олександр ХАРИТОНОВ

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Харитонову Олександру Володимировичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Ефективність управління інцидентами в автоматизованих системах управління"

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: *інциденти кібербезпеки, інформаційна безпека підприємства, методи та засоби підвищення ефективності управління інцидентами, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література*

4. Перелік питань, які потрібно розробити:
   1. Проаналізувати існуючі системи управління.
   2. Визначити і дати характеристику методам управління інцидентами.
   3. Розробити пропозиції щодо вдосконалення системи управління інцидентами.
   4. Реалізувати та протестувати пропозиції щодо підвищення ефективності управління інцидентами в АСУ.
   5. Проаналізувати результати.

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 існуючих систем управління інцидентами	27.10.2023	
4.	Дослідження основних методів управління інцидентами, визначення і надання характеристик	10.11.2023	
5.	Розробка пропозиції щодо вдосконалення системи управління інцидентами, моделювання, тестування та аналіз результатів	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.	17.01.2024	

Здобувач вищої освіти _____ Олександр ХАРИТОНОВ
(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 Харитонов О.В,. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

Освітньо-професійної програми Управління інформаційною безпекою
(назва)

на тему: "Ефективність управління інцидентами в автоматизованих системах управління"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ХАРИТОНОВ Олександр** у кваліфікаційній роботі дослідив сучасний стан управління інцидентами в автоматизованих системах управління, визначив основні проблеми та запропонував комплексне застосування критеріїв для оцінювання ефективності системи управління інцидентами в АСУ. Удосконалена модель системи управління інцидентами, яка відрізняється від відомих додатковою автоматизованою лінією управління інцидентами. Розроблені пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності управління інцидентами у автоматизованих системах управління. **ХАРИТОНОВ Олександр** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.
Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ХАРИТОНОВА Олександра** 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 . Здобувач Харитонов О.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 Харитонова Олександра Володимировича
на тему “ ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ІНЦИДЕНТАМИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ”

Актуальність. У роботі правильно визначена і обгрунтована актуальність неообохідності підвищення ефективності управління інцидентами у автоматизованих системах управління. Швидкий розвиток технологій виявив нагальну потребу у підвищенні ефективності захисту автоматизованих систем управління. Інциденти, пов’язані з автоматизованими системами управління можуть завдати небачених наслідків для людини, суспільства і держави вцілому. Тому, для ефективного захисту інформації в автоматизованих системах важливо вміти управляти інцидентами, виявляти, планувати та організовувати превентивні заходи безпеки.

Позитивні сторони. В роботі розглянуто основні поняття та опис процесів що потребують захисту в автоматизованих системах управління, проаналізовані основні проблеми управління інцидентами та проведена класифікація інцидентів в АСУ. Проведений аналіз існуючих процедур та методів управління інцидентами дозволив визначити вплив інцидентів на функціонування автоматизованих систем та потребу у підвищенні ефективності. У роботі вперше визначені комплексні критерії ефективності автоматизованої системи управління інцидентами та їх показники. Описаний процес удосконалення моделі системи управління інцидентами введенням додаткової автоматизованої лінії управління на основі результатів попередніх обробок. Реалізація запропонованого підходу дозволила суттєво підвищити значення визначених показників ефективності.

Недоліки. Разом з тим, доцільно було б приділити більше уваги застосуванню штучного інтелекту при відпрацюванні методики.
Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Харитонов Олександр Володимирович - 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: 92 стор., 25 рис., 3 табл., 66 джерел.

Метою роботи є дослідження та оцінка ефективність управління інцидентами в автоматизованій системі управління з метою вдосконалення процедур та підвищення рівня безпеки та надійності таких систем.

Об'єктом дослідження є управління інцидентами в автоматизованих системах управління

Предмет *дослідження* - методи підвищення ефективності в автоматизованих системах управління.

Методи дослідження. Для аналізу та оцінці ефективності управління інцидентами використовуються методи системного аналізу, теорія графів, теорія складних мереж, теорія множин та теорії інформаційної безпеки та інформаційного протиборства. Для моделювання системи управління інцидентами використовувалась мова програмування Python та бібліотеки NumPy, Pandas, бібліотека Matplotlib зі стеку SciPy.

Короткий зміст роботи. Як результат у роботі проведено аналіз існуючих систем управління інцидентами, представлена таблиця з існуючими інцидентами, розібрані найпоширеніші інциденти, представлена існуюча модель процесу управління інцидентами, а також її вдосконалена версія, проведено тестування вдосконалення, та представлено рекомендації щодо покращення ефективності управління інцидентами.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації автоматизованих систем управління інформаційною безпекою підприємства.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 92 pages, 25 figures, 3 tables, 66 sources.

The purpose of the study is to investigate and evaluate the effectiveness of incident management in an automated control system in order to improve procedures and increase the level of safety and reliability of such systems.

The object of research is incident management in automated control systems.

The subject of research is methods of increasing efficiency in automated control systems.

Research methods. To analyze and evaluate the effectiveness of incident management, methods of system analysis, graph theory, complex network theory, set theory, and theories of information security and information warfare are used. The Python programming language and the libraries NumPy, Pandas, and the Matplotlib library from the SciPy stack were used to model the incident management system.

Brief content of research. As a result, the paper analyzes existing incident management systems, presents a table with existing incidents, analyzes the most common incidents, presents the existing model of the incident management process, as well as its improved version, tests the improvement, and presents recommendations for improving the efficiency of incident management.

Field of research. The developed approaches can be used in the planning and implementation of automated enterprise information security management systems.

KEYWORDS : ENTERPRISE INFORMATION SECURITY, THREAT TO INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, CYBERSECURITY INCIDENTS.

ЗМІСТ

ВСТУП

Актуальність теми. Інформація у XXI столітті, це нове золото, хто володіє інформацією - володіє світом. Тому захист інформації - завдання номер 1 у світі. При швидкому розвитку технологій, захисту потребують автоматичні системи управління, бо інциденти зв’язані з автоматизованими системами управління (АСУ) можуть завдати небачених наслідків, тому, щоб уникнути катастрофи важливо вміти виявляти, реагувати, усувати і відновлювати від інцидентів АСУ, саме цьому присвячене управління інцидентами в АСУ. Але просто управляти інцидентами недостатньо, у зв`язку з тим, що кібербезпека, як канат, який потрібно перетягнути на свій бік, так і кібербезпека - процес коли хакери протидіють системам. Потрібно постійно підвищувати ефективність систем управління інцидентами.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню ефективності управління інцидентами кібербезпеки в автоматизованих системах управління

Мета роботи полягає у досліджені та оцінці ефективності управління інцидентами в автоматизованій системі управління з метою вдосконалення процедур та підвищення рівня безпеки та надійності таких систем

Об’єктом дослідження є управління інцидентами в автоматизованих системах управління

Предмет дослідження - методи підвищення ефективності в автоматизованих системах управління.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Зробити аналіз існуючих систем управління та інформаційних процесів в автоматизованих системах управління.

2. Проаналізувати вплив інцидентів на ефективність управління в автоматизованих системах.

3. Розробити пропозиції щодо вдосконалення системи управління інцидентами.

4. Оцінити запропоновані пропозиції.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки.

Наукова новизна одержаних результатів. В роботі вперше визначено комплексне застосування критеріїв для оцінювання ефективності системи управління інцидентами в АСУ. Запропонована удосконалена модель системи управління інцидентами, яка відрізняється від відомих додатковою автоматизованою лінією управління інцидентами на основі результатів попередніх ліній.

Практичне значення одержаних результатів. Розроблені підходи можуть бути використані для підвищення ефективності управління інцидентами в існуючих АСУ, та при створенні нових. Застосування напрацювань дадуть змогу підвищити ефективність управління інцидентами в існуючих АСУ, та при створенні нових АСУ.

Апробація результатів кваліфікаційної роботи було оприлюднено 23 лютого 2023 року на Всеукраїнській науковій конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (Матеріали Всеукраїнської науково-практичної Інтернет-конференції (м. Київ,) / Навчально-науковий інститут захисту інформації ДУТ. Київ, 2023. С. 96-98).

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

1.1. Опис процесів управління в автоматизованих системах, що потребують захисту

Автоматизовані системи управління включають в себе різноманітні інформаційні процеси, спрямовані на ефективне управління різними аспектами діяльності:

- збір і зберігання даних;
- обробка інформації;
- моніторинг і контроль;
- комунікації і взаємодія;
- прийняття рішень;
- забезпечення безпеки і конфіденційності;
- інтеграція систем;
- управління ресурсами;
- аналіз і звітність;
- управління версіями і конфігурацією.

У контексті технічного захисту АСУ поділяють на три рівні.

Верхній рівень - рівень візуалізації, диспетчеризації та збору даних. Тут знаходяться операторські станції та системний сервер. Найчастіше цей рівень є єдиним комплексом управління та моніторингу АСУ . Як правило, тільки на цьому рівні є взаємодія із зовнішніми джерелами. З цих причин його захист є максимально критичним.

Середній рівень – рівень обробки та прямого впливу на контрольно-вимірювальну інформацію, яка є найбільш критичним типом даних АСУ . Середній рівень також потребує технічного захисту.

Нижній рівень – рівень контрольно-вимірювального обладнання. Як правило, він надійно захищений фізично та невідомий зловмисникам.

Основні функції АСУ покликані:

- автоматизувати керування параметрами технологічного процесу. Контролером системи здійснюється регулювання досягнення оптимальних процесів зупинки і запуску устаткування, і навіть оперативної реакції системи на зовнішні зміни. Це позитивно впливає на якість інших технологічних процесів;
- здійснювати моніторинг, обробку та видачу керуючих впливів та реєструвати дані про технологічний процес та обладнання. Контролер системи автоматично збирає та обробляє інформацію від датчиків процесу. Оператор вбачає результат у режимі реального часу;
- розпізнавати, сповіщати та реєструвати аварійні ситуації та технічні збої. Контролер системи або повідомляє про порушення оператора, або автоматично блокує розвиток непередбаченої ситуації;
- дистанційно керувати технологічним обладнанням автоматично або вручну з робочого місця оператора;
- реєструвати контрольовані параметри, такі як дії чи бездіяльності оператора, та автоматично архівувати їх у базі даних на сервері системи з прив'язкою до часу. Це дозволяє визначити причину аварійної ситуації та вжити необхідних заходів, щоб уникнути повторення подібних випадків;
- надавати поточну та архівну інформацію з бази даних у вигляді графіків, таблиць та трендів. Це дозволяє організувати діловодство якісніше;
- обмежувати доступ до системи різними рівнями паролів. Передбачено рівень оператора, керівника та обмежений доступ до інженерного складу.

Автоматизація процесів має безліч плюсів і дійсно здатна підвищити економічну ефективність підприємства, але недотримання вимог забезпечення інформаційної безпеки (ІБ) можуть зробити автоматизацію критично небезпечною.

Під захистом інформації в автоматизованих системах управління слід розуміти комплекс практичних взаємопов'язаних заходів, спрямованих на запобігання розкриттю, несанкціонованому використанню, зміні, спотворенню, знищенню, копіюванню, шпигунству та іншим негативним втручанням в АСУ.

Для удосконалення заходів, спрямованих на безпеку АСУ , професійні спільноти ведуть спільні розробки базових методик у галузі захисту баз даних (БД). Діяльність у цьому напрямі включає стандартизацію технічних заходів, розробку нормативних документів, створення методик навчання адміністраторів та користувачів.

Автоматизовані системи управління здійснюють збирання, зберігання та систематизацію даних, необхідні для оптимального контролю над технологічними процесами.

АСУ створюються на основі надійної обчислювальної техніки промислової розробки та призначені для цілодобового довгострокового використання на технологічному об'єкті. Наслідки збою в роботі АСУ становлять серйозну небезпеку для людей, обладнання, довкілля можуть мати катастрофічний характер.

Для вибудовування грамотного та ефективного захисту слід виявити потенційних порушників в АСУ, визначити рівень загроз. Основну загрозу АСУ становлять терористично налаштовані групи, які мають на меті втручання в процес управління автоматизованою системою з подальшим виведенням її з ладу. Терористичні угруповання збирають технічні деталі для розробки та проведення атак, тому слід вчасно убезпечити систему. Здатність структури АСУ стабільно забезпечувати безперервний технологічний процес, який залежить від зовнішніх чинників впливу, є її основним показником.

Заходи для забезпечення збереження ресурсів автоматизованої системи управління технологічним та виробничим процесом включають:

– побудова системи захисту АСУ. Для моделювання системи інформаційної безпеки спочатку слід виділити необхідну базу даних, провести її

структурування. Структурування проводиться методом класифікації даних, що захищаються відповідно до завдань і функцій;

– затвердження вимог щодо захисту та зберігання даних в АСУ. Даний етап передбачає дослідження інформаційних ресурсів, їх структури, складу та характеристик. На підставі експлуатаційно-технічної, організаційної та розпорядчої документації затверджується регламент подальшої роботи;

– введення у дію системи АСУ. Запуск здійснюється згідно з встановленим на попередньому етапі технічним проектом. Проводяться встановлення та налагодження технічних засобів захисту інформації. Заходи щодо випробування та запуску в дію системи для зберігання даних документально фіксуються, робиться висновок, після чого проводиться запуск впроваджених захисних комплексів;

– затвердження правил для забезпечення захисту та безпечного функціонування АСУ. При розробці враховується специфіка підрозділи. Адміністратори та відповідальні за безпеку обирають найбільш оптимальний варіант захисту інформаційної бази;

– документування дій персоналу у разі виникнення непередбачених обставин. Дана документація застосовується у подальшій практичній діяльності та дозволяє вдосконалити власну нормативну базу, вести облік, планування та оптимізацію витрат;

– аналіз загроз безпеці - розглядаються можливі моделі порушників та загроз. Ризики, пов'язані з безпекою інформації, прогнозуються шляхом оцінювання мотивації та потенційних можливостей внутрішніх та зовнішніх джерел небезпеки, методів здійснення загрози. Аналізуються вразливість автоматизованої системи управління та можливі наслідки.

– розробку рекомендацій та методик, що дозволяють забезпечити збереження даних при спробі несанкціонованого доступу, витоку та розголошення.

– організацію заходів, спрямованих на безпеку. Дотримання головних принципів та простих правил полегшує виконання завдання щодо збереження

відомостей, запобігає їх втраті та дозволяє уникнути морального, матеріального та фінансового ризику.

Вся інформаційна база автоматизованої системи управління підлягає строгій класифікації.

Співробітники підприємства не мають права на поширення даних, що мають категорію вище за загальнодоступну. Користувачі автоматизованих систем управління поділяються на категорії, які визначають рівень допуску до інформаційної бази:

За даними Всесвітнього економічного форуму, у 2017 році світові збитки від кібератак становили близько трильйона доларів. За прогнозами експертів ця сума може збільшитися в рази, якщо вже сьогодні не почати вживати серйозних заходів як для оперативного виявлення, так і своєчасного реагування на атаки, причому на федеральному та регіональному рівнях

Для захисту складних автоматизованих промислових процесів на підприємствах критичної важливості необхідний комплексний підхід до забезпечення ІБ, запровадження спеціалізованих засобів, рішень та підходів. Безпека промислових мереж та АСУ здійснюється з урахуванням специфіки та особливостей таких систем, а також вимог міжнародних стандартів та російських нормативних документів щодо забезпечення ІБ. До них відносяться:

– галузеві стандарти NERC Critical Infrastructure Protection (NERC CIP);

– стандарти ISA/IEC 62443 Industrial Automation and Control Systems Security;

– рекомендації NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security»;

Комплексний підхід включає регулярний аудит стану захищеності АСУ

Усі рішення щодо забезпечення інформаційної безпеки автоматизованих систем управління технологічними процесами поділяються на дві категорії:

Система моніторингу активності, виявлення погроз та сповіщення служб безпеки. Ця система поділяється на класи:

– система виявлення комп'ютерних атак та мережевих аномалій;

– система пасивного аналізу уразливостей;

– система моніторингу подій інформаційної безпеки та бездротових мереж;

– система аналізу конфігурацій устаткування, правил доступу мережного устаткування;

– система контролю цілісності даних та ПЗ.

Система запобігання загрозам.

Системи інформаційної безпеки АСУ поділяють також на традиційні (застосовні на промислових підприємствах для побудови архітектури, управління інформаційними потоками) та спеціалізовані (актуальні для компаній важкої промисловості повинні враховувати ПЗ, промисловий трафік тощо).

Промислові системи автоматизації та управління є основними компонентами інфраструктури сучасних підприємств, що належать до різних секторів економіки (паливно-енергетичний комплекс, металургійна промисловість, хімічна промисловість та ін.) і можуть включати системи управління виробничими процесами (MES), системи диспетчерського управління і збору даних (SCADA), системи управління, побудовані на базі програмованих логічних контролерів (PLC), та ін. Забезпечення інформаційної безпеки промислових систем автоматизації та управління як критично важливих елементів бізнес-процесів є невід'ємною частиною процесу забезпечення безпеки підприємства в цілому.

В даний час, при розвитку та модернізації підприємств, у промислових системах впроваджуються уніфіковані технології (IP/Ethernet), нові сервіси (віртуалізація, IP-телефонія, мобільність та ін.), підвищується рівень автоматизації технологічних процесів та здійснюється інтеграція із системами управління підприємством (ERP). У свою чергу підвищення рівня автоматизації може призвести і до збільшення ймовірності реалізації відомих загроз, і до появи нових загроз безпеці.

Важливо, що протягом останніх десяти років спостерігається значне зростання кількості інцидентів та виявлених уразливостей, а також

цілеспрямованих атак на промислові системи автоматизації та управління, метою яких є промисловий шпигунство, шахрайство та порушення функціонування підприємства.

Забезпечення безпеки автоматизованих систем управління технологічним процесом (АСУ ТП) – складне завдання, яке потребує комплексного підходу, для вирішення якого необхідно враховувати і специфіку промислових систем (у тому числі, і використання застарілих та вразливих компонентів, протоколів, вимоги до надійності та безперервності функціонування, кліматичні умови та ін.), міжнародні стандарти та кращі практики (IEC 62443 (ISA 99), CIP NERC, NIST та ін.), вимоги регулюючих органів, спрямовані на підвищення безпеки ключових систем інформаційної інфраструктури (КСІІ): 256-ФЗ «Про безпеки об'єктів ПЕК», документ Ради Безпеки, У рамках комплексного підходу щодо забезпечення безпеки АСУ вирішуються завдання захисту інформації, що обробляється, забезпечення безперервності функціонування технологічних процесів, а також протидія шахрайствам та розкраданню.

Компанія УЦСБ (Український Центр Сталевого Будівництва) пропонує повний спектр послуг із забезпечення безпеки промислових систем автоматизації та управління:

- аудит АСУ, що включає ідентифікацію та класифікацію активів, проведення тестів на проникнення, проведення аналізу історії інцидентів, оцінку ризиків, розробку стратегії розвитку системи безпеки;
- створення комплексного рішення щодо забезпечення безпеки АСУ, включаючи роботи з обстеження, побудови моделі загроз та оцінки ризиків, формування вимог, з урахуванням міжнародних стандартів та кращих практик, розроблення проектної та робочої документації, введення в дію комплексної системи безпеки;
- сервісна підтримка, що включає комплекс послуг з технічного супроводу систем безпеки.

УЦСБ є партнером найбільших вітчизняних та міжнародних виробників і має великий штат висококваліфікованих та сертифікованих фахівців. У своїх

рішеннях компанія УЦСБ використовує передові та інноваційні розробки світових та вітчизняних виробників обладнання для побудови комплексних безпекових систем промислових систем автоматизації та управління.

Незахищені АСУ загрожують власникам великих підприємств порушенням технологічних процесів, багатомільярдними збитками та навіть техногенними катастрофами у разі несанкціонованого доступу до об'єктів управління та порушення цілісності АСУ. Своєчасне усвідомлення необхідності захисту автоматизованої системи управління технологічними процесами та вжиття комплексу заходів дозволить уникнути великих втрат і шкоди репутації.

1.2 Проблеми управління інцидентами в АСУ

На сьогоднішній момент існуючі підходи до забезпечення інформаційної безпеки елементів АСУ є недостатніми через особливості архітектури та властивості програмно-апаратного забезпечення її елементів, що надає зловмиснику кілька векторів впливу на технологічні автоматизовані системи. З розвитком інформаційних технологій та суттєвим ускладненням архітектури АСУ з'явилися множинні загрози інформаційній безпеці, реалізація яких з боку зловмисника може призвести до катастрофічних наслідків.

За період з 2008 по 2010 рік в елементах АСУ, що становлять її програмно-апаратну базу, було виявлено множинні вразливості, які можуть призвести до порушення коректної роботи технологічного процесу та реалізації загроз несанкціонованого доступу до інформації, що обробляється в:

У цьому аналітичному звіті окремо виділялися специфічні АСУ вразливості, поряд із векторами атак, які вже знайшли своє застосування щодо сучасних WEB-додатків, СУБД, компонентів операційних систем, стороннього прикладного ПЗ. Використання традиційних інформаційних технологій у елементах АСУ одна із причин низького рівня захищеності більшості їх. Даний фактор дозволяє зловмиснику апробувати існуючі знання щодо елементів АСУ, що говорить про суттєву доступність експлуатації вразливостей по відкритих

джерелах (підтверджується наявністю афішованого способу експлуатації у вигляді експлойту або Proof-of-Concept). Час усунення вразливості варіюється і було додатково вивчено під час складання звіту для уточнення можливого інтервалу перебування скомпрометованої АСУ або її елементів в аварійному стані.

Зміст звіту було побудовано виключно на загальнодоступних відомостях і фактах про інциденти інформаційної безпеки АСУ і опубліковані вразливості. Представлені вразливості на даний момент не є критичними у зв'язку з випуском оновлень безпеки для кожної з них. Додатковим джерелом походження представлених інцидентів інформаційної безпеки були спеціалізовані бази даних обліку таких інцидентів у секторі критично важливих інфраструктур зарубіжних держав:

- RISI (The Repository of Industrial Security Incidents);
- ISID (Industrial Security Incident Database).

Публікація спрямована на підвищення рівня обізнаності фахівців у галузі автоматизації технологічних процесів, співробітників підрозділів інформаційної безпеки даного сектору, фахівців із аналізу захищеності автоматизованих систем критично важливих об'єктів.

При складанні даного аналітичного звіту фахівцями НТЦ «Станкоінформзахист» використовувалася загальна система оцінки вразливостей версії 2 (CVSS v2), яка дозволяє найбільш ємко описати властивості вразливості та відповідні ризики, які вона може спричинити. CVSS v2 розбита на три групи описових метрик: базові, тимчасові та метрики оточення.

Базові метрики - описують основні властивості вразливості.

Тимчасові метрики - описують характеристики, що змінюються з часом, середовище застосування вразливості (оточення) не впливає на їх зміну.

Метрики оточення – властивості вразливості, характерні для певного середовища застосування вразливості.

До кожної групи визначені параметри, значення яких підраховуються за спеціальною методикою. Після виставлення відповідних значень результат

обчислення градуюється за шкалою від 1 до 10, пропорційною шкалою від низького рівня критичності до високого.

Для тих уразливостей, підрахунок показників CVSS v2 яких не проводився, були проведені додаткові описи з виставленням значень груп метрик за інформаційно-аналітичними ресурсами, що зафіксували появу вразливості (стрічки уразливостей «Bugtrack», ресурси технічної підтримки користувачів на офіційних сайтах).

Якщо значення показників наслідків експлуатації вразливостей мають те саме значення, розрахунок і застосування показників Bias не проводиться. Показник Bias використовується для виділення та додаткової градації збитків щодо конфіденційності, цілісності та доступності.

Після визначення властивостей уразливостей у програмних продуктах елементів АСУ проводився порівняльний аналіз загроз реалізації НСД щодо АСУ з використанням:

- організації апробації вразливості у стендових умовах лабораторії;
- аналізу категорії безпеки (КБ, SC) та відповідної сумарної шкоди (Impact), яка може бути завдана інформаційній системі на прикладі інформаційних систем федерального рівня зарубіжних держав відповідно до документа FIPS 199 «Standards for Security Categorization of Federal Information and Information Systems» [3].

В основі методики лежить опис збитків від впливу на кожну із складових інформаційної системи за критеріями показників розкриття конфіденційності, порушення цілісності та доступності.

Значення показників завданих збитків:

- низький рівень шкоди (НИЗЬКИЙ, розкриття конфіденційності, порушення цілісності та доступності спричиняють несуттєві, обмежені або запобіжні наслідки);
- середній рівень шкоди (СЕРЕДНІЙ, розкриття конфіденційності, порушення цілісності та доступності тягнуть за собою суттєві негативні

наслідки щодо діяльності Власника інформаційної системи, її користувальницьких активів);

- високий рівень шкоди (ВИСОКИЙ, розкриття конфіденційності, порушення цілісності та доступності спричиняють катастрофічні наслідки).

Приклад FIPS 199: система диспетчеризації та розподілу електроенергії військового формування.

Система SCADA електроенергетичної підстанції, термінали накопичення даних про розподіл енергії, рознесені територією. Система SCADA обробляє інформацію з боку терміналів накопичення даних (показники рівня енергії, кількісна оцінка, інформація про відмови), так і звичайну службову інформацію.

КБ дані терміналу = {(конфіденційність, НЕ ВИЗНАЧЕНИЙ), (цілісність, ВИСОКИЙ), (доступність, ВИСОКИЙ)},

КБ службова інформація = {(конфіденційність, НИЗЬКИЙ), (цілісність, НИЗЬКИЙ), (доступність, НИЗЬКИЙ)}.

Результуюча категорія безпеки інформаційної системи:

КБ система SCADA = {(конфіденційність, НИЗЬКИЙ), (цілісність, ВИСОКИЙ), (доступність, ВИСОКИЙ)}.

Власником інформаційної системи може бути змінено будь-який із показників категорії, відповідно до загрози розкриття даних про перебіг технологічного процесу, особливостей архітектури технологічної мережі критично важливого об'єкта, що входить до складу ключових інфраструктур зарубіжної держави, показник заподіяння шкоди щодо конфіденційності системи SCADA було змінено на « СЕРЕДНІЙ»:

КБ система SCADA = {(конфіденційність, СЕРЕДНІЙ), (цілісність, ВИСОКИЙ), (доступність, ВИСОКИЙ)}.

Ця результуюча категорія системи диспетчеризації була взята за основу при описі можливих наслідків реалізації загроз НДД до інформації, що обробляється в АСУ .

Огляд виявлених уразливостей протягом чотирьох років разом з аналізом згруповань в табл.1.1.

Таблиця 1.1.

Статистика виявлених уразливостей в елементах АСУ (2016-2020 р.)

Назва продукту	Тип уразливості	Опис вразливості	Доповнення
DATAC RealWin 2.0 (Система диспетчеризації)	Виконання довільного коду авторизованим користувачем	Переповнення стека при обробці спеціально сформованого FC_INFOTAG/SET_CONTROL пакета, спрямованого на прийом у TCP-порт 910 дистанційної системи	Дата виявлення – 2008 рік. Доступний повнофункціональний код, що експлуатує.
GE Fanuc Proficy Information Portal 2.6 (WEB-додатки для аналізу виробничих даних)	Завантаження та виконання довільних файлів	Автентифікований користувач може завантажити будь-який довільний файл на сервер, використовуючи сценарій «Add WebSource», потім виконати його шляхом звернення до WEB-сервера. Ця вразливість може призвести до несанкціонованого розміщення на WEB-сервері програмних закладок класу WEB-shell	Дата виявлення – 2008 рік. Вразливість викликана через небезпечне використання Java RMI виклику до вказаного сценарію WEB-програми, який дозволяє задати ім'я файлу та каталог, куди буде розміщено файл.
ABB PCU400 4.4-4.6 (Блок зв'язку)	Неавторизоване виконання довільного коду	Дистанційне переповнення буфера в модулі обробки протоколів IEC60870-5-101, IEC60870-5-104	Дата виявлення – 2008 рік. ABB PCU 400 є FEP-сервером системи диспетчеризації ABB SCADA, що відповідає за керування підсистемою телеметричних пристроїв.
GE Fanuc Cimplicity 6.1 (Система диспетчеризації)	Неавторизоване виконання довільного коду	Видалене переповнення купи, яке може експлуатуватися віддаленим зловмисником за доступності системи «ззовні»	Дата виявлення – 2008 рік. На 2007-2008 рік цей продукт був єдиним, який підтримував інтеграцію з обладнанням

Назва продукту	Тип уразливості	Опис вразливості	Доповнення
			ЧПУ сімейства GE Fanuc.
AREVA e-terrahabitat (Система диспетчеризації)	Множинні вразливості, що призводять до відмови в обслуговуванні, підвищення привілеїв	Успішна експлуатація вразливості виводить із ладу WEB-сервер WebFGServer, платформу NETIO. Підвищення привілеїв у середовищі WEB-сервера та програми MLF	Дата виявлення – 2009 рік. Активно використовують на малих об'єктах нафтогазового сектора.
OSISoft PI Server (OPC-сервер)	Розкриття критичних даних для доступу до бази даних	Зловмисник може розкрити дані, що передаються під час автентифікації кінцевого клієнта до бази даних	Дата виявлення – 2009 рік. Для усунення вразливості рекомендується використовувати IPSec між клієнтами мережі
CitectSCADA (Система диспетчеризації)	Неавторизо ване виконання довільного коду	За наявності запущеного ODBC-сервера (TCP-порт 20222) віддалений зловмисник може скомпрометувати цільову систему	Дата виявлення – 2008 рік. Для усунення вразливості рекомендується не використовувати службу ODBC
Контролери Rockwell Automation (Allen Bradley) Micrologix 1100/1400 (віддалений термінал)	Відмова в обслуговуванні, несанкціонован ий доступ із можливістю підвищення привілеїв	Множинні вразливості, що призводять до можливості несанкціонованої модифікації PLC, пізнання сторонніх пристроїв	Дата виявлення – 2010 рік. Контролери Micrologix є однією з найпоширеніших платформ для систем керування з програмованою логікою
WonderWare SiteLink version 2.0, WonderWare InTouch version 8.0 (Система диспетчеризації)	Відмова в обслуговуванні	Експлуатація вразливості призводить до позаштатного порушення коректної роботи системи та її відключення.	Дата виявлення – 2008 рік. Системи Intouch є одними з найпоширеніших систем SCADA

Окремою загрозою, що частково використовує штатні методи для виконання, є поширення зловмисного коду для крадіжки критично важливих даних про проекти технологічних процесів та порушення їх коректної роботи, підтвердження чого є факт поширення шкідливого коду Rootkit.TmpHider і Scope.Rookit.Tmp. Багато популярних систем диспетчеризації (SCADA) базуються на платформі ОС Microsoft Windows, тому цей факт вказує на необхідність забезпечення інформаційної безпеки операційної системи, на яку встановлюється прикладне програмне забезпечення.

Названі зразки шкідливого коду використовували вразливість MS10-046 (http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx) у Windows Shell, що дозволяє неавторизовано виконати довільний код за допомогою відображення спеціально сформованого ярлика оболонки ОС Windows. Основним методом поширення було застосування відокремлюваних носіїв (USB-flash, Compact-Flash, сторонні знімні носії інформації), які можуть використовувати Оператори для управління проектами технологічних процесів, обміну інформацією між собою.

1.3 Класифікація інцидентів у автоматизованих системах управління

Класифікація інцидентів у автоматизованих системах управління допомагає категоризувати події та проблеми, які виникають у процесі функціонування таких систем. Це важливий етап для кращого розуміння та управління безпекою, надійністю та ефективністю АСУ. Інциденти можуть бути класифіковані на різні способи, але ось декілька загальних категорій для класифікації інцидентів в АСУ:

Перелік категорій кіберінцидентів (далі – Перелік) розроблений з використанням та відповідає рекомендації Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy, січень 2018 року), а також спільному документу ENISA та Європейського центру боротьби з

кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs).

Перелік призначений для впровадження єдиної таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

Перелік може застосовуватись суб'єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, наведених у цьому документі.

Перелік має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб'єктів забезпечення кібербезпеки.

Суб'єкти забезпечення кібербезпеки при обміні та поширенні інформації про кіберінциденти, підготовці звітів і публічних повідомлень про кіберінциденти застосовують Перелік.

Цей перелік є обов'язковим для основних суб'єктів забезпечення кібербезпеки при реєстрації, обліку та обміні інформацією про кіберінциденти, передачі звітів до НКЦК, зокрема із використанням автоматизованих платформ обміну інформацією про кіберзагрози.

У випадку, коли на початковій стадії реагування кіберінцидент може бути віднесений до декількох категорій (табл.1.2), вибирається категорія із більшим рівнем загрози.

Таблиця 1.2.

Класифікація інцидентів

Код	Категорія інциденту	Назва інциденту
01	Шкідливий (образливий) вміст (Abusive content)	Спам
		Образливий контент
		Шкідливий контент
Код	Категорія інциденту	Назва інциденту
02	Шкідливий програмний код (Malicious Code)	Вірус
		Хробак
		Троян

Код	Категорія інциденту	Назва інциденту
		Шпигунське програмне забезпечення
		Діалер
		Руткіт
		Шкідливе програмне забезпечення
		Управління ботами
		Програма здирник
		Конфігурація шкідливого програмного забезпечення
		Командно-контрольний центр
03	Збір інформації зловмисником (Information Gathering)	Сканування
		Перехоплення і аналіз мережевого трафіку
		Соціальна інженерія
04	Спроби втручання (Intrusion Attempts)	Експлуатація відомих вразливостей
		Спроби авторизації
		Експлуатація раніше невідомих вразливостей
05	Втручання (Intrusion)	Компрометація привілейованого облікового запису
		Компрометація непривілейованого облікового запису
		Компрометація застосунку
		Бот
		Дефейс
		Компрометація системи
		Бекдор
06	Порушення доступності (Availability)	Атака на відмову в обслуговуванні
		Розподілена атака на відмову в обслуговуванні
		Саботаж, диверсія
		Збій без участі зловмисника
07	Порушення властивостей інформації (Information Content Security)	Несанкціонований доступ до інформації
		Несанкціоноване внесення змін до інформації
		Сервер з публічними правами на запис
08	Шахрайство (Fraud)	Несанкціоноване використання ресурсів
		Порушення авторських прав
		Маскарадинг
09	Відома вразливість (Vulnerable)	Вразливості, відкриті для експлуатації
10	Інше (Other)	Чорний список
		Недостатньо даних
		Інше

Небажаний контент, в тому числі расистський чи ксенофобний матеріал, погрози особі чи групі осіб.

Шкідливий контент, в тому числі дитяча порнографія, насильство, пропаганда.

Спроба компрометації чи пошкодження функціонування системи або сервісу шляхом експлуатації вразливостей, які мають стандартизований ідентифікатор (наприклад, CVE).

Численні спроби авторизації: підбір паролів, злам паролів і т.п..

Використання раніше невідомих вразливостей і експлойтів.

Зловмисники використовують сервери з правами на запис для тимчасового збереження викраденої із скомпрометованих систем інформації, в тому числі даних кейлогерів, скомпрометованих облікових даних і т. ін.

Використання копії ідентифікаторів суб'єкта або системи, в тому числі крадіжка особистості.

Інциденти, які не відносяться до будь-якого вищезазначеної категорії.

РОЗДІЛ 2
АНАЛІЗ ВПЛИВУ ІНЦИДЕНТІВ НА ЕФЕКТИВНІСТЬ УПРАВЛІННЯ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

2.1. Типи інцидентів та їх класифікація

Інцидент кібербезпеки може статися в будь-якій компанії незалежно від її штату та діяльності. Подібні ситуації можуть мати випадковий і заздалегідь підготовлений характер. У будь-якому випадку вони становлять потенційну небезпеку для репутації організації, несуть ризики фінансових збитків та розголошення конфіденційної інформації.

Причини інцидентів кібербезпеки в організації:

Неуважність та помилки персоналу компанії. Це одна з головних причин витоку конфіденційної інформації, наслідки якої складно спрогнозувати, як і збитки. Незаблокований монітор робочого комп'ютера з відкритою документацією, спільні паролі для всіх, нехтування захищеними каналами зв'язку та шифрування даних, загальний доступ до важливих файлів здатні призвести до численних ризиків.

Події інсайдерів. Власні співробітники організації нерідко мають на меті збагачення або отримання особистої вигоди, використовують своє службове становище та можливості проти власного роботодавця. Передача конфіденційних відомостей конкурентам, розкриття рекламних кампаній та методів роботи організації, змова з партнерами або шантаж власних колег здатні запустити цілий ланцюжок несприятливих сценаріїв.

Спрямовані хакерські атаки. Підготовлені дії зловмисників, спрямовані на конкретні цілі та жертви. Як правило, це особливо важлива інформація на кшталт фінансової звітності, розробки та ноу-хау компанії, бізнес-плани, відомості, що відкривають доступ до активів компанії.

Як підготуватися та діяти при виявленні інциденту кібербезпеки?

Спочатку необхідно оцінити потенційні ризики для організації та бізнесу. У кожній ніші є своя специфіка та найбільш уразливі місця. Найбільш типовими загрозами є шкідливе програмне забезпечення, DDoS-атаки, фішинг, уразливості використовуваних додатків, внутрішні загрози. Як правило, пріоритетними є 2-3 види загроз, і саме до них потрібно готуватись.

Розставити пріоритети та оцінити клас загрози інциденту кібербезпеки. При цьому враховують ступінь серйозності та масштаб події. Одні інциденти, як, наприклад, заражений і втрачений файл несе локальний ризик, тоді як DDoS-атака здатна вивести з ладу сайт організації та уповільнити робочі процеси. Пріоритизація ризиків та використання інструментів для їх оцінки дозволяють швидше і точніше реагувати на виявлену загрозу або негативну подію, що сталася.

Створити алгоритм реагування інцидент безпеки. Щоб швидше усунути загрозу та мінімізувати збитки, дуже важливо реагувати якнайшвидше і діяти за чітко визначеною схемою. Нейтралізація інциденту ведеться послідовними кроками, де співробітники компанії та служби безпеки виконують конкретні дії та несуть за них відповідальність.

Проінструктувати персонал і провести репетицію заходів у відповідь на інцидент. Кожен співробітник компанії має бути навчений, підготовлений до позаштатних ситуацій. Це дозволить йому діяти, а не чекати, аніж усе закінчиться. Відповідно до ролі та повноважень, за персоналом необхідно закріпити правила поведінки та заходи у відповідь на інцидент. Оптимально періодично проводити реальний тест-драйв для того, щоби співробітники мали практичний досвід.

Регулярно оновлювати та вдосконалювати план реагування на кіберінциденти. Загрози та методи зловмисників не стоять на місці. Вони стає складнішими і скритнішими, що потребує оновлення та вдосконалення захисту. Для цього потрібно використовувати релевантний досвід, останні розробки в галузі кібербезпеки, актуальне програмне забезпечення та захисні системи.

Які інструменти використовують для виявлення та запобігання інцидентам кібербезпеки?

Засоби захисту веб-трафіку (наприклад, Solar WebProxy).

Системи виявлення та запобігання вторгненням.

Антивірусне ПЗ.

Сканери вразливостей.

Комплексні системи запобігання витоку даних, які ведуть регулярний збір інформації та допомагають керувати інформаційною безпекою в компанії (DLP, SIEM-системи).

Оптимально задіяти якнайбільше інструментів, щоб охопити все інформаційне середовище організації та не пропустити прихованих загроз. Як інструмент моніторингу та запобігання внутрішнім загрозам використовуються DLP-системи, наприклад, Solar Dozor. Він захистить від витоків інформації, надасть детальну статистику щодо робочих процесів та дій користувачів та їх аномальної поведінки.

Шкідливе програмне забезпечення або «Малварь», скорочено від англійського «шкідливе програмне забезпечення» - шкідливе програмне забезпечення, яке має своєю метою в тій або іншій формі завдати шкоди користувачу або комп'ютеру та його вмісту. Малварь - загальна назва для всіх видів кібер-загроз, таких як: віруси, трояни, шпіонські програми, кейлогери, рекламне ПЗ та ін. Шкідливі програми або шкідливі програми - достатній вид кібер-загрози, і стикнутися з шкідливим ПО може кожен.

Рекламні програми або програми, існуючі за рахунок демонстрації реклами, відображають небажану, а іноді і корисну рекламу на екрані пристроїв, перенаправляють результати пошуку на рекламних сайтах і збирають дані користувачів, які можна продати рекламодавцям без згоди самих користувачів. Не всі рекламні програми є шкідливими, деякі з них легальні та безпечні у використанні.

У більшості випадків користувачі можуть впливати на частоту показу рекламних програм і на дозволені види завантажень за допомогою елементів

управління у вікнах, що відкриваються, налаштувань браузерів, а також за допомогою блокувальника реклами.

Шпіонські програми – це різновиди шкідливих програм, що відкриваються на пристрої, відстежують активність і здійснюють крадіжку конфіденційної інформації: фінансових даних, облікових записів, даних для входу та інших даних. Шпіонські програми можуть поширюватися через уразливість програмного забезпечення, бути пов'язаними з легальними програмами або бути частиною троянських програм.

Програми-вимагателі – це корисні програми, що здійснюють блокування або відмову доступу користувачів до системи або даних до моменту виплати викупу.

Програми-шифрувальники – це тип програм-виконавців, що виконують шифрування файлів користувача і вимагають оплати в певний термін і часто в цифровій валюті, наприклад, в біткойнах. Програми-виконавці вже багато років представляють загрозу для компаній усіх відростків (рис.2.1-2.3). За мірою того, як всі компанії більше переходять на цифрові технології, ймовірність стати жертвою нападу програм-вимагателем значно зростає.

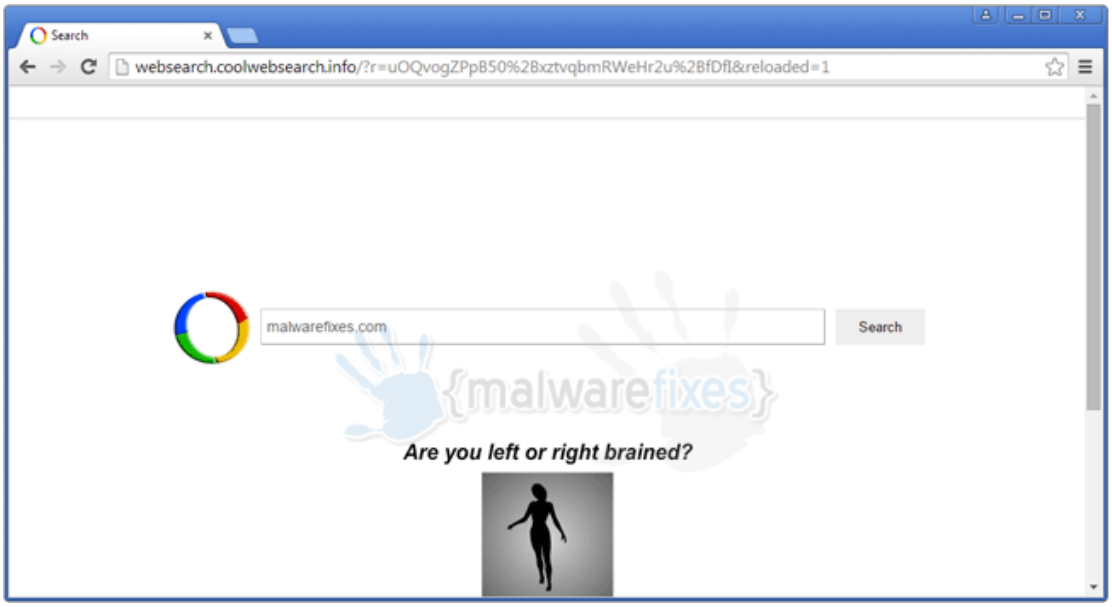

Рис. 2.1. Інтерфейс шпигунської пошукової системи CoolWebSearch

Рис. 2.2. Інтерфейс програми CryptoLocker

Рис. 2.3. Інтерфейс програми Phobos

Троянські програми маскуються під легальне програмне забезпечення, щоб обманом задати користувачам запустити шкідливі програми на комп'ютері. Оскільки вони виглядають досить надійними, користувачі завантажують їх, непередбачено заражаючи свої пристрої шкідливими програмами. Троянські програми – це, свого роду, точки входу зловмисників у систему. В відміну від червей, їм для роботи необхідно пристрій. Після встановлення троянської програми на пристрої зловмисники можуть використовувати її для видалення, редагування та збору даних з пристроїв у рамках ботнету, а також для слідки за пристроями та отримання доступу до мережі.

Черви – це один із найбільш часто зустрічаються типів шкідливих програм, що поширюються комп’ютерними мережами, використовуючи вразливості операційної системи. Черви представляють собою окремі програми, що поширюються шляхом самокопіювання зі сторони захисту інших комп'ютерів, при цьому ніяких дій з користувачами або зловмисниками не потрібно. Завдяки можливості швидкого поширення, черви часто використовуються для виконання фрагментів коду, створеного для пошкодження системи, наприклад, вони можуть видаляти файли в системі, шифрувати дані для атак програм-виконавців, красти інформацію та створювати ботнети.

Вірус – це фрагмент коду, який встановлюється в додаток і запускається при його запуску. Попавши в мережу, вірус може використовуватися для збереження конфіденційних даних, запуску DDoS-атак або атак програм-виконавців. Звичайний вірус поширюється через заражені веб-сайти, при спільному доступі до файлів, при завантаженні заражених внесених електронних листів. Вірус не діє в момент активації зараженого файлу або програми. Після цього вірус починає поширюватися в системі.

DoS-атака (Denial of Service) - буквально "відмова в обслуговуванні". Це тип атаки, в якому шахраї нападають з метою викликати навантаження підсистеми сервісу. У цьому випадку комп'ютер (або комп'ютери) використовується для заповнення сервера пакетами TCP та UDP.

Простота координації DoS-атак означає, що вони стали однією з найпоширеніших загроз кібербезпеці, з якими стикаються сучасні організації. DoS-атаки прості, але були дуже ефективними у 90 роки. Нині ж вони перетворилися на DDoS-атаки і можуть завдати нищівних збитків компаніям або приватним особам, на яких вони спрямовані. Однією атакою організація може бути виведена з ладу на кілька днів і навіть тижнів.

DDoS-атака (Distributed Denial of Service) - по суті, це та сама DoS-атака, але реалізована з декількох машин на один цільовий хост. Складність захисту від цього виду нападу залежить кількості машин, з яких здійснюється відправка трафіку, тому цей тип атаки займає важливе місце в арсеналі хакерів.

Під час DDoS-атаки виникають великі складнощі з виявлення її джерела, так як хакер використовує цілу мережу пов'язаних між собою машин або ботів. Традиційно атаки ведуться із заражених вірусами комп'ютерів звичайних користувачів, які навіть не підозрюють, що стали мимовільними учасниками правопорушення. Але нещодавно з'явився новий спосіб - проводити атаки за допомогою IoT пристроїв (розумні чайники, кавоварки, пилососи та інша техніка). Справа в тому, що раз у розумних гаджетів є доступ в інтернет, а значить, є і можливість брати участь в DDoS-атаці (рис.2.4).

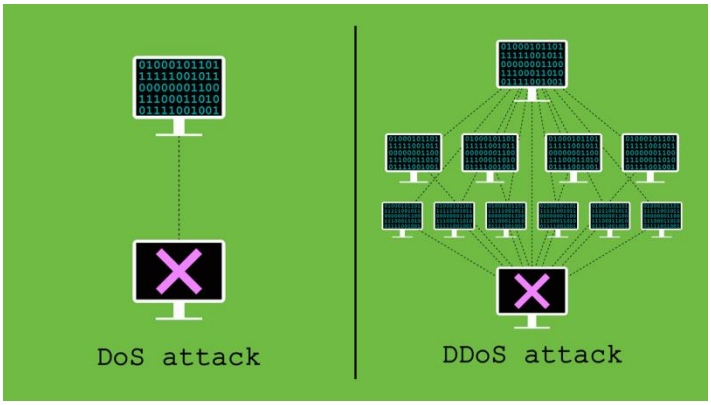

Рис. 2.4. Різниця між DoS DDoS

Ці комп'ютери та техніка утворюють ботнет – єдину мережу, якою керує зловмисник –ботмайстер, з головного контрольного сервера (C&C). Подібна

структура дозволяє хакеру координувати атаки одночасно з кількома системами, чисельність яких коливається від десятків до мільйонів пристроїв.

Перехоплення автентифікації відноситься до несанкціонованого доступу до облікового запису користувача зловмисником, який краде ваші облікові дані для входу або ідентифікатор сеансу. Потім зловмисник може використовувати цю інформацію, щоб отримати доступ до облікового запису користувача та виконувати дії від його імені без його відома. Цей тип атаки зазвичай здійснюється з допомогою таких методів, як фішинг, фіксація сеансу або атаки типу "людина посередині". Як тільки зловмисник отримує доступ до облікового запису користувача, він потенційно може вкрасти конфіденційну інформацію, зробити несанкціоновані покупки або участь в інших шкідливих діях.

Як тільки зловмисник отримує доступ до облікового запису користувача, він потенційно може отримати доступ до конфіденційної інформації, такої як особисті дані, фінансова інформація або ділова конфіденційна інформація. Зловмисник може використовувати цю інформацію для крадіжки особистих даних, фінансового шахрайства або корпоративного шпигунства.

2.2 Аналіз існуючих процедур та методів управління інцидентами

Сучасні комп’ютерні мережі потребують високого рівня захищеності від вторгнень (неавторизованого доступу або мережної атаки). Як правило для цього використовуються системи виявлення та попередження вторгнень (IDS/IPS).

Система виявлення вторгнень (СВВ) (Intrusion Detection System) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп’ютерну систему або мережу.

Система запобігання вторгненням (СЗВ) (Intrusion Prevention System)) – програмний або апаратний засіб, який здійснює моніторинг комп’ютерної

системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

Проведені дослідження виявили, що IDS все частіше стають необхідним доповненням інфраструктури мережевої безпеки. На додаток до міжмережевих екранів (firewall), робота яких відбувається на основі політики безпеки, IDS служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які обійшли Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від IDS існує і не маленька. Зазвичай IDS включає: Сенсорну підсистему, призначену для збору подій, пов'язаних з безпекою мережі або системи, що захищається; Підсистему аналізу, призначену для виявлення мережевих атак і підозрілих дій; Сховище, в якому накопичуються первинні події і результати аналізу; Консоль управління, що дозволяє конфігурувати IDS, спостерігати за станом системи, що захищається і IDS, переглядати виявлення підсистемою аналізу інцидентів. За способами моніторингу IDS системи підрозділяються на network-based (NIDS) і host-based (HIDS). Що ж стосується IPS, то вони щодо класифікації та за своїми функціями є аналогічними IDS. Головна їхня відмінність полягає в тому, що вони функціонують в реальному часі і можуть в автоматичному режимі блокувати мережеві атаки. Кожна IPS включає в себе модуль IDS.

Таким чином, розвиток систем виявлення та попередження вторгнень у комп'ютерні мережі є актуальною задачею, яка потребує відповідних програмних та апаратних реалізацій, які можуть модифікуватися з появою нових загроз.

Управління інцидентами (IM) – це процес, який IT-команди використовують для реагування на незаплановані перерви в обслуговуванні. Несподівані збої виникають через такі інциденти, як втрата або погіршення підключення до мережі, невиконання запланованого завдання (наприклад, резервного копіювання) або непрацездатність API. Процес управління

інцидентами спрямований на швидке відновлення нормальної роботи IT-сервісу та мінімізацію впливу на компанію. У ході цього процесу команда виявляє та розслідує інциденти, усуває проблеми та документує кроки, зроблені для відновлення роботи сервісу.

Які події вимагають керування інцидентами?

Термін «управління інцидентами» використовується не лише у IT-сфері. За її межами з управлінням інцидентами можна зустрітись у таких галузях, як аварійно-рятувальні служби, управління великими заходами, експлуатація підприємств.

У разі управління інцидентами сфокусовано на управлінської діяльності, що стосується якості обслуговування і обслуговування клієнтів.

Інциденти в рамках управління інцидентами можна визначити як непередбачувані події, які призводять до зниження очікуваної або узгодженої якості послуг IT. Масштаб інциденту може бути невеликим або великим і можна вказати ступінь критичності. Наприклад, зниження якості обслуговування може бути мінімальним і обмежуватись конкретним географічним положенням, або сервіс може повністю перестати працювати у багатьох регіонах.

Під проблемою мається на увазі основна причина інциденту, яка виявляється після подальшого розслідування. Для вирішення інциденту необхідно знайти проблему. Наприклад, якщо веб-сервер працює повільно, проблема може полягати в неправильній конфігурації маршрутизатора в центрі обробки даних або обірваному мережевому кабелі на периметрі.

Для керування інцидентами використовується набір документованих процесів, які чітко визначають, що необхідно зробити, щоб мінімізувати негативні наслідки та тривалість збоїв у роботі IT. Крім технічного управління помилками цей процес також включає управління очікуваннями клієнтів, користувачів і зацікавлених сторін під час інциденту.

Існують різні платформи, які організації використовують із моделювання методів управління інцидентами. Двома прикладами є методи управління інцидентами з Бібліотеки IT-інфраструктури (ITIL) 4 та платформа кібербезпеки

Національного інституту зі стандартизації та технології (NIST). Ці платформи можна використовувати в існуючому вигляді або в розширеному, адаптувавши їх до свого унікального бізнес-середовища, послуг, стандартів комунікації з клієнтами та зацікавленими сторонами (рис.2.5).

Програмне забезпечення для управління інцидентами часто використовується, щоб розгорнути в організації платформу. Конкретно використовувана платформа залежить від послуг.

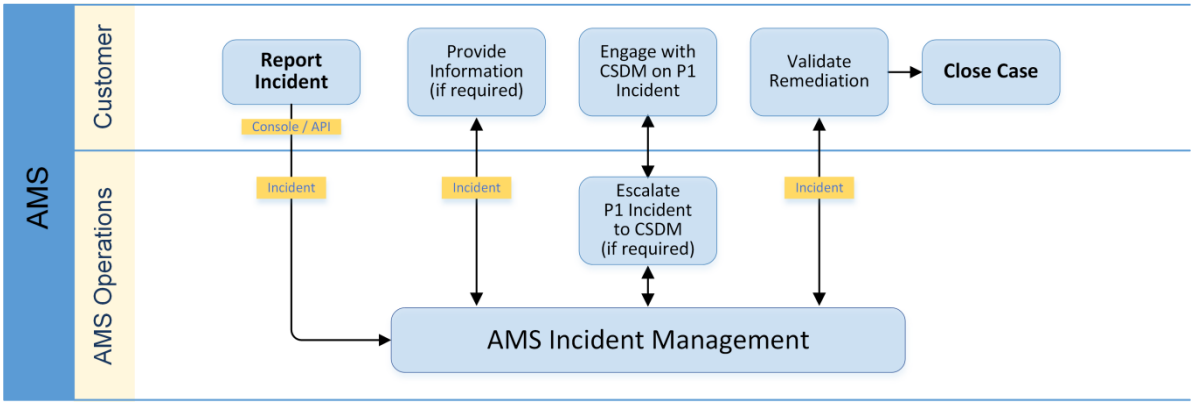

Рис. 2.5. Система управління інцидентами AMS Incident Management

Найкращі практики допомагають організаціям працювати на найвищому рівні в рамках певного бізнес-підрозділу чи стратегічної галузі. Наслідуючи передові практики в системах управління інцидентами, ви можете надавати своїм клієнтам найкращий сервіс.

Ви повинні мати можливість класифікувати інциденти відповідно до їх пріоритету та серйозності, щоб визначити терміни, заходи щодо усунення несправностей та розслідування. Стратегії ескалації слід застосовувати у таких випадках: якщо реагування на інциденти не виправдало очікувань або якщо стався серйозний інцидент високого ступеня пріоритетності чи серйозності. Без цих стратегій, ваша команда може витрачати час на те, щоб вирішувати, з ким зв'язатися і що робити.

Зацікавлені сторони, від IT-відділу до кінцевих користувачів, повинні бути в курсі інциденту. Також важливо мати чіткі канали зв'язку, щоби постраждалі

знали, куди звертатися за новою інформацією чи повідомляти про нові інциденти. Завдяки чіткому комунікаційному плану ви зможете завоювати довіру та уникнути непотрібних звинувачень. Критичні інциденти завжди вирішуються дипломатичним шляхом.

Після усунення інциденту слід провести аналіз першопричин, щоб зрозуміти, чому інцидент взагалі стався. Це допомагає виявити прогалини або вразливості в системі, які можна усунути, щоб запобігти подібним інцидентам у майбутньому. Уроки, зроблені з кожного інциденту, допомагають постійно вдосконалювати IT-інфраструктуру та процеси.

Хаотичний інжиніринг – це дисципліна в галузі розробки програмного забезпечення, в якій системи навмисно зазнають деструктивних умов, таких як збої серверів, затримки мережі або обмеження ресурсів. Впровадження хаосу в системи перевіряє їхню стійкість, а також зміцнює процеси реагування на інциденти та управління ними всередині організації. Цей метод аналогічний використанню етичного злому під час управління інцидентами кібербезпеки.

2.3 Вплив інцидентів на функціонування автоматизованих систем

Останні кілька десятиліть намітилися тенденції автоматизації процесів виробництва. На багатьох підприємствах запроваджуються автоматизовані засоби управління операціями виробничого циклу, технічного процесу (ТП). Це спричиняє значне збільшення обсягів оброблюваної інформації. З розвитком технологій автоматизовані системи управління технологічними процесами поступово перетворилися із закритих керуючих пристроїв на багаторівневі промислові мережі на базі стандартних мережевих протоколів, які мають безліч подібностей з корпоративними мережами, що активно використовуються. На жаль, це стосується й уразливостей, які тісно пов'язані із загрозами кібербезпеці. Ці мережі схильні до зараження шкідливими програмами, злому, виведення з ладу ПЗ та інших видів зовнішнього впливу. Це істотно впливає на виробничі

процеси, і з кожним роком кількість подібних інцидентів збільшується. Класифікація та способи атак на АСУ. Хто і навіщо втручається у технологічні процеси? Фахівці з інформаційної безпеки виділяють кілька типів порушників для АСУ: ворожі держави та їхні силові структури, терористичні організації, промислові шпигуни та представники організованих злочинних груп, хакери-активісти. Дії кіберпідрозділів силових структур ворожих держав спрямовані на порушення функціонування об'єктів інфраструктури, що може призвести до руйнувань та людських жертв. Даний вид атак є одним з найнебезпечніших при кібервійнах.

Фахівці вважають, що найближчими роками він буде найпоширенішим. Людство вже бачило його застосування на практиці: між 2009 та 2011 роками відбувалася так звана операція Stuxnet, під час якої американські спецслужби за допомогою комп'ютерної програми-хробака порушували роботу іранських заводів зі збагачення уранового палива. На рис. 2.6. показана статистика впливу різних видів інциденту на АСУ.

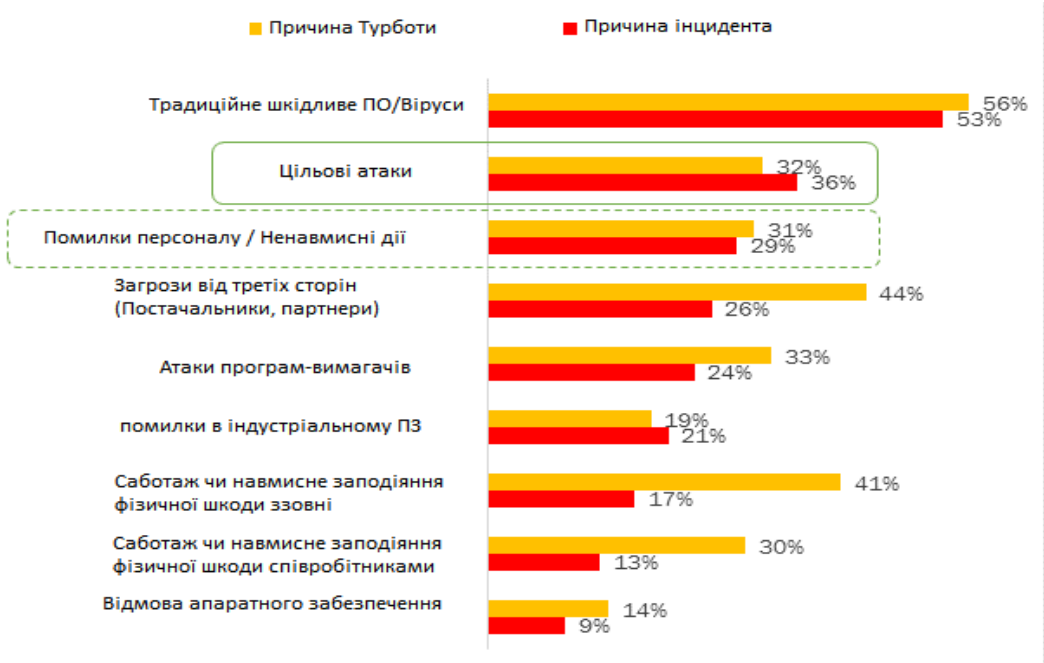

Рис. 2.6. Статистика впливу різних видів інцидентів на АСУ

Основною метою терористів є паніки серед населення. Оскільки традиційні теракти мають більший резонанс у суспільстві, ніж проведення

кібератак, такий вид впливу в найближчому майбутньому навряд чи часто зустрічатиметься. Промислові шпигуни та представники ОЗУ здійснюють атаки для отримання прибутку. Їх дії призводять до підриву інфраструктури, що зазвичай вигідно конкурентам, і навіть до порушення безпеки даних. Хактивістами є налаштовані проти держави люди. Їхні акції рідко завдають істотних збитків і використовуються в основному для донесення порушниками власних політичних поглядів. Найбільших збитків промисловій інфраструктурі завдають дії хакерів – через численність цієї групи. Ці операції переслідують різні мети: від виявлення вразливостей їхнього подальшого усунення до маніпулювання приладами обліку з метою крадіжки готової продукції.

Існує ще одна категорія порушників, які мають доступ до обладнання, що полегшує процес порушення інформаційної безпеки. Це – співробітники, які виявили службову недбалість або скривджені на начальство, а також інсайдери, спеціально впроваджені у виробничі компанії. Відомі випадки, коли працівники грали в комп'ютерні ігри або дивилися відео на робочому обладнанні, налаштовували вихід в інтернет та підключали до мережі особисті пристрої. Назвемо основні методи атак АСУ.

Найпоширеніший спосіб - безпосереднє відправлення команд обладнання. Більшість програмного забезпечення, що використовується в промисловості, не вимагає ідентифікації користувача. Зловмисникам достатньо проникнути в технологічну мережу підприємства та встановити зв'язок із потрібним об'єктом. За допомогою спеціальних утиліт злочинці можуть перехопити керуючий екран. У цьому випадку всі рухи курсору, що здійснюються ними, будуть видно оператору, а самі зловмисники будуть обмежені правами активного користувача. У деяких випадках внесення правок до бази даних дозволяє також змінити та пов'язані з нею об'єкти.

Технологія Man-in-the-Middle використовується у випадках, коли зловмисникам відомі параметри функціонування мережі. Тоді вони можуть змінювати інформацію на головному екрані та отримати повний контроль над

будь-якою системою. Зламування датчиків виробництва та подача на них неправильних даних для перешкоджання коректній роботі обладнання.

Об'єктом несанкціонованого доступу до технологічної мережі може стати будь-яке підприємство чи його структурний підрозділ. Засоби для проведення подібних атак підбираються з урахуванням особливостей систем, що атакуються, і зазвичай мають вузькоспеціалізовану дію.

Практика показує, що зловмисники мають обладнання та програмне забезпечення для проведення цільових нападів, при цьому можливий одночасний вплив на різні блоки та комбінування спеціально створених та загальнодоступних засобів. Стандартна АСУ зазвичай складається із двох або трьох мережевих рівнів. Багато підприємств використовують середовище для управління виробничими процесами, що об'єднується у загальну корпоративну ЛОМ з підрозділами, що керують фінансовою та організаційною діяльністю компанії.

Непоодинокі випадки, коли до локальної технологічної мережі підключені відділи постачання та продажу. Самі АСУ на верхньому рівні мають станції інженерів та операторів, а також сервери. На середньому рівні розташовані програмовані контролери, а на нижньому знаходяться виконавчі механізми та підключені безпосередньо до обладнання датчики. Зв'язок між різними рівнями забезпечується комутаційними вузлами, а доступ до датчиків здійснюється через польові шини за спеціальними протоколами: Modbus, Profibus, Foundation Fieldbus, DeviceNet, HART та багато інших. Зазвичай їх розробники не передбачають встановлення додаткових засобів захисту.

Часто на верхніх рівнях архітектури використовуються IP- та Ethernet-мережі, а промислові пристрої постачаються стандартними портами та використовують загальні протоколи. Найімовірніше, атаки будуть спрямовані на галузі, де перебої в роботі компонентів можуть призвести до найбільших збитків та людських жертв. Це – підприємства ПЕК та енергетичні компанії, транспорт, інші організації, порушення діяльності яких має економічні наслідки та може спровокувати катастрофу у гуманітарній чи екологічній сфері.

Дослідження показують, що для виявлення проведених кібератак може знадобитися від кількох місяців до трьох років (див., наприклад, дослідження Positive Technologies). Максимальний зафіксований термін присутності зловмисників у закритій системі становить 7 років. Через 10-14 днів після проникнення виявити зламані компоненти стає складніше, оскільки злочинці починають застосовувати діючі облікові записи та штатні засоби адміністрування.

Встановлені системи захисту можуть ідентифікувати подію як вірусну атаку, для усунення якої виконують перевірку антивірусами, форматують жорсткі диски і встановлюють ОС. Це призводить до знищення доказів атаки, які могли б допомогти надалі. АСУ працюють за спеціальними мережевими стандартами і повинні забезпечувати безперервність виробничого циклу, що унеможливлює зупинення технологічного процесу для збирання та аналізу отриманих даних. Для забезпечення їхньої безпеки необхідно враховувати специфіку функціонування конкретного підприємства та застосовувати комплексний підхід для протидії загрозам.

Системи ІБ у цьому випадку повинні відповідати певним вимогам: максимально докладно виконувати аналіз уразливостей всіх компонентів системи за допомогою контролю мережевих з'єднань (міжмережевий екран, IDS/IPS), програм, що використовуються (антивірус), що передаються через периметр файлів (шлюзовий антивірус з пісочницею, DLP) та дій користувачів (контроль привілейованих облікових записів); виявляти багатоступінчасті таргетовані атаки; надавати інформацію у зручному для фахівців з безпеки та автоматизації вигляді; враховувати особливості досліджуваної системи, не впливати на її роботу у процесі перевірки.

2.4 Оцінка ефективності існуючих методів та практик управління інцидентами.

Управління інцидентами – це процес, спрямований на ефективне та своєчасне реагування на виникнення інцидентів в інформаційних системах чи організаційних процесах. Інцидент – це будь-яка подія, яка призводить до порушення нормального функціонування системи або процесу і вимагає негайного втручання для її усунення та відновлення нормальної роботи.

Мета управління інцидентами – мінімізувати негативні наслідки інцидентів та забезпечити швидке відновлення нормальної роботи системи чи процесу. Для досягнення цієї мети необхідно визначити та застосувати оптимальні методи та інструменти для виявлення, класифікації, пріоритизації, реєстрації, відстеження та усунення інцидентів.

Управління інцидентами включає такі завдання та принципи:

- принцип документування та аналізу передбачає фіксацію всіх деталей інциденту, його наслідків та вжитих заходів щодо його усунення. Це дозволяє провести аналіз причин інциденту, виявити вразливості та проблеми в системі, а також розробити заходи щодо їх запобігання у майбутньому;
- принцип постійного покращення передбачає постійне вдосконалення процесів управління інцидентами. Це включає аналіз ефективності вжитих заходів, впровадження нових технологій і методів, а також навчання співробітників для підвищення їх компетенції в галузі управління інцидентами.

Дотримання цих принципів допоможе організації ефективно управляти інцидентами, мінімізувати їх вплив на бізнес-процеси та забезпечити безпеку інформаційних систем.

Управління інцидентами включає кілька етапів, які допомагають організації ефективно реагувати на проблеми, що виникли, і мінімізувати їх вплив на бізнес-процеси.

Розглянемо кожен етап докладніше:

- перший етап управління інцидентами – виявлення інциденту. На цьому етапі відбувається виявлення аномалій, збоїв чи інших проблем, які можуть вплинути на роботу інформаційної системи чи порушити безпеку даних.

Виявлення може відбуватися автоматично за допомогою моніторингових систем або повідомлень від користувачів або співробітників;

- після виявлення інциденту необхідно зареєструвати його та провести його класифікацію. Реєстрація дозволяє створити запис про інцидент, що містить інформацію про його характер, час виникнення, місце та інші деталі. Класифікація інциденту допомагає визначити його пріоритетність та рівень важливості для організації;

- оцінка та пріоритизація інциденту - на цьому етапі відбувається оцінка та пріоритизація інциденту. Оцінка дозволяє визначити масштаб проблеми, її потенційні наслідки та можливі ризики. Пріоритизація допомагає визначити порядок реагування на інциденти в залежності від їх важливості та впливу на бізнес-процеси.

- реагування на інцидент - на цьому етапі відбувається активне реагування на інцидент. Це включає в себе вжиття заходів щодо ліквідації проблеми, відновлення працездатності системи та мінімізації впливу інциденту на бізнес-процеси. Реагування може включати такі дії, як аналіз причин інциденту, вжиття заходів щодо запобігання повторного виникнення і відновлення даних.

- моніторинг та контроль - після реагування на інцидент необхідно здійснювати моніторинг та контроль, щоб переконатися, що проблема повністю усунена та не виникають нові інциденти. Моніторинг дозволяє відстежувати стан системи та своєчасно реагувати на будь-які аномалії чи збої. Контроль допомагає перевірити ефективність вжитих заходів та внести необхідні коригування у процес управління інцидентами.

Послідовне виконання цих етапів дозволяє організації ефективно управляти інцидентами, мінімізувати їх вплив на бізнес-процеси та забезпечити безпеку інформаційних систем.

Управління інцидентами включає використання різних інструментів і методів, які допомагають ефективно виявляти, аналізувати і вирішувати проблеми.

Системи моніторингу дозволяють відстежувати стан системи та виявляти можливі інциденти. Вони можуть попереджати про проблеми за допомогою оповіщень, що дозволяє оперативно реагувати на інциденти та запобігати їхньому негативному впливу на бізнес-процеси.

Журнали інцидентів використовуються для документування та відстеження всіх інцидентів, що відбулися в організації. Вони містять інформацію про час виникнення інциденту, його опис, причини та вжиті заходи щодо його усунення. Журнали інцидентів допомагають аналізувати минулі інциденти та запобігати їх повторенню у майбутньому.

Системи керування інцидентами (ITCM) надають централізоване сховище для керування всіма інцидентами. Вони дають змогу відстежувати статус інцидентів, призначати відповідальних осіб, встановлювати терміни рішення та надавати звіти про процес управління інцидентами. ITCM також можуть інтегруватися з іншими системами, такими як системи моніторингу та оповіщення для автоматичного створення інцидентів.

ITIL (Information Technology Infrastructure Library) – це набір найкращих практик у галузі управління інформаційними технологіями. Методика ITIL надає структурований підхід до управління інцидентами, включаючи визначення процесів, ролей та відповідальності, а також рекомендації щодо покращення процесу управління інцидентами.

Комунікаційні інструменти, такі як електронна пошта, чати та системи тикетів, використовуються для обміну інформацією та координації дій між учасниками процесу управління інцидентами. Вони дозволяють оперативно спілкуватися та ділитися інформацією, що сприяє більш швидкому та ефективному вирішенню проблеми.

Використання цих інструментів та методів допомагає організації ефективно керувати інцидентами, мінімізувати їх вплив на бізнес-процеси та підвищувати якість послуг.

Вибір показників управління інцидентами або KPI (ключових показників ефективності) допомагає менеджерам з технічного обслуговування визначити, чи вони досягають своїх цілей. Ці метрики слід включити до контрольного списку сервісу активів з метою оцінки ефективності команди зокрема.

Список найпоширеніших показників інцидентів включає:

- MTBF (Mean Time Before Failure); середній час безвідмовної роботи;
- MTTR (Mean Time to Recovery, Repair, Respond, or Resolve), середній час відновлення, ремонту, відповіді чи дозволу;
- MTTF (Mean Time to Failure) середній час вщент;
- MTTA (Mean Time to Acknowledge) – середній час підтвердження.

Примітка про MTTR: хоча це звучить як одна метрика, вона представляє чотири різні речі та значення. Отже, під час налаштування MTTR важливо точно знати, що саме вимірює команда.

Тепер, коли визначені метрики, заглибимося в те, що вони являють собою, як розраховуються і коли їх слід використовувати.

Середній час повністю розраховує тривалість періоду між ремонтами і збоями обладнання. Мета - зрозуміти, наскільки надійна техніка. MTBF також вимірює, як довго обладнання можна експлуатувати. Чим вищий час між відмовами, тим надійніша система.

Розрахунок MTBF включає отримання даних за певний період, наприклад 6 місяців, а потім розподіл часу безвідмовної роботи системи на загальну кількість збоїв, що відбулися.

MTBF ідеально підходить для систем, які можна ремонтувати у разі поломки. Цей метод використовується для підприємств, де простий може призвести до збитків, наприклад, загибелі людей (повітряні судна або виробниче обладнання з високим ступенем ризику).

Інформація, зібрана для розрахунку MTBF, також корисна для внутрішніх команд при виробленні рекомендацій щодо планового технічного обслуговування, заміни деталей та модернізації.

MTTR охоплює середній час ремонту, відновлення, дозволу та реагування. Що означає кожна з цих метрик із погляду управління об'єктами?

Середній час ремонту - період, необхідний відновлення працездатності системи. Сюди входить тестування. Ця метрика розраховується шляхом виміру загального часу, витраченого на ремонт системи за певний період, а потім поділу отриманого результату на кількість ремонтів, проведених за цей період.

Ця метрика не здатна розпізнати необхідність лагодження до її виникнення або виявити потенційні проблеми в системі. Середній час ремонту використовується лише з оцінки ефективності роботи технічних фахівців. Це допомагає персоналу відстежувати майбутні операції з усунення несправностей. В ідеалі, що нижчий цей показник, то краще для компанії.

Середній час відновлення - це період, необхідний відновлення системи до вихідного стану. Він включає час бездіяльності системи та її відновлення. Показник розраховується шляхом складання всього відрізку простою за певний період, поділеного на кількість інцидентів, які спричинили збій

Ця метрика розраховує швидкість всього процесу відновлення системи та допомагає порівняти її з певними цілями, а також із середнім показником у конкурентів.

Тим не менш, щоб зрозуміти інші змінні, такі як час між збоєм та попередженням, ефективність команди обслуговування або проблему з процесом діагностики, потрібно збирання глибших даних.

Проміжок часу для вирішення - це середній час, необхідний для усунення збою від початку до кінця, включаючи ідентифікацію, діагностику, ремонт та вжиття заходів для запобігання повторенню інциденту. По суті це вимагає, щоб технічні бригади зробили ще один крок, крім простого процесу відновлення.

Цей показник розраховується шляхом підсумовування повного часу, витраченого на вирішення проблем, що виникли за певний період, та поділу на кількість інцидентів. Також важливо відзначити, що ця метрика вимагає обліку робочих, а не понаднормового годинника.

Також важливо відзначити, що середній час усунення розраховується для екстрених збоїв, а не запланованих робіт з технічного обслуговування.

Середній час реагування - це середній час, необхідний відновлення системи після збою з першого попередження. Він розраховується шляхом поділу загального періоду реакції від збою до ремонту на кількість разів, коли інцидент мав місце протягом заданого відрізка.

Середній час до підтвердження дає змогу оцінити, наскільки оперативно реагують команди технічного обслуговування. Воно розраховується шляхом підсумовування відрізка між оповіщенням та підтвердженням несправності за певний період. Потім загальна величина поділяється на кількість інцидентів, що сталися цей інтервал.

Середній час повністю вимірює середній час між одним збоєм і наступним. Мета полягає в тому, щоб зробити цей показник якнайбільше.

Ця метрика допомагає розрахувати, як довго має прослужити система, та скласти відповідний розклад профілактичного обслуговування. Її отримують шляхом обчислення сумарного часу роботи пристроїв, що оцінюються, розділеного на загальну кількість приладів.

Наприклад, ви перевіряєте акумулятори димової сигналізації у будівлі. Батарея типу A працює 18 годин, типу B - 20 годин, типу C - 22 години, а типу D - 24 години. Таким чином, загальний час становить 84 години і ділиться на 4. Отже, MTTF становить 21 год.

Вибір правильних показників інцидентів залежить від низки чинників, зокрема від цього, про яку галузі йдеться, і потреби жителів керованого об'єкта. Постачальники виїзних послуг допоможуть налаштувати метрики збоїв для активу, що розглядається.

Існує кілька кроків до зв'язування метрик інцидентів із задоволеністю клієнтів.

Складіть карту шляху користувача. Це допоможе визначити, що для клієнта найважливіше. Поставте запитання, наприклад, що сповільнює процес, що найбільше дратує і яке обладнання чи системи вони найбільше покладаються.

Керівники об'єктів можуть зробити це безпосередньо поговоривши з користувачами, і навіть з тими, хто в минулому відповідав за ремонт.

Визначте показники рівня обслуговування. Розуміння того, що ваші клієнти вважають найбільш цінним, допоможе визначити, які дані найкраще відповідають потребам людей та які відомості ви повинні збирати.

Встановіть цілі рівня обслуговування (SLO) для болючих точок клієнтів. Запитайте людей, які інциденти були б для них неприйнятними. Їх слід проаналізувати з погляду впливу збою на задоволеність клієнтів. Крім того, їх необхідно оцінити з точки зору "бюджету помилок" і того, наскільки критичним є той чи інший інцидент і як він впливає на надійність системи.

Створення ретроспективи інциденту.

Управління інцидентами – це постійне навчання на основі нових даних. Метрики подій дають цінне уявлення про низку факторів, і з їхньою допомогою можна значною мірою уникнути майбутніх аварій. Це називається ретроспективою інциденту, коли ви знаєте подію і перетворюєте досвід на знання.

У міру того, як організації вдосконалюють свій аналіз інцидентів, згодом розвиваються і їх заходи у відповідь.

Ідеальна ретроспектива має включати таке:

- короткий, але повний опис події;
- фактори, що викликали його, з використанням тверджень «бо» та «чому»;
- вплив інциденту на споживачів, включаючи ступінь їхньої загальної задоволеності.

Які подальші дії було здійснено у відповідь на інцидент і для забезпечення мінімізації подібних ситуацій у майбутньому. Опис дій має бути таким, ніби ви розповідаєте історію. У ньому будуть згадані всі люди, які брали участь у виявленні інциденту та вжиття заходів.

Викладіть хронологію всього інциденту, включаючи використання скріншотів та журналів.

Проведіть технічний аналіз інциденту, включаючи помилки або недоробки та фактори, що залежать один від одного.

Проведіть аналіз процесу, як інцидент було врегульовано і що не так.

Задокументуйте спілкування між ключовими співробітниками під час інциденту.

Переконайтеся, що ретроспектива створена протягом 48 годин після інциденту, і зберігайте звіти таким чином, щоб можна було легко отримати доступ до них, якщо подібний випадок станеться в майбутньому.

Переваги та вигоди від ефективного управління інцидентами:

- швидке реагування на проблеми - ефективне управління інцидентами дозволяє організації швидко реагувати на проблеми, що виникають. Завдяки чітким процедурам і певним ролям і відповідальність, команда може швидко та ефективно вживати заходів щодо усунення інцидентів та мінімізації їх впливу на бізнес-процеси;
- мінімізація простоїв та втрат - ефективне управління інцидентами допомагає мінімізувати простої та втрати, пов'язані з непередбаченими збоями та проблемами. Завдяки оперативному реагуванню та швидкому відновленню працездатності системи, організація може скоротити час простою та уникнути значних фінансових втрат;
- поліпшення якості послуг - ефективне управління інцидентами сприяє покращенню якості послуг. Завдяки швидкому реагуванню на проблеми та оперативному усуненню інцидентів, організація може забезпечити безперервність роботи системи та задоволення потреб клієнтів;
- поліпшення репутації організації - ефективне керування інцидентами допомагає покращити репутацію організації. Коли клієнти бачать, що організація оперативно реагує на проблеми та швидко вирішує їх, це створює позитивне враження та підвищує довіру до організації;
- поліпшення комунікації та співробітництва - управління інцидентами сприяє покращенню комунікації та співробітництва всередині організації. Коли у всіх учасників процесу є чіткі ролі та відповідальності, а також доступ до

загальних комунікаційних інструментів, це сприяє більш ефективному обміну інформацією та координації дій;

- зворотній зв'язок та покращення процесів - управління інцидентами дозволяє організації отримувати зворотний зв'язок від клієнтів та учасників процесу. Це допомагає виявити слабкі місця та проблеми в системі, а також запропонувати покращення та оптимізацію процесів.

Загалом, ефективне управління інцидентами дозволяє організації мінімізувати проблеми, покращити якість послуг, підвищити репутацію та забезпечити безперервність роботи системи.

Сфокусуюсь на конкретному процесі, щоб наочно продемонструвати, як проводиться його оцінка. За основу візьму процеси управління інцидентами та запитами. Чому говорю про один процес, а оцінюю два?

Справа в тому, що у Cobit своє бачення процесної моделі. Процеси методології ITIL RFF Request Fulfilment та INC Incident management у CobiT консолідуються в DSS02 Manage Service Request and Incidents, а процес ITIL SACM Service Asset & Configuration Management поділено на два: BAI09 Manage Assets та BAI10 Manage Configuration. У мережах можна знайти таблицю мапінгу процесів із суміжних методологій, щоб консультантам полегшити працю зі зіставлення.

Розповім про своє бачення як ця методологія допомагає у досягненні високих, а головне обґрунтованих та зрозумілих результатів.

ITIL, на відміну від CobiT, сам собою систематично примусово «прокачує» практикуючих консультантів, будучи стандартом де-факто в IT-впровадженнях. У зв'язку з цим ступеня сертифікації недосяжні без постійного вивчення методології з різних ракурсів. А ось до CobiT зазвичай руки не доходять. Але раптом, за обставинами, «руки дійшли», і погляду почали відкриватися безмежні оціночні можливості.

CobiT 5 – це серія книг, що містить велику методологічну інформацію щодо процесів управління інформаційними технологіями.

Для оцінки скористаємося Process Assessment Model (PAM): Using COBIT® 5.

CobiT виділяє шість рівнів можливостей процесів, включаючи рівень «неповного процесу», коли процес не відповідає своєму призначенню (рис. 2.7):

Figure 4—Capability Levels and Process Attributes

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Process optimization

Source: This figure is adapted from ISO/IEC 15504-2:2003 with the permission of ISO at *www.iso.org*. Copyright remains with ISO.

Рис. 2.7. шість рівнів можливостей процесів CobiT

Рівень 0 – Неповний процес – процес ще не впроваджений чи неспроможний відповідати своєму призначенню. На цьому рівні відсутні свідчення систематичного досягнення процесом своєї мети або таких свідчень мало.

Рівень 1 - Здійснений процес - процес впроваджений і відповідає своєму призначенню. Визначено необхідні результати виконання процесу, опрацьовуються види діяльності для досягнення цілей та результатів процесу.

Рівень 2 – Керований процес – здійснений процес попереднього рівня керований (планується, відстежується та коригується). Створюються, контролюються та підтримуються робочі продукти процесу. Розроблено повний набір проектної документації. Використовується єдина система автоматизації.

Рівень 3 – Встановлений процес – керований процес попереднього рівня здатний отримувати очікувані результати. Усі процесні процедури уніфіковані. Розроблено процедуру масштабування процесу, а також виділення ресурсів та навчання персоналу.

Рівень 4 – Передбачуваний процес – встановлений процес попереднього рівня отримує результати за умов заданих обмежень – процес виміряємо. Розроблено процедури перевірки та коригування процесної діяльності, їх періодичність.

Рівень 5 – Процес, що оптимізується – передбачуваний процес попереднього рівня постійно вдосконалюється, щоб забезпечувати досягнення поточних та майбутніх цілей підприємства.

Кожен із рівнів поділяється на атрибути можливостей, наявність яких свідчить про досягнення процесом відповідного рівня.

У свою чергу, атрибути можливостей досягаються шляхом перевірки процесу набору фіксованих індикаторів відповідно до ISO/IEC 15504-2:2003. (ГОСТ Р ІСО/МЕК 15504-2-2009)

У таблиці зведено всі атрибути та індикатори з зазначених стандартів, трохи суб'єктивно «зачесано» за результатами практики щодо формулювань та з урахуванням особливостей перекладу (оригінал – у 4.0 Process Capability Indicators). Вони адаптовані під сприйняття як аудитором, і учасниками обстеження.

Повнота атрибута оцінюється за шкалою (рис. 2.8.):

Figure 6—Rating Levels		
Abbreviation	**Description**	**% Achieved**
N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
F	Fully achieved	>85% to 100% achievement
Source: This figure is reproduced from ISO/IEC 15504-2:2003, with the permission of ISO/IEC at *www.iso.org*. Copyright remains with ISO/IEC.		

Рис. 2.8. Шкала оцінки повноти атрибуту

N (не досягається) – в процесі, що оцінюється, не існує або існує мало свідчень того, що певний атрибут в оцінюваному процесі досягається (від 0 до 15% досягнення);

P (частково досягається) - в оцінюваному процесі є свідчення того, що існує підхід до досягнення і відбувається часткове досягнення заданих цілей. Деякі аспекти того, як досягається мета (атрибут), є непередбачуваними (від 15% до 50% досягнення);

L (переважно досягається) – в оцінюваному процесі існують свідчення системного підходу та системного досягнення заданих цілей. Існують деякі недоліки досягнутих результатів (від 50% до 85% досягнення);

F (досягається повністю) – в оцінюваному процесі є свідчення повного системного підходу та фактичного досягнення заданих цілей. Значних недоліків, пов'язаних з одержаним результатом, не виявлено (від 85% до 100% досягнення).

Оцінка можливостей процесів розпочинається з нульового рівня. Оцінка кожного наступного рівня має сенс лише у тому випадку, якщо забезпечено 100% досягнення попереднього.

При оцінці:

- спочатку перевіряється наявність індикаторів атрибутів в обстежуваному процесі;
- потім за повнотою індикаторів приймається рішення про частку наявності атрибута;

- далі за наявності атрибутів визначається міра досягнення рівня. Рівень вважається досягнутим, якщо він повною мірою присутні потрібні атрибути;
- спочатку проводиться збір інформації за допомогою анкетування та інтерв'ювання ключових співробітників;
- потім вся отримана інформація зводиться у єдиний звіт і її оцінка. Для оцінки можна скористатися табличками-шаблонами Self-assessment Template (Appendix B of the Self-assessment Guide), у якому необхідно проставити чекбокс на перетині індикатора та її рейтинга.

Перевірка досягнення першого рівня.

Для кожного процесу передбачено таблицю, що містить довідкову інформацію. Ця таблиця зручна не тільки при оцінці, але і при проектуванні процесу, як шпаргалка за ключовими процесними особливостями. Для оцінки досягнення процесом DSS02 першого рівня допоможе відповідна таблиця. А саме її розділи: Мета процесу (ProcessPurposeStatement), Результати (Outcomes), Артефакти (Outputs).

Атрибут, що свідчить про досягнення першого рівня, – Продуктивність процесу. Процес існує, досягається його мета:

Підвищення продуктивності та мінімізація збоїв завдяки швидкому вирішенню запитів користувача та інцидентів.

Якщо у нас за результатом обстеження немає у звіті статистичних даних про динаміку підвищення продуктивності та стабільне зниження збоїв, то рекомендується оцінити результати та навести будь-які можливі приклади на підтримку висновку:

DSS02-O1 IT-послуги доступні – 80% L;

DSS02-O2 Інциденти дозволяються відповідно до узгоджених рівнів обслуговування – 90% F;

DSS02-O3 – Запити на обслуговування DSS02-O3 обробляються відповідно до узгодженого рівня обслуговування та задоволеності користувачів – 90% F.

Якщо з першого підходу розібратися не вдалося, то найправильніший спосіб просто «прочекати» артефакти на предмет «є/ні». Це дасть загальну картину фактичну продуктивність процесу (рис. 2.9).

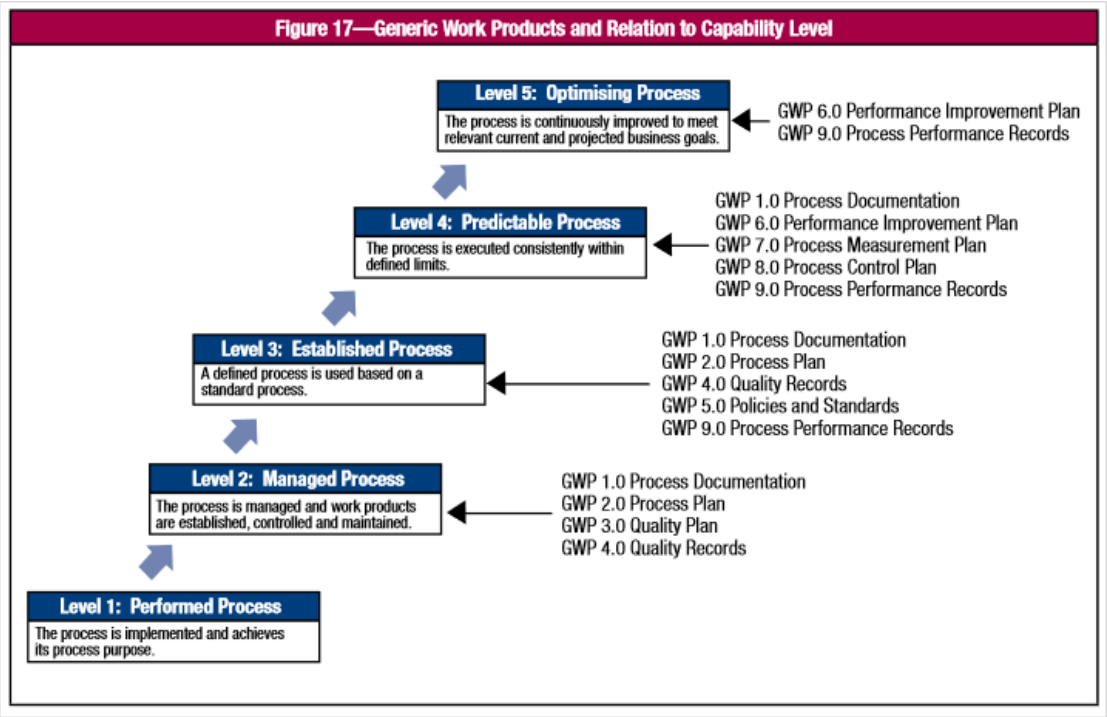

Рис. 2.9. Загальні робочі продукти та відношення до рівня можливостей

CobiT у цій частині пропонує оцінювати досягнення процесом цілей того чи іншого рівня щодо наявності певних результатів та якості їх опрацювання. На малюнку вказано, які результати допоможуть визначити досягнення рівня. Докладніше про результати можна дізнатися у Appendix B generic and level 1 outPut work Products.

Мною виділено певні чекпойнти, наявність яких у зібраній інформації за результатами обстеження я приймаю за успішне досягнення рівня. Нижче запропоновано їх перелік із наскрізною нумерацією, але умовним поділом за рівнями методології.

Для визначення ступеня проходження процесом третього рівня рекомендую шукати у зібраній документації опис методик масштабування. Якщо на другому рівні ми просто шукали опис процедур або ролей, то на третьому

рівні ці процедури повинні бути знеособленими і повинні вільно виконуватися в будь-якій філії, підрозділі, організації без прив'язки до конкретної оргструктури, ресурсів, особливостей технологічних процесів тощо.

Якщо роль другої лінії виконує інженер відділу технічної підтримки користувачів і на нього посилається процедура другого рівня, то процедура третього рівня повинна виконуватися знеособленим відповідальним виконавцем, роль якого, у свою чергу, грає той самий інженер ОТП або начальник служби підтримки користувачів і т.п. (залежно від філії/територіального розподілу). У цьому обов'язково має бути таблиця розподілу типових ролей на конкретних співробітників/відділи/групи, тобто. відповідальність має бути явно зафіксовано.

Методологія дуже насичена та велика. На мій погляд, вона асоціюється з поняттям «мозковий штурм», коли величезна група людей старанно думає в одному напрямку і всі думки десь фіксує. Так і в Cobit – впорядкована фіксація всіх корисних відомостей, затребуваних у процесах. Для мене ця методологія – криниця ідей, ґрунт для натхнення, засіб для виходу з логічного глухого кута.

Мінуси методології – надмірність. Цілеспрямовано дотримуватись її не виходить. Є відчуття дублювання понять чи то через особливості перекладу, чи то через непрозорість сприйняття всіх ідей, запропонованих авторами. Тому:

ІДЕАЛЬНО взяти за основу як точку опори;

НЕМОЖЛИВО сліпо дотримуватися методології розробки процесу «під ключ».

В другому розділі було розлянуто типи інцидентів, способи виявлення та інструменти, Були розглянуті системи DLP, як приклад Solar Dozor, його функції, також були приведені приклади та опис самих відомих уразливостей та інцидентів, які були представлені з використанням малюнків. Провів аналіз існуючих процедур та методів управління інцидентами, розлянуті платформи які організації використовують із моделювання методів управління інцидентами. Була розлянута Система Управління інцидентами AMS Incident Management, яка супроводжувалась схемами. Потім було розглянуто наслідки уразливостей і

вплив інцидентів на функціонування АСУ. Була представленна статистика впливу різних видів інцидентів на АСУ

РОЗДІЛ 3
ОЦІНКА ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНЦИДЕНТАМИ

3.1 Визначення критеріїв ефективності системи управління інцидентами та їх показників

У світі безперервної роботи систем технічні інциденти ведуть до серйозних наслідків. Щогодини простою в роботі системи обходиться компаніям у середньому 300 тисяч доларів США втраченої вигоди, втраченої продуктивності співробітників та витрат на технічне обслуговування. У разі масштабних відмов витрати можуть зростати як на дріжджах (можна згадати компанію Delta Airlines, яка втратила близько 150 млн. доларів США через збій у роботі IT у 2017 році). Клієнти, які не можуть сплатити рахунки, провести важливу відеоконференцію або купити авіаквиток, швидко йдуть до конкурентів.

На карту поставлено дуже багато. Тому командам дуже важливо відстежувати KPI управління інцидентами, а також використовувати результати для виявлення, діагностики, виправлення та, нарешті, запобігання інцидентам.

Позитивний момент полягає в тому, що при обробці інцидентів у веб-сфері та програмному забезпеченні (на відміну від механічних поломок та відключення систем) команди зазвичай отримують набагато більше даних. Тому вони можуть ефективніше розібратися в ситуації та провести покращення.

Але є і мінуси. Іноді стає складніше зрозуміти проблему за наявності великого обсягу даних. Ключові показники ефективності (KPI) допомагають компаніям визначити, чи вони досягають конкретних цілей. У контексті управління інцидентами цими показниками може бути кількість інцидентів, середній час розв'язання або середній час між інцидентами.

Під час відстеження KPI керування інцидентами можна виявити та діагностувати проблеми з процесами та системами, визначити орієнтири та

поставити реалістичні цілі для роботи команди, а також знайти відправну точку для вирішення масштабних питань.

Припустимо, що компанія прагне вирішення всіх інцидентів протягом 30 хвилин, але вашій команді це вдається в середньому за 45 хвилин. Без конкретних показників важко зрозуміти, у чому проблема. Система оповіщення спрацьовує надто повільно? У процесі щось працює? Потрібні сучасніші діагностичні інструменти? Ця проблема пов'язана з командою чи обладнанням?

Тепер додайте показники. Якщо відомо, скільки часу потрібно системі оповіщення для спрацьовування, ви зможете зрозуміти, чи є вона причиною проблеми. Якщо діагностика займає більше половини часу, ви можете зосередитись на усуненні несправностей у ній. Якщо команда B працює на 25 % повільніше, ніж команди A, C та D, можна спробувати зрозуміти, чому це відбувається.

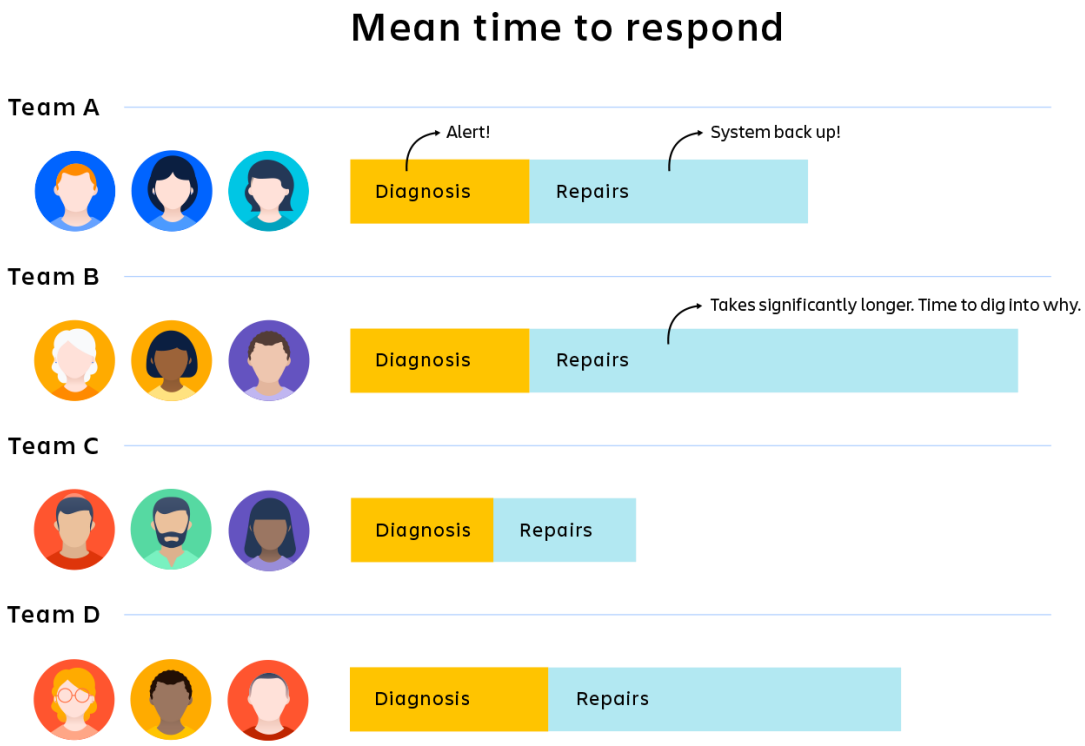

Рис. 3.1. Середній час до відповіді

KPI не усунуть ваші проблеми автоматично, але вони допоможуть зрозуміти суть неполадок і вкажуть, куди потрібно звернути увагу та зусилля.

Якщо ви використовуєте інструмент оповіщення, корисно знати, скільки оповіщень генерується протягом певного періоду часу. За допомогою рішення Jira Service Management ви зможете надсилати оповіщення, а також створювати звіти та дашбоарди для їх відстеження.

Шукайте періоди, коли спостерігається значне чи нетипове зростання чи падіння, і навіть позитивна динаміка. При виявленні таких змін проаналізуйте причини та способи реагування ваших команд на них.

Відстеження кількості інцидентів за певний період передбачає підрахунок середньої кількості інцидентів за певний період. Цим періодом може бути тиждень, місяць, квартал, рік чи навіть день.

Згодом інциденти відбуваються частіше чи рідше? Кількість інцидентів вважається прийнятною чи її можна скоротити? Після того, як ви зрозумієте, в чому полягає проблема з кількістю інцидентів, ви зможете припустити, чому це число зростає або залишається високим і що команда може зробити для вирішення проблеми.

MTBF (середнє напрацювання на відмову) – середній час роботи технічного продукту між усунутими збоями. За допомогою цього показника можна відстежувати доступність та надійність усіх продуктів.

Як і інші показники, він наводить на серйозніші питання. Якщо значення MTBF недостатньо високе, варто задуматися, чому системи так часто виходять з ладу і як можна зменшити чисельність майбутніх збоїв або запобігти їм.

MTTA (середній час підтвердження) - це середній час, який проходить між отриманням оповіщення та моментом, коли учасник команди підтвердить інцидент і почне працювати над його усуненням. Цей показник є важливим тим, що за його допомогою можна зрозуміти, наскільки швидко ваша команда реагує на інциденти.

Якщо з'ясувалося, що швидкість реагування недостатньо висока, можна поставити нові питання. Чому значення MTTA таке велике? Команди перевантажені, відволікаються чи можуть зрозуміти, кому адресовано

оповіщення? За допомогою MTTA можна визначити проблему, а подібні питання допоможуть дістатися її суті.

MTTD (середній час виявлення) – це середній час, необхідний вашій команді, щоб виявити проблему. Цей термін часто використовується у сфері кібербезпеки командами, які зосереджені на виявленні атак та випадків несанкціонованого доступу.

Якщо значення цього показника різко змінюється чи залишається недостатньо високим, варто з'ясувати причину.

MTTR може означати середній час виправлення, рішення, реагування чи відновлення. Мабуть, найбільшу користь становить середній час рішення. Цей показник дозволяє зафіксувати не лише час, витрачений на діагностику та усунення безпосередньої проблеми, а й час на запобігання повторенню такої проблеми у майбутньому. Відновлення є основним показником DevOps; саме його, на думку програми DevOps Research and Assessment (DORA), можна використовуватиме оцінки стабільності команди DevOps.

Цінність цього показника найкраще проявляється під час діагностики. Чи дозволяються інциденти так швидко і ефективно, як ви очікували? Якщо ні, потрібно з'ясувати причину, через яку час вирішення не відповідає цільовому значенню.

Відновлення є основним показником DevOps; саме його, на думку програми DevOps Research and Assessment (DORA), можна використовуватиме оцінки стабільності команди DevOps. Це сукупний час, що йде на виявлення проблеми, пом'якшення її наслідків та повне усунення.

Якщо у вас є ротація чергових, рекомендується відстежувати, скільки часу працівники та підрядники витрачають на виклик. За допомогою цього показника можна стежити за тим, щоб жоден співробітник чи команда не були перевантажені.

За допомогою Jira Service Management можна створювати вичерпні звіти, щоб миттєво дізнаватися значення цих показників.

SLA (угода про рівень обслуговування) – це угода між постачальником та клієнтом про вимірювані показники, такі як час безвідмовної роботи, час реагування, а також заходи відповідальності.

У цих угодах про рівень обслуговування фіксуються обіцянки компанії (про час безвідмовної роботи, середній час відновлення тощо). Щоб їх стримати, команди управління інцидентами повинні відстежувати ці показники. Якщо і коли значення таких показників, як середній час відгуку або середній час між збоями, змінюються, потрібно оновити угоди та (або) внести виправлення (і це має відбутися швидко).

SLO (мета за рівнем обслуговування) – це угода в рамках SLA про цільове значення того чи іншого показника, наприклад, часу безвідмовної роботи. Як і у випадку з угодою SLA, SLO є важливими показниками, які слід відстежувати, щоб гарантувати, що компанія виконує свою частину угоди щодо обслуговування клієнтів.

Тимчасова мітка – це закодована інформація про те, що сталося у певний час під час інциденту, до або після нього. Така інформація зазвичай не вважається показником, але ці важливі дані необхідно враховувати при оцінці стану управління інцидентами та розробці стратегії щодо вдосконалення.

За допомогою тимчасових міток команди визначають хронологію інциденту, а також попередні події та заходи, вжиті для його вирішення. Зрозуміла та доступна всім учасникам хронологія є одним із найкорисніших артефактів під час розбору інцидентів.

Час безвідмовної роботи - це кількість часу (у відсотках), протягом якого системи доступні та працездатні.

З розширенням взаємозв'язків онлайн-сервісів та зростанням складності самих систем стало зрозуміло, що гарантія безвідмовної роботи протягом 100% часу неможлива. У випадку більшості продуктів прагнуть забезпечити високу доступність, тобто створити таку систему або продукт, які можуть працювати без перерви протягом тривалого часу. Згідно з галузевим стандартом, безвідмовна

робота протягом 99,9% часу – це дуже добрий результат, а протягом 99,99% – відмінний.

Відстежувати значення цього показника обов'язково до виконання обіцянок, даних клієнтам. Як і інші показники, він становить лише відправну точку. Якщо безвідмовну роботу не вдається забезпечувати на рівні 99,99 %, для розуміння причини потрібно буде глибше вивчити проблему, поговорити з командою, а також проаналізувати процес, структуру, доступ чи технологію.

KPI має недоліки. Так, можна легко потрапити у залежність від малозмістовних даних. Якщо ваша команда дозволяє інциденти недостатньо швидко, для вирішення проблеми знадобиться щось більше, ніж просте усвідомлення цього факту. Вам потрібно розуміти, як і чому команда вирішує чи не вирішує проблеми. Крім того, потрібно знати, чи можна порівняти проблеми, які ви порівнюєте.

На підставі KPI не можна зрозуміти, як ваші команди підходять до вирішення складних завдань, чому інциденти відбуваються все частіше або чому на дозвіл інциденту А пішло втричі більше часу, ніж інцидент Б.

Для цього потрібні аналітичні висновки. Однак дані можуть стати не лише відправною точкою на шляху до цих висновків, а й перешкодою. Через них може скластися помилкове враження ефективної роботи, коли показники не покращуються. Показники не враховують відмінності (іноді дуже суттєві) між інцидентами або підходами до їх вирішення. Крім того, за кадром залишається досвід ваших команд та фундаментальна складність самих інцидентів.

«Інциденти набагато унікальніші, ніж прийнято про них думати. Два інциденти, дозволити які можна за один проміжок часу, можуть значно відрізнятися за тим, наскільки вони несподіваними і незбагненними виявилися для відповідальних фахівців. Крім того, заходи щодо пом'якшення наслідків або виправлення ситуації можуть нести абсолютно різні ризики у різних інцидентах. Інциденти – це не деталі з конвеєра, у яких показником якості є обмежений розкид фізичних розмірів»,

– Джон Оллспоу, «Як уникнути малозмістовних даних про інциденти» (John Allspaw, Moving Past Shallow Incident Data)

Ми не стверджуємо, що KPI є неефективними, і не закликаємо до відмови від них. Справа в тому, що лише KPI недостатньо. Їх потрібно використовувати як відправну точку. Вони допоможуть виявити причину проблеми та стануть першим кроком на складному шляху до ефективного покращення.

Jira Service Management пропонує можливості створення звітів, щоб ваша команда могла відслідковувати KPI, а також контролювати та оптимізувати управління інцидентами.

В сучасному світі технологій, де швидкість та надійність є ключовими факторами успіху, виявлення та усунення інцидентів є невід'ємною частиною розробки та управління програмними продуктами. DevOps-підхід, що поєднує розробку та операції, використовується для забезпечення безперебійної роботи систем та вирішення проблем, які виникають в процесі розробки та експлуатації. Давайте розглянемо ефективні методи виявлення та усунення інцидентів у контексті DevOps.

Моніторинг: Використання систем моніторингу, таких як Prometheus, Nagios або ELK Stack, дозволяє виявляти аномалії, спостерігати за метриками продуктивності та використання ресурсів, а також отримувати сповіщення про можливі проблеми.

Журнали подій: Збір та аналіз журналів подій (logs) дозволяє виявляти помилки, несправності та неочікувані поведінки системи. ELK Stack, Splunk або Graylog – це лише деякі з популярних інструментів для аналізу журналів подій.

Тестування: Ефективне використання автоматизованих тестів, включаючи одиницеві, інтеграційні та відмовостійкі (resiliency) тести, дозволяє виявляти проблеми ще на ранніх етапах розробки.

1. Контейнеризація: Використання контейнерів, таких як Docker або Kubernetes, допомагає створити середовище, що легко розгортається та масштабується. Це дозволяє швидко перенести застосунки з одного середовища в інше і легко управляти їхнім життєвим циклом. Коли виявляється інцидент,

DevOps-інженер може швидко створити новий контейнер з оновленою версією програмного забезпечення та замінити пошкоджений контейнер, що допомагає усунути проблему швидко і без перерви в роботі системи.

2. Резервне копіювання та відновлення: Регулярне створення резервних копій даних і налаштувань системи дозволяє відновлювати систему в разі виникнення серйозних інцидентів, таких як втрата даних або відмова обладнання. Застосування методів резервного копіювання, таких як резервне копіювання в хмарні сховища або реплікація даних на віддалені сервери, дозволяє забезпечити відновлення системи в мінімальні терміни.

3. Культура відповідальності та співпраці: Успішна робота з інцидентами вимагає культури відповідальності та співпраці між розробниками, тестувальниками, операторами та іншими учасниками команди. DevOps-інженери відіграють ключову роль у цьому процесі, співпрацюючи з різними командами та координуючи реагування на інциденти. Вони виконують функції моніторингу системи, аналізу причин інцидентів, управління комунікаціями та впровадження заходів для запобігання подібним інцидентам у майбутньому.

Інцидент-трекінгові системи: Інструменти, такі як Jira, ServiceNow або Zendesk, дозволяють команді відстежувати та керувати інцидентами. Вони дозволяють створювати та призначати задачі, встановлювати пріоритети, моніторити стан вирішення інцидентів та забезпечувати прозорість процесу виявлення та усунення проблем.

Автоматизація та оркестрація: Використання інструментів автоматизації, таких як Ansible, Puppet або Chef, дозволяє автоматизувати рутинні завдання, що пов’язані з усуненням інцидентів. Це сприяє прискоренню процесу відновлення та зменшенню можливих помилок під час втручання людини.

Системи сповіщень та комунікації: Інструменти, такі як Slack, Microsoft Teams або PagerDuty, дозволяють швидко сповіщати членів команди про виникнення інциденту та координувати їхню спільну роботу для швидкого реагування. Це полегшує комунікацію, спільне розуміння ситуації та прийняття рішень для усунення інциденту.

Ефективні методи виявлення та усунення інцидентів відіграють важливу роль у сучасному світі програмного забезпечення. Недосягнення надійності, та невідповідні усунення інцидентів можуть мати серйозні наслідки для організації. Шлях до успіху полягає у використанні сучасних інструментів моніторингу, автоматизації та оркестрації, а також активної ролі DevOps-інженерів у виявленні та вирішенні проблем. Забезпечення безперебійності, надійності та швидкості відновлення системи стає ключовим фактором успіху в цифровому світі, де навіть найменша перешкода може призвести до фінансових втрат, втрати довіри користувачів та погіршення репутації організації.

DevOps-інженери відіграють активну роль у виявленні та усуненні інцидентів. Вони відповідають за моніторинг системи, аналіз причин інцидентів, координацію роботи команди та впровадження заходів для запобігання подібним проблемам у майбутньому. Вони співпрацюють з розробниками, тестувальниками, операторами та іншими членами команди для швидкого реагування та ефективного вирішення інцидентів.

3.2 Створення моделі системи управління інцидентами

Ефективність діяльності компанії безпосередньо залежить від злагодженої (гармонійної) роботи керівництва бізнесу та IT-фахівців. Складнощі у побудові конструктивного діалогу між керівництвом компанії та її IT-департаментом, призводять до зростання витрат, виконання досить великого обсягу рутинної роботи. З метою ліквідації розриву між керівництвом та IT-департаментом застосовують різні підходи, наприклад на основі методології COBIT, яка вводить ряд показників з метою оцінки ефективності реалізації системи управління інформаційними технологіями (IT) у компанії. В IT-департаменті функціонує служба технічної підтримки, яка вирішує завдання реагування на різні інциденти Під інцидентом розуміється незапланованe переривання чи зниження якості IT-послуги. Інцидент може спричинити призупинення процесу надання сервісу або

зниження якості його роботи, у результаті надходять масові звернення від користувачів сервісу. Таким чином, під інцидентом можна розуміти будь-яку подію, яка не є частиною нормального (штатного) функціонування системи/сервісу/процесу.

Основним завданням служби технічної підтримки, що є складовою IT-департамент є забезпечення підтримки безперервності бізнесу шляхом управління життєвим циклом інцидентів. Швидкість реакції на інцидент та терміни вирішення інцидентів, що реєструються у службі технічної підтримки, повинні відповідати значенням, прийнятим у Угоді про рівень надання послуг (SLA), основний документ, що регламентує взаємодію служби IT та замовника, у ролі якого може виступати як бізнес-керівництво, а також кінцевий користувач послуги. Основна мета процесу управління інцидентами – якнайшвидше відновлення послуги для клієнтів Для підвищення ефективності процесу.

Управління інцидентами використовуються численні інструменти, як правило, це різні інформаційно-аналітичні системи, такі як HP ServiceDesk, IBM ServiceDesk, HelpDesk, Jira, BPM-Online. Подібні системи є дорогими, і їх досить складно адаптувати до потреб конкретної служби технічної підтримки, враховуючи всю специфіку її роботи.

Проведений аналіз показав, що існуючі моделі управління інцидентами в умовах функціонування розподілених інформаційних систем компанії з великим кількістю користувачів, у тому числі віддалених, не повною мірою відповідають вимогам, що пред'являються, і не завжди забезпечують необхідний рівень надання послуг.

Наукова новизна роботи визначається обґрунтуванням необхідності побудови трирівневої моделі обробки інцидентів із використанням бази знань, що забезпечує підтримка процесу в актуальному стані та своєчасне реагування на вступники запити. Запропоновано підхід, що забезпечує підвищення доступності каналів обробки звернень за рахунок визначення їх мінімально необхідної кількості. Використання релевантних метрик для об'єктивної оцінки ступеня досягнення показниками процесу управління інцидентами їх цільових

значень дозволило підвищити ефективність останнього. Проблематика підвищення ефективності процесу управління інцидентами присвячено досить багато досліджень.

Так, у роботі [34] запропоновано комплекс моделей, алгоритмів та програмних засобів на базі бібліотеки ITIL, які забезпечують підвищення ефективності обробки запитів, що надходять до служби технічної підтримки Інтернет-провайдера за рахунок раціонального розподілу персоналу з робіт та пріоритизації запитів користувачів. У роботі аналізуються питання щодо підвищення якості вирішення інцидентів. У ній представлені математичні моделі та методи

управління інцидентами, зокрема математична модель, що описує залежність кількості звернень від кількості обслуговуваних робочих місць.

У роботі [35] для оцінки та контролю якості IT-послуг запропоновано розглядати сервісні послуги показники ефективності, такі як відсоток пропущених дзвінків за період, відсоток вирішених інцидентів за період, середня кількість заявок на другій лінії підтримки за період та середня кількість заявок за період одному співробітнику другий лінії підтримки.

Аналіз результатів досліджень у галузі управління інцидентами в інформаційній системі підприємства показав, що існуючі моделі процесу управління інцидентами не повною мірою відповідають вимогам, що висуваються.

На рис. 3.2 представлено структурну схему типової моделі управління інцидентами.

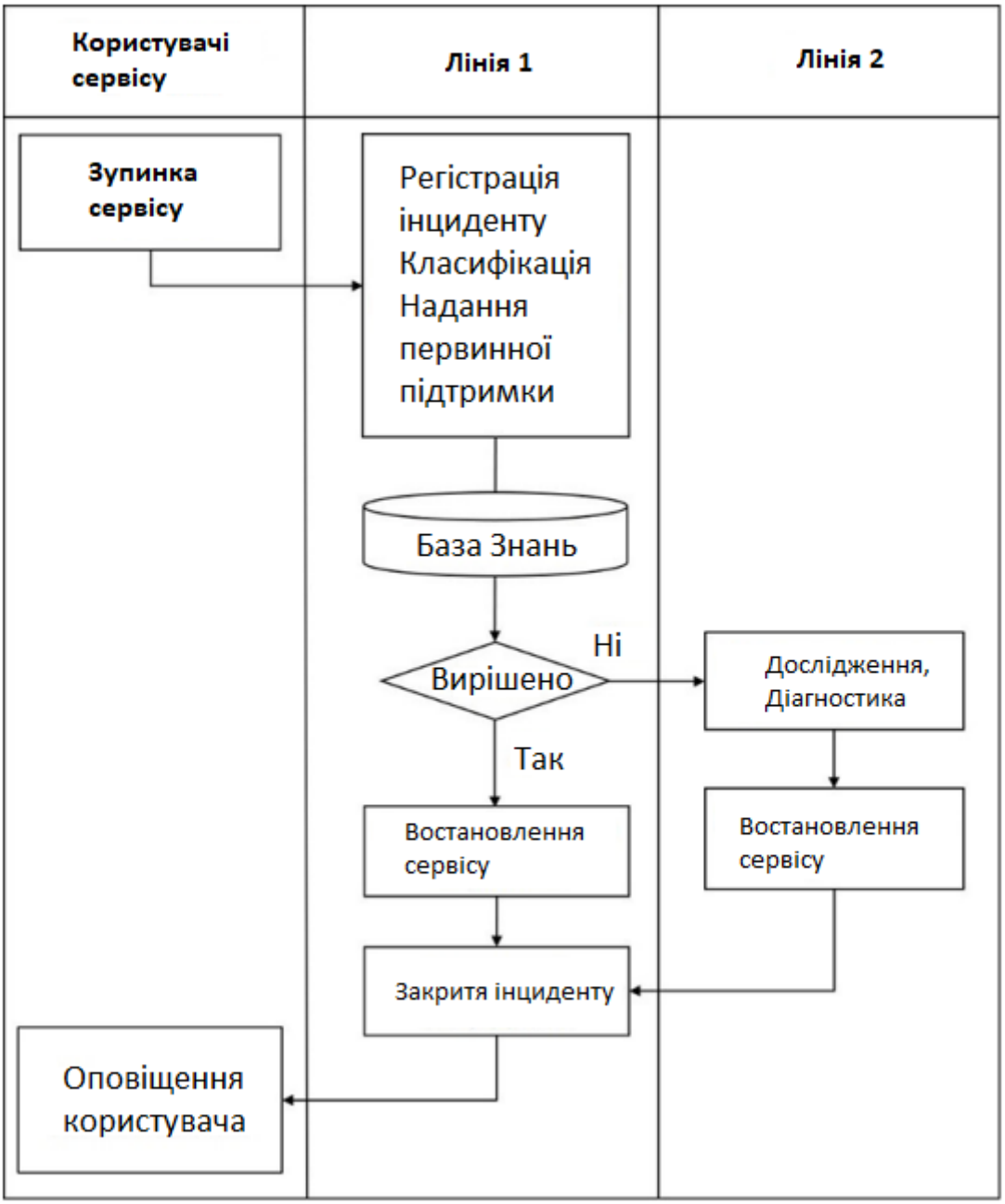

Рисунок 3.2. Існуюча модель процесу управління інцидентами

В основі моделі лежить дворівнева система обробки інцидентів, що включає першу лінію підтримки, на якій здійснюється реєстрація інциденту, класифікація проблеми, що виникла, і реалізація етапу початкової підтримки. Якщо під час надання початкової підтримки проблема усувається, інцидент закривається. За неможливості вирішити інцидент у межах першої лінії інцидент прямує на другу лінію підтримки. Інженери другої лінії глибше досліджують

проблему, діагностують несправності і спрямовують результат на першу лінію для закриття. Якщо проблему не вдалося вирішити на другій лінії технічної підтримки, то проблема спрямовується на більш глибоке дослідження та діагностику, а перша лінії інформує про це користувача. Таким чином, у моделі управління інцидентами на виході генерується повідомлення користувачеві про відновлення сервісу, зберігається запис про інцидент і запис про проблему. При цьому в основі знань накопичується статистика: кількість відкритих інцидентів, відсортованих за пріоритетом, за минулим часом, за робочими групами; кількість інцидентів, дозволених на кожній лінії підтримки; середній час вирішення інциденту у робочій групі; середнє відновлення сервісу, відсоток інцидентів, вирішених у межах крайнього терміну та інших.

При аналізі існуючої моделі управління інцидентами виявлено такі недоліки: утворення черг та низька доступність каналів обробки звернень при масових збоях; На першій лінії реєстрація та класифікація звернень займає значне час, при цьому практично не залишається час для консультування та найважливішим недоліком є не структурованість та неактуальність бази знань, що призводить до неможливості її використання у ході дозволу інциденту; - передача інциденту на 2-й рівень підтримки найчастіше здійснюється до закінчення його дозволу на 1-му рівні. Проблема маршрутизації більшості інцидентів на другу лінію виникає через обмежене часу на пошук відповіді у існуючій базі знань. Зазначена проблема суттєво впливає на швидкість вирішення інциденту; перевищення встановлених термінів обробки інциденту відповідно до прийнятої на підприємстві Угоди про рівень надання послуг (англ. Service Level Agreement, SLA). Кожен інцидент, зареєстрований в інформаційній системі управління інцидентами має свої терміни виконання. Вказані в SLA рівні якості надання послуг, терміни відновлення та час доступності послуг, що надаються, повинні дотримуватися. З урахуванням сказаного, сформульовано завдання:

Розробка моделі процесу управління інцидентами, яка має забезпечити підвищення його ефективності. З цією метою обґрунтовано необхідність

використання набору релевантних метрик, таких як: швидкість усунення інцидентів; задоволеність користувачів якістю IT-підтримки; рівень доступності каналів обробки звернень. Задля більш гнучкого процесу обробки інцидентів розроблена модель процесу управління інцидентами включає додаткову лінію підтримки, що забезпечує обробку складних інцидентів, моніторинг помилок, збоїв, які мають критичний та блокуючий пріоритети, наслідком чого можуть бути великі фінансові ризики, падіння рівня сервісу, доступності і навіть працездатності сервісу (рис. 3.3).

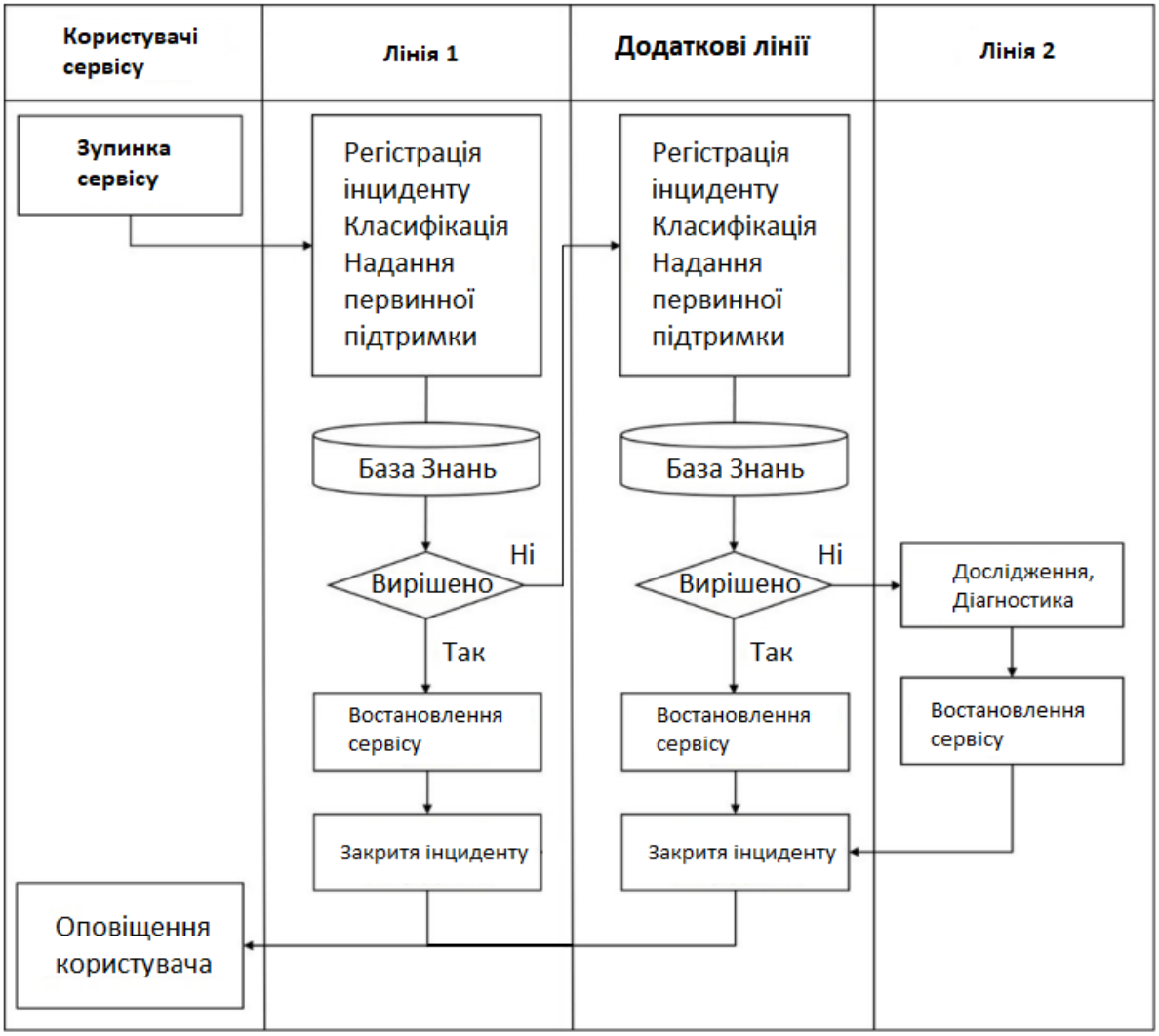

Рисунок 3.3. Вдосконалена модель процесу управління інцидентами

3.3 Рекомендації щодо покращення ефективності

Управління інцидентами – це процес, спрямований на ефективне управління та вирішення проблем і ситуацій, що виникли, з метою мінімізації негативних наслідків для організації та її клієнтів.

Управління інцидентами є важливою частиною інформаційної безпеки та IT-управління в організації. У процесі роботи з комп'ютерними системами та мережами виникають різні інциденти, такі як збої в роботі, порушення безпеки, втрата даних та інші проблеми. Управління інцидентами спрямоване на ефективне та своєчасне реагування на такі інциденти, мінімізацію їх впливу та відновлення нормальної роботи системи.

Управління інцидентами – це процес, спрямований на ефективне та своєчасне реагування на виникнення інцидентів в інформаційних системах чи організаційних процесах. Інцидент – це будь-яка подія, яка призводить до порушення нормального функціонування системи або процесу і вимагає негайного втручання для її усунення та відновлення нормальної роботи.

Мета управління інцидентами – мінімізувати негативні наслідки інцидентів та забезпечити швидке відновлення нормальної роботи системи чи процесу. Для досягнення цієї мети необхідно визначити та застосувати оптимальні методи та інструменти для виявлення, класифікації, пріоритизації, реєстрації, відстеження та усунення інцидентів.

Управління інцидентами є важливою частиною загального процесу управління інформаційною безпекою та дозволяє організаціям оперативно реагувати на загрози та проблеми, пов'язані з інформаційними системами, та мінімізувати їх вплив на бізнес-процеси.

Основними завданнями управління інцидентами є:

- виявлення та реєстрація інцидентів: основне завдання полягає у своєчасному виявленні та реєстрації інцидентів, щоб розпочати їх усунення якомога раніше. Для цього використовуються моніторингові системи, журнали подій та інші інструменти;

- класифікація та пріоритизація інцидентів: кожен інцидент повинен бути класифікований та пріоритизований залежно від його важливості та впливу на бізнес-процеси. Це дозволяє визначити порядок усунення інцидентів та розподілити ресурси ефективно;
- усунення інцидентів: основне завдання управління інцидентами – це оперативне та ефективне усунення інцидентів. Для цього необхідно мати процедури та інструкції щодо усунення різних типів інцидентів, а також забезпечити працівників, відповідальних за усунення, необхідними ресурсами та повноваженнями;
- комунікація та координація - важливим завданням управління інцидентами є організація комунікації та координації дій між різними учасниками процесу. Це включає інформування зацікавлених сторін про хід усунення інциденту, обмін інформацією та узгодження дій;
- аналіз та оцінка ефективності - після усунення інциденту необхідно провести аналіз та оцінку ефективності процесу управління. Це дозволяє виявити причини виникнення інциденту, оцінити ефективність вжитих заходів та вжити додаткових кроків для запобігання повторному виникненню;
- запобігання повторному виникненню - одним із завдань управління інцидентами є запобігання повторному виникненню подібних інцидентів у майбутньому. Для цього необхідно аналізувати причини інцидентів, впроваджувати заходи щодо покращення безпеки та навчати співробітників.

Цілі та завдання управління інцидентами спрямовані на безпеку інформаційних систем організації та мінімізацію ризиків, пов'язаних з інцидентами. Це дозволяє зберегти нормальну роботу бізнес-процесів та захистити конфіденційність, цілісність та доступність даних.

Управління інцидентами ґрунтується на ряді принципів, які допомагають ефективно та систематично реагувати на проблеми, що виникли. Один із основних принципів управління інцидентами – це швидке виявлення та реагування на інциденти. Чим швидше ви виявите інцидент і вживете заходів щодо його усунення, тим меншим буде його вплив на роботу організації.

Важливим принципом є класифікація та пріоритизація інцидентів. Кожен інцидент має бути оцінений за ступенем його впливу на бізнес-процеси та визначено його пріоритет. Це дозволяє оптимізувати роботу з усунення інцидентів та зосередитись на найбільш критичних проблемах.

Принцип комунікації та координації передбачає встановлення ефективного обміну інформацією між усіма учасниками процесу управління інцидентами. Це включає своєчасне інформування про проблеми, обмін досвідом і знаннями, а також узгодження дій для ефективного вирішення інцидентів.

Принцип документування та аналізу передбачає фіксацію всіх деталей інциденту, його наслідків та вжитих заходів щодо його усунення. Це дозволяє провести аналіз причин інциденту, виявити вразливості та проблеми в системі, а також розробити заходи щодо їх запобігання у майбутньому.

Принцип постійного покращення передбачає постійне вдосконалення процесів управління інцидентами. Це включає аналіз ефективності вжитих заходів, впровадження нових технологій і методів, а також навчання співробітників для підвищення їх компетенції в галузі управління інцидентами.

Дотримання цих принципів допоможе організації ефективно управляти інцидентами, мінімізувати їх вплив на бізнес-процеси та забезпечити безпеку інформаційних систем.

Управління інцидентами включає кілька етапів, які допомагають організації ефективно реагувати на проблеми, що виникли, і мінімізувати їх вплив на бізнес-процеси. ~~Розглянемо кожен етап докладніше~~:

На першому етапі управління – виявити інцидент. На цьому етапі відбувається виявлення аномалій, збоїв чи інших проблем, які можуть вплинути на роботу інформаційної системи чи порушити безпеку даних. Виявлення може відбуватися автоматично за допомогою моніторингових систем або повідомлень від користувачів або співробітників.

Після виявлення інциденту необхідно зареєструвати його та провести його класифікацію. Реєстрація дозволяє створити запис про інцидент, що містить інформацію про його характер, час виникнення, місце та інші деталі.

Класифікація інциденту допомагає визначити його пріоритетність та рівень важливості для організації.

На цьому етапі відбувається оцінка та пріоритизація інциденту. Оцінка дозволяє визначити масштаб проблеми, її потенційні наслідки та можливі ризики. Пріоритизація допомагає визначити порядок реагування на інциденти в залежності від їх важливості та впливу на бізнес-процеси.

На цьому етапі відбувається активне реагування на інцидент. Це включає в себе вжиття заходів щодо ліквідації проблеми, відновлення працездатності системи та мінімізації впливу інциденту на бізнес-процеси. Реагування може включати такі дії, як аналіз причин інциденту, вжиття заходів щодо запобігання повторного виникнення і відновлення даних.

Після реагування на інцидент необхідно здійснювати моніторинг та контроль, щоб переконатися, що проблема повністю усунена та не виникають нові інциденти. Моніторинг дозволяє відстежувати стан системи та своєчасно реагувати на будь-які аномалії чи збої. Контроль допомагає перевірити ефективність вжитих заходів та внести необхідні коригування у процес управління інцидентами.

Послідовне виконання цих етапів дозволяє організації ефективно управляти інцидентами, мінімізувати їх вплив на бізнес-процеси та забезпечити безпеку інформаційних систем.

У процесі управління інцидентами виділяються різні ролі та відповідальності, які виконують різні працівники організації. Кожна роль має свої завдання та обов'язки, які спрямовані на ефективне вирішення проблеми та мінімізацію впливу інциденту на бізнес-процеси.

Менеджер управління інцидентами є головним координатором процесу управління інцидентами. Його основне завдання – організувати та контролювати всі етапи управління інцидентами, а також забезпечити своєчасне та ефективне вирішення проблеми. Менеджер з управління інцидентами також відповідає за комунікацію із зацікавленими сторонами та надання їм інформації про поточний стан інциденту.

Фахівець із управління інцидентами є основним виконавцем у процесі управління інцидентами. Він відповідає за аналіз та класифікацію інцидентів, розробку та реалізацію плану дій щодо їх усунення, а також за моніторинг та контроль за процесом вирішення проблеми. Спеціаліст з управління інцидентами також може взаємодіяти з іншими спеціалістами та відділами організації для отримання необхідної інформації та ресурсів.

Команда підтримки складається із фахівців, які надають безпосередню допомогу у вирішенні інцидентів. Це можуть бути IT-фахівці, системні адміністратори, мережеві інженери та інші фахівці, які мають необхідні знання та навички для усунення проблеми. Команда підтримки працює в тісній взаємодії з менеджером з управління інцидентами та спеціалістом з управління інцидентами, щоб забезпечити швидке та ефективне вирішення проблеми.

Користувачі та зацікавлені сторони також відіграють важливу роль в управлінні інцидентами. Вони повинні своєчасно повідомляти про проблеми, що виникли, і надавати необхідну інформацію для аналізу та вирішення інциденту. Користувачі також можуть бути залучені до тестування та перевірки виправленої проблеми, щоб переконатися в її ефективності.

Відпрацьовані рекомендації щодо покращення управління інцидентами.

Управління інцидентами є важливою частиною роботи будь-якої організації, особливо у сфері інформаційних технологій. У таблиці 3.1 представлена порівняльна таблиця управління інцидентами. Ось кілька рекомендацій, які допоможуть покращити процес керування інцидентами:

Створення чіткої та структурованої системи управління інцидентами

Необхідно розробити та впровадити чітку та структуровану систему управління інцидентами. Це включає визначення ролей і відповідальності, встановлення процедур і політик, а також розробку інструментів і методів для відстеження та реєстрації інцидентів.

Важливо навчити та підготувати персонал, який займатиметься управлінням інцидентами. Це включає навчання за методологіями та

процедурами управління інцидентами, а також тренування на симуляторах або практичних вправах.

Необхідно встановити систему моніторингу та оповіщення, яка відстежуватиме стан системи та автоматично сповіщатиме відповідальних осіб про виникнення інцидентів. Це дозволить швидко реагувати на проблеми та запобігати їх розвитку.

Необхідно регулярно оновлювати та тестувати плани управління інцидентами. Це дозволить врахувати зміни у системі та процедурах, а також перевірити їх ефективність. Тестування планів також допоможе навчити персонал та виявити можливі проблеми чи покращення.

Важливо проводити аналіз процесу управління інцидентами та вносити покращення на основі отриманих результатів. Це дозволить оптимізувати процес, покращити його ефективність та знизити ризики виникнення інцидентів.

Дотримання цих рекомендацій допоможе організації покращити свою здатність ефективно керувати інцидентами, мінімізувати їх вплив на бізнес та забезпечити високий рівень обслуговування клієнтів.

Таблиця 3.1

Порівняльна таблиця управління інцидентами

Аспект	Визначення	Властивості
Управління інцидентами	Процес управління та вирішення інцидентів, що виникають в організації	Ціль – мінімізація негативних наслідків інцидентів Завдання – швидке виявлення, аналіз та вирішення інцидентів Принципи – своєчасність, ефективність, прозорість
Цілі і завдання	Мета – мінімізація простою та шкоди від інцидентів, завдання – швидке відновлення сервісів та повідомлення зацікавлених сторін	Цілі – зменшення часу простою, покращення якості обслуговування Завдання – класифікація та пріоритизація інцидентів, комунікація з клієнтами Принципи – оперативність,

Аспект	Визначення	Властивості
		співпраця, безперервне покращення
Етапи управління	Етапи – виявлення, реєстрація, класифікація, пріоритизація, діагностика, рішення, закриття	Виявлення – моніторинг та оповіщення про виникнення інциденту Реєстрація – створення запису про інцидент у системі управління Класифікація – визначення типу та категорії інциденту Принципи – оперативність, співпраця, безперервне покращення

Висновок до 3 розділу. У третьому розділі були розглянуті наступні показники ефективності: середнє напрацювання на відмову, середній час підтвердження, середній час виявлення, та інші, розглянута поточна та представлена вдосконалена модель управління інцидентами, в кінці були представлені рекомендації щодо покращення ефективності управління інцидентами, наприклад: Створення чіткої та структурованої системи управління інцидентами, підготовка, навчання персоналу, встановити систему моніторингу та оповіщення.

Необхідно регулярно оновлювати та тестувати плани управління інцидентами. Це дозволить врахувати зміни у системі та процедурах, а також перевірити їх ефективність. Тестування планів також допоможе навчити персонал та виявити можливі проблеми чи покращення

РОЗДІЛ 4
ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ ВДОСКОНАЛЕНЬ

4.1 Розробка прототипу методом моделювання

В даний час актуальним завданням є підтримка функціонування інформаційної системи підприємства на заданому рівні ефективності. При досить великому потоці заявок, пов'язаних з погіршенням характеристик функціонування інформаційної системи, виникає необхідність оперативного реагування на заявки користувачів з метою мінімізації їх втрат. Один із підходів для вирішення поставленого завдання пов'язаний із застосуванням рекомендацій ITIL у системі управління служби технічної підтримки, які дозволяють суттєво зменшити час реакції на заявки, що надходять, від реальних користувачів за рахунок автоматизації процесу обліку та обробки їх звернень.

В основі побудови математичної моделі обробки заявок, що надходять, доцільно використовувати математичний апарат теорії масового обслуговування (теорії черг).

Для вирішення поставленої задачі систему управління служби технічної підтримки можна уявити, як багатоканальну систему масового обслуговування з відмовами, яка дозволить оцінити такі характеристики як середня кількість зайнятих каналів в даний момент часу та ймовірність відмови в обслуговуванні, які у свою чергу дозволять обґрунтувати рішення щодо вдосконалення системи управління служби технічної підтримки.

Метою дослідження є підвищення ефективності надання інформаційно-комунікаційних послуг шляхом знаходження мінімальної кількості каналів обробки заявок за заданих обмежень.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі завдання:

- аналіз існуючої системи управління інцидентами;

- розробка пропозицій щодо підвищення ефективності функціонування служби технічної підтримки;

- оцінка цільової ефективності розроблених пропозицій.

Як об'єкт дослідження у роботі виступає існуюча система управління технічною підтримкою та вирішення інцидентів.

Предметом дослідження є процеси функціонування системи керування технічної підтримки.

Автоматизація роботи служби технічної підтримки в даний час полягає у прийомі великої кількості звернень від різних джерел: електронна пошта, веб-форми з сайтів, прийом та реєстрація звернень по телефону, прийом службових записок через особистий кабінет користувача та за допомогою порталу самообслуговування.

Всі звернення, що надійшли, оформляються оператором у заявки. Робота із заявками здійснюється за певним алгоритмом, який загалом однаковий у всіх службах технічної підтримки (рис. 4.1).

Рис. 4.1. Існуючий алгоритм роботи з інцидентами

При аналізі існуючої моделі управління інцидентами виявлено такі недоліки:

- утворення черги на лінії при великому потоці дзвінків (заявок);
- обмежений час для консультування та обробки звернень операторами. Реєстрація та класифікація звернень займає значний час;
- недостатня кількість операторів при великому потоці заявок, завантаженість операторів;
- неструктурованість бази знань та її невчасне оновлення. При спробі надання початкової підтримки орієнтуватися в неструктурованій базі знань щодо консультації вкрай складно;
- передача інциденту на 2-й рівень підтримки без його дозволу на 1-му рівні;
- виникнення черги необслужених інцидентів на 2-й лінії підтримки. Великий відсоток спрямованих на 2-у лінії інцидентів - це негативний і вкрай низький показник якості роботи першої лінії підтримки, яка повинна закривати не менше 80% всіх звернень, що надходять;

перевищення встановлених термінів обслуговування інциденту відповідно до Угоди про рівень надання послуг (SLA). Кожен інцидент, зареєстрований в інформаційній системі управління інцидентами, має свої терміни виконання. У угоді про рівень надання послуг (Service Level Agreement (SLA)) вказані рівні якості надання послуг, терміни відновлення та час доступності послуг. При управлінні інцидентами необхідно дотримуватись термінів вирішення інциденту згідно з термінами, зазначеними в Угоді про рівень надання послуг (SLA).

У більшості випадків проблема маршрутизації більшості звернень на другу лінію відбувається через обмежений час на пошуку відповіді в неструктурованій базі знань.

Для побудованої математичної моделі розроблено наступний алгоритм розв'язання задачі, який можна використовувати для розрахунку мінімальної кількості каналів обробки заявок.

Графік станів системи технічної підтримки представлений на рисунку 4.2, де:

λ – інтенсивність вхідних заявок;

μ – інтенсивність обробки заявок;

n – кількість станів;

Si - стан системи технічної підтримки, коли в ній знаходиться і заявок.

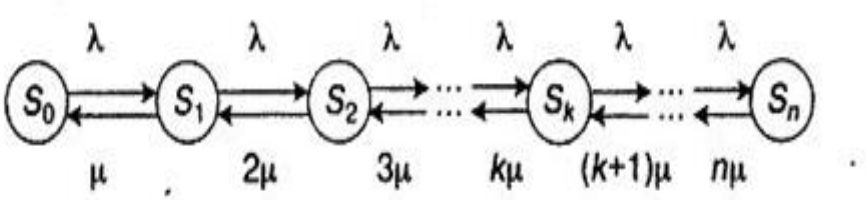

Рис. 4.2. Графік стану системи технічної підтримки

Поданий граф дозволяє вирішити задачу розрахунку ймовірностей переходів зі стану Skв сусідній Sk+1.

Вхідний потік заявок є найпростішим, тому перехід зі стану Si Si +1 відбувається з однією і тією ж інтенсивністю.

Переходи зі стану Si до сусіднього Si+1 відбувається з інтенсивністю k (кратна кількості зайнятих каналів). На основі розподілу Ерланга обчислюється ймовірність відмови P_0, коли система знаходиться в стані S_0, і ймовірність відмови Pi, коли система знаходиться в стані Si:

$$P_0 = \left(1 + \frac{\lambda}{\mu} + \frac{\lambda^2}{2\mu^2} + \frac{\lambda^3}{3!\mu^3} + \ldots + \frac{\lambda^n}{n!\mu^n}\right)^{-1} \quad (1)$$

$$P_i = \frac{\lambda^i}{i!\mu^i} \cdot P_0, \qquad i = 1,2,3,\ldots,n \quad (2)$$

Якщо відношення $\frac{\lambda}{\mu}$ позначити через ρ, то отримаємо:

$$P_0 = \left(1 + \rho + \frac{\rho^2}{2!} + \ldots + \frac{\rho^n}{n!}\right)^{-1} \quad P_i = \frac{\rho^i}{i!} \cdot P_0 \;\; i = 1,2,3,\ldots,n \tag{3}$$

Величина **ρ** визначає середню кількість заявок, що надходять за середній час обслуговування однієї заявки. Її називають коефіцієнтом завантаження системи.

Обчислимо ймовірність відмови системи управління служби технічної підтримки в обслуговуванні заявки:

$$P_{отк} = P_n = \frac{\rho^n}{n!} \cdot P_0 \tag{4}$$

В результаті можна знайти середню кількість зайнятих каналів у поточний момент часу за формулою

$$\bar{k} = \frac{A}{\mu} = \rho \cdot \left(1 - \frac{\rho^n}{n!} \cdot P_0\right) \tag{5}$$

де *A*- середня кількість зайнятих каналів у поточний момент часу;

n – кількість каналів зв'язку.

Отримані значення і дозволяють оцінити ефективність функціонування системи управління службою технічної підтримки та виробити обґрунтовані рішення щодо її вдосконалення.

Отримання шуканого рішення забезпечується порівняно невелика кількість кроків і вимагає великих тимчасових витрат і обчислювальних ресурсів.

Крім розробленого вище алгоритму, підвищення ефективності функціонування служби технічної підтримки пропонується використовувати у

процесі управління інцидентами наступний алгоритм управління інцидентами, представлений на рисунку 4.3.

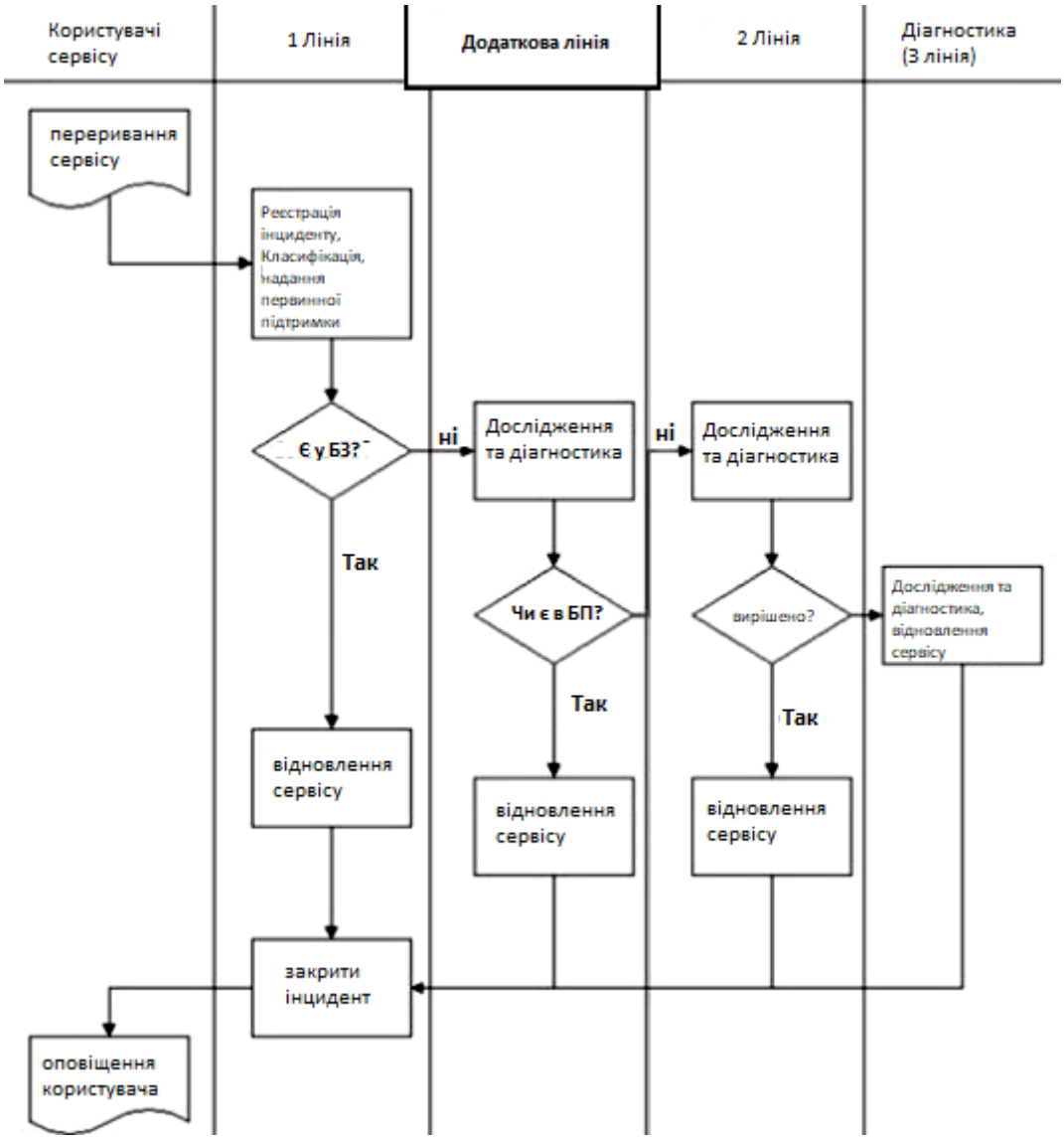

Рис. 4.3 Алгоритм управління інцидентами

Алгоритм управління інцидентами показує запровадження додаткової лінії підтримки з допомогою розподілу завдань 1-ї лінії, розвантаження обов'язків 2-ї лінії. Особливість даної лінії в тому, що вона не вимагає виділення додаткових фахівців, достатньо задіяти частину фахівців з 1 лінії, при цьому виявивши мінімальну кількість каналів обробки заявок при заданих обмеженнях. Функції спеціаліста додаткової лінії технічної підтримки:

- проведення аналізу призначених на робочу групу інцидентів з метою визначення правильності призначення та контролю коректності, вказаних оператором (диспетчером Контакт Центру) даних;
- розподіл інцидентів за фахівцями 2-ї лінії технічної підтримки (інженерам);
- залучення додаткових ресурсів;
- контроль прийняття у роботу та часу виконання інцидентів;
- формування та направлення на регулярній основі спеціалістам 2-ї лінії підтримки переліку стандартних питань, які оператор (диспетчер КЦ) повинен задати Контактній особі при прийомі Звернення;
- вихідні дзвінки та консультування користувачів за вирішеними заявками;
- консультування із бази прецедентів;
- актуалізація бази знань з листа від спеціалістів 2-ї лінії;
- своєчасне інформування про зміни в системі, оновлення або технічні збої, що спостерігаються (за листом від фахівців 2-ї лінії);
- складання звітності про надійшли та направлені заявки, ведення рахунку звернень та інцидентів, оброблених оператором та фахівцями 2-ї лінії;
- своєчасне інформування фахівців 2-ї лінії про заявки, у яких закінчується термін рішення.

Додаткова лінія підтримки використовує базу прецедентів, де вирішуються питання, які були вирішені під час розмови з користувачем.

Дана методика передбачає використання алгоритму управління інцидентами, який показує запровадження додаткової лінії підтримки з допомогою розподілу завдань 1-ї лінії, розвантаження обов'язків 2-ї лінії. Організація додаткової лінії підтримки, яка поділяє обов'язки операторів, підвищує показники ефективності служби технічної підтримки.

Розрахунок кількості операторів при великому потоці заявок проводиться згідно з алгоритмом розв'язання задачі знаходження мінімальної кількості каналів обробки заявок при заданих обмеженнях. Рекомендується застосовувати блок-схему цього алгоритму, попередньо реалізувавши її у вигляді програми

однією з мов об'єктно-орієнтованого програмування для прискорення розрахунків.

Запропонована методика дозволяє розрахувати достатню кількість фахівців при великому потоці заявок, тим самим зменшити кількість неприйнятих дзвінків та незареєстрованих заявок. Пропозиція щодо структуризації бази знань та впровадження бази прецедентів дозволяє прискорити процес обробки заявок фахівцями 1-ї лінії.

Актуалізація та структурування бази знань можлива за класифікацією звернення. Наприклад, у зверненні завжди вказується тематика питання, до якої послуги, що надається технічною підтримкою, належить те чи інше питання, до якого пріоритету належить, і який термін SLA виділено для вирішення проблемного питання. Якщо базі знань інформація буде структурована в такий спосіб, але можна провести прив'язку бази знань із системою управління інцидентами.

В результаті застосування запропонованої методики передбачається зменшення кількості заявок, переданих фахівцям 2-ї лінії, що дозволить інженерам дотримуватися обумовленого терміну виконання заявки.

4.2 Тестування та оцінка результатів

З метою проведення імітаційних експериментів для дослідження поведінки математичної моделі ГРІІБ використано програмний пакет реалізації імітаційної моделі досліджуваної ГРІІБ, тобто M/M/1/0 із підвищенням інтенсивності надходження заявки за умови незайнятості системи (модель СМО з навантаженням). Для здійснення моделювання вибрано мову програмування Python, яка застосовується для рішень широкого спектру завдань, зокрема, для роботи з даними у наукових дослідженнях, DataMining, DataScience тощо. Використаний ряд бібліотечних та сторонніх модулів, серед яких: пакети NumPy, Pandas, бібліотека Matplotlib зі стеку SciPy; Statsmodels, Plotly тощо.

Програмний продукт розбитий на модулі: динаміки вхідних даних; попередніх вихідних даних з прогнозованими аналітично розрахованими показниками ефективності; для проведення експерименту; серії експериментів; отримання графічних даних, зокрема 3D графіка; статистичної обробки за переліком метрик.

До вхідних даних моделювання належать: інтенсивність потоку заявок λ (інтенсивність надходження заявок), параметр навантаження α (параметр підвищення інтенсивності надходження заявок), продуктивність каналу (серверу) обслуговування заявок (інтенсивність обслуговування заявок), кількість реалізацій μ (кількість циклів для проведення сценаріїв в рамках одного експерименту) та кількість проведених експериментів N_e.

З використанням вхідної інформації програма забезпечує генерацію послідовностей випадкових чисел: $\tau^{\alpha\lambda}, \tau^{\lambda}, \eta^{\mu}$ – показниково розподілені випадкові величини відповідно до параметрів $\alpha\lambda, \lambda, \mu$. На рис. 4.4 вказані вхідні значення параметрів для моделювання роботи системи та представлені гістограми щільності розподілів інтервалів години надходження заявок і розподілу години обслуговування заявок для різних вхідних параметрів та графіки значень інтервалів між надходженням заявок для вхідного потоку чи інтервалу години для обслуговування в межах кількості циклів експерименту.

Рисунок 4.4 демонструє подання Пуассонівського вхідного потоку в варіаціях: інтенсивності надходження заявок у звичайному режимі функціонування системи, виділено синім кольором, та з застосуванням параметра підвищення цієї інтенсивності – виділено червоним кольором.

Оскільки параметр, використаний для генерації інтервалів часу обслуговування – виділено зеленим кольором, найбільший, то спостерігається фіксація відповідних пропорційних значень.

Закон розподілу станів системи (1), (2), на відміну від середньої кількості заявок у ній (завантаженості), більш повно характеризує функціонування СМО під впливом випадкових факторів. Таким чином у ланцюзі Маркова потік

випадкових величин визначається лише імовірністю переходу (3) від попереднього значення випадкової величини (стану системи) до наступного.

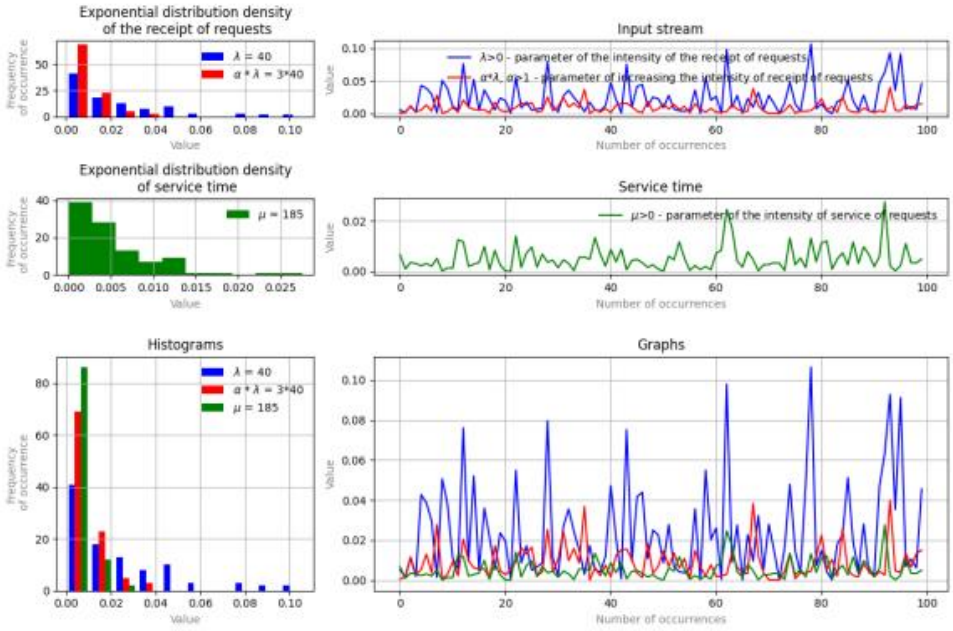

Рис. 4.4. Приклади гістограм щільності розподілів та графіків послідовностей випадкових значень для характеристик ГРІІБ

Приклад масиву даних, що моделює поведінку системи, що досліджується, продемонстровано на рис. 4.5.

lambda	alpha * lambda	mu	from_state1_to01	system_in_state0_intensive	system_in_state1
0.019834775862926236	0.028755848548413416	0.003946903136970928	0	0.028755848548413416	0.003946903136970928
0.03863564658508987	0.0024761127253955808	0.002216281963840574	0	0.0024761127253955808	0.002216281963840574
0.015536290861032327	0.003088377881424763	0.002015935296157324	0	0.003088377881424763	0.002015935296157324
0.0037814969975190 42	0.0023840602354755053	0.002202640388163617	0	0.0023840602354755053	0.002202640388163617
0.0024651177601278623	0.010271570538348842	0.006024260823362612	1	0.010271570538348842	0.0024651177601278623
0.011196225608147063	0.00713635495061559	0.0030586442251805735	0	0.00713635495061559	0.0030586442251805735
0.015959951560756157	0.009043218809090483	0.002204326844936368 6	0	0.009043218809090483	0.002204326844936368 6
0.0454970613786084	0.014576436099344718	0.002133863981164457	0	0.014576436099344718	0.002133863981164457
0.024679951316641087	0.008899182210496659	0.00707429450535314	0	0.008899182210496659	0.00707429450535314
0.03368252511098172	0.006981755879556672	0.013030878316272606	0	0.006981755879556672	0.013030878316272606
0.004589970393518583	0.004327952193881813	0.006125574016003025	1	0.004327952193881813	0.004589970393518583
0.031417355593235226	0.0033272547168088197	0.004746763319601698	0	0.0033272547168088197	0.004746763319601698
0.04135329789677394	0.0035501210466522 9	0.002112988447065639 4	0	0.0035501210466522 9	0.002112988447065639 4
0.007969852663897641	0.011860365369183052	0.010801548849876259	1	0.011860365369183052	0.007969852663897641
0.016326839833657236	0.015606040339828217	0.000161414643807734206	0	0.015606040339828217	0.000161414643807734206
0.012594111452934481	0.004144727055692858	0.003964226736402503	0	0.004144727055692858	0.003964226736402503
0.02499284630305134	0.003251202902945514	0.002103124229362223 7	0	0.003251202902945514	0.002103124229362223 7
0.008492785863792604	0.0017734360683349098	0.003916599801790467	0	0.0017734360683349098	0.003916599801790467
0.054235840071181575	0.0066690839611641154	0.004710545357725302	0	0.0066690839611641154	0.004710545357725302

Рис. 4.5. Дані експерименту для моделі ГРІІБ

Рисунок 4.5 демонструє проведення кожного окремого експерименту, зокрема генерацію послідовностей випадкових чисел необхідних для

забезпечення проведення експерименту, значення стану якому перебуває система та інтервалі часу перебування у відповідних станах, що відповідає аналітичному опису діяльності ГРІІБ в умовах навантаження у межах марківського процесу ξ(t), який характеризується множиною станів $\{e_0, e_1\}$ та умовами переходу до відповідних станів (1) та (2).Для СМО граничний розподіл ймовірностей станів ланцюга Маркова не повинен залежати від початкового розподілу і визначається перехідною матрицею, ймовірність станів у міру збільшення переходів практично перестають змінюватись і система переходити до стаціонарного режиму функціонування. За результатами проведеного експерименту отримаємо (рис. 4.6.) значення експериментальних практичних статистичних характеристик та теоретичних, аналітично розрахованих за формулами для M/M/1/0 з підвищенням інтенсивності надходження вимоги за умови незайнятості системи (4).

static_characteristics	theoretical	practical
π_0	0.6066	0.6015
π_1	0.3934	0.3985
total_system_uptime	-	1.0000

Рис. 4.6. Результати теоретичних та імітаційних статистичних характеристик

Серія експериментів моделювання функціонування M/M/1/0 з підвищенням інтенсивності надходження вимоги за умови незайнятості системи в рамках одного експерименту формує вибірку стаціонарних параметрів системи для статистичного дослідження рисунок 4.7.

practical π_0	practical π_1
0.6022455267485098	0.39775447325149005
0.6406159078058036	0.3593840921941965
0.6442642936624592	0.355735706337541
0.6220262690359886	0.3779737309640115
0.5913479104059476	0.4086520895940524
0.5914650743122567	0.4085349256877433
0.571009460933337	0.428990539066663
0.6423990176429085	0.3576009823570915
0.6670377194389605	0.3329622805610394
0.5827047548230427	0.41729524517695715

Рис. 4.7. Приклад потоку даних для вибірки експериментальних даних

Алгоритм управління інцидентами на Python може бути реалізований за допомогою наступних кроків (рис.4.8).

Перший крок - ідентифікація інциденту. Це можна зробити, відстежуючи повідомлення про помилки, моніторинг даних продуктивності або отримуючи повідомлення від користувачів.

```python
def identify_incident():
    # Перегляньте повідомлення про помилки
    for error_message in error_messages:
        # Якщо повідомлення про помилку відповідає критеріям інциденту,
        if error_message.severity >= CRITICAL:
            # Інцидент виявлено
            return True

    # Перегляньте дані продуктивності
    for metric in metrics:
        # Якщо значення метрики перевищує допустимий діапазон,
        if metric.value > metric.threshold:
            # Інцидент виявлено
            return True

    # Отримайте повідомлення від користувачів
    for user_message in user_messages:
        # Якщо повідомлення користувача відповідає критеріям інциденту,
        if user_message.subject == "Incident":
            # Інцидент виявлено
            return True

    return False
```

Рис. 4.8 Ділянка коду, щ вілповілає за виявлення інциденту

Після виявлення інциденту його потрібно оцінити, щоб визначити його вплив і пріоритет (рис.4.9).

```python
def evaluate_incident(incident):
    # Визначте вплив інциденту
    incident.impact = calculate_impact(incident)

    # Визначте пріоритет інциденту
    incident.priority = calculate_priority(incident)

    return incident
```

Рис. 4.9. Код оцінки інциденту

Після оцінки інциденту необхідно розгорнути план реагування. План реагування визначає кроки, які необхідно виконати для усунення інциденту (рис. 4.10).

```python
def deploy_response_plan(incident):
    # Ідентифікуйте відповідальних осіб
    incident.responsible_parties = identify_responsible_parties(incident)

    # Визначте кроки, які необхідно виконати
    incident.steps = identify_steps(incident)

    # Почніть виконувати кроки
    for step in incident.steps:
        step()
```

Рис. 4.10. Код плану реагування на інциденти

Після розгортання плану реагування необхідно спостерігати за інцидентом, щоб переконатися, що він усунений (рис. 4.11).

```python
def monitor_incident(incident):
    # Перегляньте повідомлення про помилки
    for error_message in error_messages:
        # Якщо повідомлення про помилку пов'язане з інцидентом,
        if error_message.incident_id == incident.id:
            # Інцидент не усунено
            return False

    # Перегляньте дані продуктивності
    for metric in metrics:
        # Якщо значення метрики все ще перевищує допустимий діапазон,
        if metric.value > metric.threshold:
            # Інцидент не усунено
            return False

    # Інцидент усунено
    return True
```

Рис. 4.11. Код моніторингу інцидентів

Коли інцидент усунений, його необхідно завершити. Це включає в себе закриття всіх відповідних квитків і записів (рис. 4.12).

```python
def close_incident(incident):
    # Закрийте всі квитки, пов'язані з інцидентом
    for ticket in incident.tickets:
        ticket.close()

    # Запишіть інформацію про інцидент
    log_incident(incident)

    return incident
```

Рис. 4.12. Код закриття тікетів, та запис інциденту в базу

Вивід записаного журналу представлен на малюнку 4.13

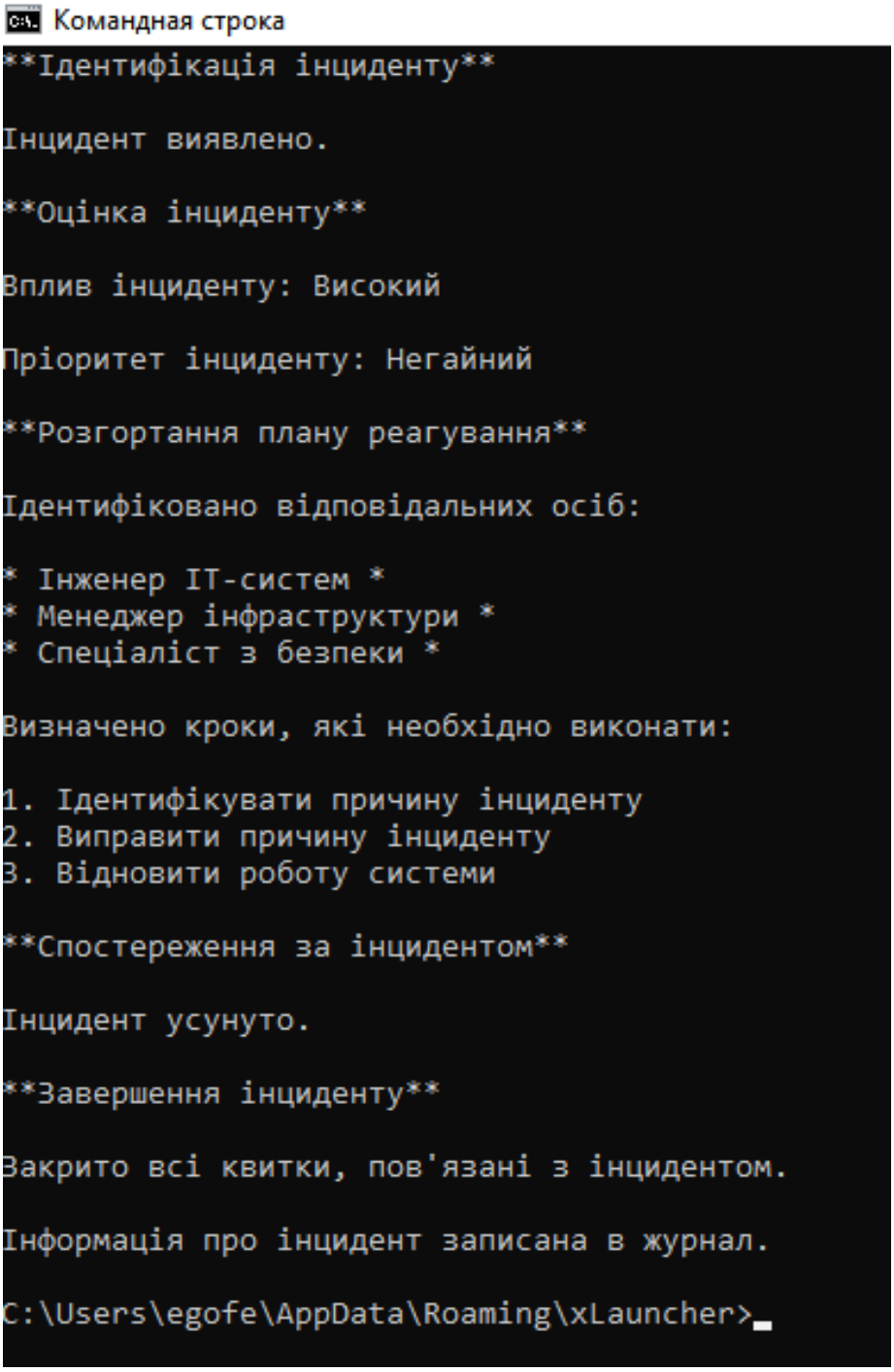

Рис. 4.12. Результат обробки інциденту записаного в журнал

4.3 Висновки та рекомендації для подальшого розвитку управління інцидентами в автоматизованих системах

Управління інцидентами – один із найважливіших процесів, які компанія має правильно налаштувати. Збої в обслуговуванні можуть дорого коштувати компанії, тому командам необхідно швидко та ефективно реагувати на такі проблеми та вирішувати їх. Командам потрібен надійний спосіб розставити пріоритети інцидентів, швидко дозволити їх та надати користувачам обслуговування належного рівня. Процес управління інцидентами дозволяє IT-командам розслідувати, реєструвати та вирішувати такі проблеми, як збої в роботі сервісу та простої в обслуговуванні. Робочий процес управління інцидентами ITIL націлений на скорочення часу простою та зменшення впливу інцидентів на роботу співробітників. Використовуючи шаблони для керування інцидентами, ви можете створити робочі процеси, що відтворюються, завдяки яким ваші команди зможуть реєструвати, діагностувати і дозволяти інциденти, а також вести їх хронологію. Методологія ITIL переважно використовується в IT сфері для вирішення інцидентів внутрішніх служб компанії. ITIL описує майже всі види інцидентів та проблем, з якими можуть зіткнутися IT-фахівці, тому зазвичай команди беруть тільки те, що потрібно саме їм. ITIL відмінно підходить для розвитку в команді культури активного пошуку та усунення несправностей. Описані процеси допомагають командам відстежувати інциденти і послідовно вирішувати їх, вести звітність і аналізувати їх, щоб удосконалювати обслуговування і зростати як успішна команда. Згідно з останніми рекомендаціями щодо ITIL, традиційним IT-командам слід керувати як проблемами, так і інцидентами, але робити це окремо. Управління проблемами - це практика, спрямована на запобігання інцидентам або зменшення їхнього впливу. Управління інцидентами наголошує на усуненні інцидентів у режимі реального часу. Перевага підходу ITIL полягає в тому, що він приділяє першорядну увагу основним цілям управління і проблемами та інцидентами. Ймовірно, поділ їх на окремі та рівнозначно важливі практики у керівних

принципах - це спроба уникнути загальної проблеми IT-команд: постійного вирішення інцидентів без усунення їхньої причини. Якщо основною метою менеджера інцидентів є швидке вирішення інцидентів, а основною метою менеджера проблем – їх запобігання, то при об'єднанні цих ролей може виявитися так, що одна з цих життєво важливих для організації цілей виключена з пріоритетних на користь іншої. Недоліком цього підходу є те, що при поділі цих двох практик, які так тісно пов'язані в реальності, можуть з'явитися прогалини у знаннях та порушення зв'язку між вирішенням інцидентів та аналізом основних причин, що ведуть до першопричини. Застосування ІІ та машинного навчання в кібербезпеці має ряд переваг, такі як підвищена точність визначення та запобігання загрозам, прискорення процесів обробки даних, прогнозування ймовірних атак та багато інших. Однак, воно також становить певні ризики, пов'язані з атаками на системи ІІ. Для мінімізації подібних загроз необхідно розвивати інтенсивні заходи щодо покращення безпеки систем ІІ, такі як забезпечення шифрування даних, фільтрація та аналіз аномальної активності.

ВИСНОВКИ

Захист АСУ є критично важливим, тому що атака на промислові об’єкти завдає більше збитків, ніж викрадення даних у бізнесу або впровадження ransomware в якийсь офіс. Простій соцмереж або неробочий банкінг – це, звичайно, неприємно, але не зрівняється із ситуацією, коли цілі міста можуть опинитись бути без світла чи води, чи коли не можуть працювати цілі вузли інфраструктури, і це не кажучи про можливі техногенні катастрофи.

В першому розділі розглянуто основні поняття АСУ, опис процесів управління в автоматизованих системах, що потребують захисту, основні проблеми управління інцидентами АСУ, також розглянута класифікація інцидентів в АСУ.

В другому розділі було детальніше розкриті типи інцидентів, та їх класифікація, також було описано деякі приклади інцидентів. Проведено аналіз існуючих процедур та методів управління інцидентами, оцінено вплив інцидентів на функціонування автоматизованих систем. Також оцінено ефективність існуючих методів та практик управління інцидентами.

В третьому вперше визначені комплексні критерії ефективності автоматизованої системи управління інцидентами та їх показників. Описаний процес удосконалення моделі системи управління інцидентами введенням додаткової автоматизованої лінії управління на основі результатів попередніх обробок. Представлено рекомендації щодо покращення ефективності.

У заключній частині - змоделював покращену систему обробки заявок інцидентів, для мінімізації втрат, з використанням мови програмування Python та бібліотек NumPy, Pandas, бібліотека Matplotlib зі стеку SciPy; Statsmodels, Plotly, на основі моделі були проведені тести і оцінка результатів. Реалізація запропонованого підходу дозволила суттєво підвищити значення зазначених показників (швидкості вирішення інцидентів – на 7,4%, ступеня задоволеності користувачів – на 13.6%, доступності каналів обробки звернень – на 7,8%.На

основі отриманих результатів були зроблені висновки та рекомендації для подальшого розвитку управління інцидентами в автоматизованих системах.

Розроблені рекомендації щодо підвищення ефективності управління інцидентами в АСУ які включають: регулярне проведення аудиту кібербезпеки АСУ, а також навчання персоналу з питань кібербезпеки, використання тільки сучасних систем виявлення вторгнень, а також розроблення процедури реагування на інциденти кібербезпеки. Також потрібно постійно підсилювати профілактичні заходи, постійне впровадження систем виявлення та реагування на інциденти IDS/IPS.

Реалізація цих пропозицій дозволяє підвищити ефективність управління інцидентами кібербезпеки в АСУ і захистити критичну інформаційну інфраструктуру системи від кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яновський О. Кібербезпека та управління ризиками IT. KPMG. URL: https://kpmg.com/ua/uk/home/services/consulting/technology/information-protection-and-cyber-security.html (дата звернення: 03.10.2023).

2. ERP Project. Автоматизація управління бізнес-процесами: за і проти. ERP Project. URL: http://erp-project.com.ua/index.php/uk/korisni-materiali/statti/upravlinnya/497-avtomatizatsiya-upravlinnya-biznes-protsesami-za-i-proti (дата звернення: 03.10.2023).

3. Учасники проектів Вікімедіа. Автоматизована система керування – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Автоматизована_система_керування (дата звернення: 03.10.2023).

4. ProNET. Системи інформаційної безпеки. ProNET. URL: https://pronet.ua/sistemi-informaczijnoi-bezpeki/ (дата звернення: 04.10.2023)

5. Перелік Національних стандартів України для створення, впровадження та супроводження автоматизованих і інформаційних систем | Національна бібліотека України імені В. І. Вернадського. Національна бібліотека України імені В. І. Вернадського. URL: http://nbuv.gov.ua/node/1469 (дата звернення: 05.10.2023).

6. Автентифікація, авторизація та ідентифікація: як не сплутати | Онлайн-курси від компанії QATestLab. Онлайн-курси від компанії QATestLab | Головна сторінка. URL: https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/ (дата звернення: 04.10.2023).

7. Аудит інформаційної безпеки: що це, види | Блог Colobridge. blog.colobridge.net. URL: https://blog.colobridge.net/uk/2023/06/information_security_audit-ua/ (дата звернення: 03.10.2023).

8. Colobridge. Аудит інформаційної безпеки: що це і навіщо потрібно,

коли проводити. Colobridge. URL: https://cip.gov.ua/ua/news/protidiya-kiberzagrozam-ta-zakhist-ob-yektiv-kritichnoyi-infrastrukturi-sered-prioritetiv-derzhspeczv-yazku. (дата звернення: 05.10.2023).

9. Від інциденту до вирішення: основні кроки протидії та відновлення у випадку кібератаки. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/ot-intsidenta-k-resheniyu-osnovnyye-shagi-protivodeystviya-i-vosstanovleniya-v-sluchaye-kiberataki/ (дата звернення: 06.10.2023).

10. Технічний захист інформації - IT-Solutions, Україна. IT-Solutions, Україна. URL: https://it-solutions.ua/tehnichnij-zahist-informatsiyi/ (дата звернення: 06.10.2023).

11. Харківський національний університет внутрішніх справ. URL: https://www.univd.edu.ua/general/publishing/konf/06_12_2019/pdf/58.pdf (дата звернення: 06.10.2023).

12. Web Academy Media. Що таке DevSecOps?. Web Academy Media. URL: https://web-academy.ua/blog/junior/what-is-devsecops (дата звернення: 02.10.2023).

13. Шифрування та захист баз даних. IITD Inteligent IT Distribution. URL: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/ (дата звернення: 02.10.2023).

14. Захист даних і систем від зловмисних загроз - Підтримка від Microsoft. Microsoft Support. URL: https://support.microsoft.com/uk-ua/office/захист-даних-і-систем-від-зловмисних-загроз-9c03cf4e-8c2c-47e9-8a07-7270b2a81b2c (дата звернення: 06.10.2023).

15. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. Державний університет телекомунікацій. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf?file=p_303_79299367.pdf (дата звернення: 01.12.2023).

16. Безпека для мережі автоматизованих пралень. Ajax Systems. URL: https://customers.ajax.systems/ua/study-laundry-self-service (дата звернення: 06.10.2023).

17. Пам’ятка щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет. Михайлівська громада Запорізька область, Василівський район. URL: https://mihajlivska.gromada.org.ua/news/1613648057/ (дата звернення: 06.10.2023).

18. Хмарна безпека: ключові поняття, загрози та рішення – IT-компанія SL Global Service. IT-компанія SL Global Service – IT-компанія SL Global Service. URL: https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html (дата звернення: 06.10.2023).

19. Перевірка стійкості паролю на предмет атак вгадування. elakpi: Home. URL: https://ela.kpi.ua/bitstream/123456789/25296/1/S.122-125.pdf (дата звернення: 04.10.2023).

20. LibreTexts. Управління ризиками проекту. LibreTexts - Ukrayinska. URL: https://ukrayinska.libretexts.org (дата звернення: 04.10.2023).

21. Поглиблена співпраця компанії Siemens і НАТО в галузі кібербезпеки критично важливих об’єктів інфраструктури | Press | Company | Siemens. Press | Company | Siemens. URL: https://press.siemens.com/ua/uk/presreliz/pogliblena-spivpracya-kompanii-siemens-i-nato-v-galuzi-kiberbezpeki-kritichno-vazhlivikh (дата звернення: 04.10.2023).

22. Novak N. Від штучного інтелекту до квантових обчислень: інновації в кібербезпеці. Dou. URL: https://dou.ua/forums/topic/33707/ (дата звернення: 08.10.2023).

23. Мялковський Д. В. Науково методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Shon1. URL: https://shron1.chtyvo.org.ua/Semenchenko_Andrii/Naukovo-metodolohichni_pidkhody_do_provedennia_ohliadu_kiberzakhystu.pdf (дата звернення: 08.10.2023).

24. Охорона здоров’я та безпека праці в галузі IT. Важливі вимоги до роботодавців та працівників - Охорона праці і пожежна безпека. Охорона праці і пожежна безпека. URL: https://oppb.com.ua/articles/ohorona-zdorov-ya-ta-

bezpeka-pratsi-v-galuzi-it-vazhlyvi-vymogy-do-robotodavtsiv-ta-pratsivnykiv (дата звернення: 08.10.2023).

25. Рішення для кібербезпеки. Schneider Electric. URL: https://www.se.com/ua/uk/work/solutions/cybersecurity/ (дата звернення: 08.10.2023).

26. Що таке реагування на інциденти?. Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-incident-response (дата звернення: 15.10.2023).

27. Що таке автоматизація інцидентів?. Unite.AI. URL: https://www.unite.ai/uk/what-is-incident-automation/ (дата звернення: 15.10.2023).

28. Перелік категорій кіберінцидентів. Державна служба спеціального зв`язку та захисту інформації України. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv (дата звернення: 15.10.2023).

29. Від інциденту до вирішення: основні кроки протидії та відновлення у випадку кібератаки. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/ot-intsidenta-k-resheniyu-osnovnyye-shagi-protivodeystviya-i-vosstanovleniya-v-sluchaye-kiberataki/ (дата звернення: 17.10.2023).

30. Academic Journals and Conferences. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3663/harasymyurromakavarybiimm.pdf (дата звернення: 17.10.2023).

31. Що таке автоматизація інцидентів?. Unite.AI. URL: https://www.unite.ai/uk/what-is-incident-automation/ (дата звернення: 17.10.2023).

32. Оркестрація, автоматизація і реагування, SOAR. IITD Inteligent IT Distribution. URL: https://iitd.com.ua/orkestracija-avtomatizacija-i-reaguvannja-soar/ (дата звернення: 18.10.2023).

33. Петрашко В. Дослідження існуючих підходів для створення безпечної мережі. Молодий вчений. URL: https://molodyivchenyi.ua/index.php/journal/article/view/6034 (дата звернення: 19.10.2023).

34. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Методичні_рекомендації_щодо_управління_операційним_ризиком_опі.pdf?v=4 (дата звернення: 19.10.2023).

35. Why Your Organisation Needs Automated Incident Management. Crises Control. URL: https://www.crises-control.com/blogs/automated-incident-management/ (дата звернення: 19.10.2023).

36. FAQ: What Is Automated Incident Response?. The New Stack. URL: https://thenewstack.io/faq-what-is-automated-incident-response/ (дата звернення: 19.10.2023).

37. The Impact of AI on Proactive Incident Management - IBM Blog. IBM Blog. URL: https://www.ibm.com/blog/announcement/the-impact-of-ai-on-proactive-incident-management/ (дата звернення: 18.10.2023).

38. Top 5 Reasons to Invest in an Automated Incident Response System. LogRhythm. URL: https://logrhythm.com/blog/top-5-reasons-to-invest-in-automated-incident-response/ (дата звернення: 18.10.2023).

39. Impact of Security on Automated Test Systems. Mess- und Prüfsysteme, bei Emerson - NI. URL: https://www.ni.com/en/support/security/impact-automated-test-systems.html (дата звернення: 17.10.2023).

40. VIA Process Automation: Detect and Resolve Issues Before Impact. Vitria. URL: https://www.vitria.com/via-process-automation (дата звернення: 17.10.2023).

41. How to automate incident response to security events with AWS Systems Manager Incident Manager | Amazon Web Services. Amazon Web Services. URL: https://aws.amazon.com/ru/blogs/security/how-to-automate-incident-response-to-security-events-with-aws-systems-manager-incident-manager/ (дата звернення: 20.10.2023).

42.What is Security Automation?. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-security-automation (дата звернення: 20.10.2023).

43.What is security automation?. Red Hat - We make open source technologies for the enterprise. URL: https://www.redhat.com/en/topics/automation/what-is-security-automation (дата звернення: 20.10.2023).

44. Incident Management: Assessing Long-Term Impact and Success. Medium. URL: https://medium.com/@manojsebastiankulatharayil/measuring-the-success-of-an-incident-management-process-c95fffe124d2 (дата звернення: 15.11.2023).

45. 10 Strategies for a More Effective Incident Management Process. Xybiot. URL: https://www.xybion.com/blog/10-strategies-for-a-more-effective-incident-management-process/ (дата звернення: 15.11.2023).

46. Parikka K. Understanding Incident Reporting Friction: Its Significance and Impact. Blog | Falcony. URL: https://blog.falcony.io/en/understanding-incident-reporting-friction (дата звернення: 15.11.2023).

47. Udasi A. Incident Management KPIs Guide | Zenduty. Zenduty Blog - Incident Management & Alerting. URL: https://www.zenduty.com/blog/incident-management-kpis/ (дата звернення: 15.11.2023).

48. 10 Keys To An Effective Post-Incident Management Review & Analysis. Jensen Hughes. URL: https://www.jensenhughes.com/insights/10-keys-to-an-effective-post-incident-management-review (дата звернення: 17.11.2023).

49. Guide to ISO 27001 incident management - Sprinto. Sprinto. URL: https://sprinto.com/blog/how-to-implement-iso-27001-incident-management/ (дата звернення: 17.11.2023).

50. IT incident management process: 8 steps with examples. ManageEngine ServiceDesk Plus. URL: https://www.manageengine.com/products/service-desk/it-incident-management/what-is-it-incident-management.html (дата звернення: 17.11.2023).

51. SAP Help Portal. SAP Help Portal. URL:

https://help.sap.com/docs/EHSM/a4a3b0356a634323b471315055ef1ab7/0a94b243bc7646499fed391e1f37eb49.html?version=5.0 (дата звернення: 17.11.2023).

52. Incident Response Guide: Best Practices | Squadcast. Squadcast | Incident Management | Incident Response | SRE | DevOps. URL: https://www.squadcast.com/blog/incident-response-guide (дата звернення: 17.11.2023).

53. Zuridinova Z. Incident Management Metrics That Matter. Custom Software Development Company. URL: https://maddevs.io/blog/incident-management-metrics-guide/ (дата звернення: 19.11.2023).

54. Дьогтєва І. О., Шиян А. А. Моделювання роботи групи реагування на інциденти інформаційної безпеки в умовах зростання інтенсивності кібератак | Вісник Вінницького політехнічного інституту. Вісник Вінницького політехнічного інституту. URL: https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/2715 (дата звернення: 02.12.2023).

55. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Головна сторінка DSpace. URL: https://ir.nmu.org.ua/handle/123456789/151308 (дата звернення: 05.12.2023).

56. Кібервплив і кіберзахист в умовах війни. Одеська національна наукова бібліотека. Офіційний веб-сайт.
URL: https://odnb.odessa.ua/view_post.php?id=4361 (дата звернення: 04.12.2023).

57. Modelling language for cyber security incident handling for critical infrastructures. ScienceDirect.
URL: https://www.sciencedirect.com/science/article/pii/S0167404823000494 (дата звернення: 02.12.2023).

58. Dhamankar R. 5 steps to implement threat modeling for incident response | TechTarget. Security. URL: https://www.techtarget.com/searchsecurity/post/5-steps-to-implement-threat-modeling-for-incident-response (дата звернення: 02.12.2023).

59. Creating a cybersecurity response team for SMEs. Bocasay. URL: https://www.bocasay.com/cybersecurity-incident-response-team-sme/ (дата звернення: 05.12.2023).

60. Modelling language for cyber security incident handling for critical infrastructures : UEL Research Repository. Welcome to UEL Research Repository : UEL Research Repository. URL: https://repository.uel.ac.uk/item/8vv52 (дата звернення: 20.12.2023).

61. Incident Response Models. ISACA. URL: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models (дата звернення: 10.12.2023).

62. NIST Incident Response Plan: Building Your IR Process. Cynet. URL: https://www.cynet.com/incident-response/nist-incident-response/ (дата звернення: 09.12.2023).

63. 6 steps to accelerate cybersecurity incident response. SC Media. URL: https://www.scmagazine.com/native/6-steps-to-accelerate-cybersecurity-incident-response (дата звернення: 04.12.2023).

64. Cybersecurity Incident Response in Organizations: An Exploratory Case Study and Process Model of Situation Awareness. The Univercity of Melbourne. URL: https://findanexpert.unimelb.edu.au/scholarlywork/1481155-cybersecurity-incident-response-in-organizations--an-exploratory-case-study-and-process-model-of-situation-awareness (дата звернення: 15.12.2023).

65. Incident Response Steps and Frameworks for SANS and NIST. AT&T Cybersecurity | Managed Security Services for Network, XDR & more. URL: https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide (дата звернення: 19.11.2023).

66. Cyber Security Incident Response Maturity Assessment. CREST. URL: https://www.crest-approved.org/buying-building-cyber-services/cyber-security-incident-response-maturity-assessment/ (дата звернення: 13.12.2023).