**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**
**КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«__»_____ 2021 р.

На правах рукопису
УДК 004.056.510(043.2)

**ДИПЛОМНА РОБОТА**
**ЗДОБУВАЧА ВИЩОЇ ОСВІТИ**
**ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»**

**Тема:** Програмний застосунок для управління інцидентами інформаційної безпеки

**Виконавець:** Д.Я. Махачек

**Керівник:** д.т.н., проф. В.А. Лахно
**Нормоконтролер:** д.т.н., проф. В.А. Лахно

**Київ 2021**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп'ютерної та програмної інженерії

**Кафедра:** Комп'ютеризованих систем захисту інформації

**Освітній ступінь:** «Бакалавр»

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма:** «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«____»_____ 2021 р.

**ЗАВДАННЯ**

**на виконання дипломної роботи**

**здобувача вищої освіти Махачека Дмитра Ярославовича**

1. Тема: *Програмний застосунок для управління інцидентами інформаційної безпеки*

затверджена наказом ректора від 29.04.2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021р. по 20.06.2021р.

3. Вихідні дані: проаналізувати методи, моделі, системи виявлення інцидентів інформаційної безпеки; розробка методу контролю та виявлення інцидентів інформаційної безпеки; проведення експериментального дослідження розробленого застосунку.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці): аналіз методів та засобів обробки інцидентів інформаційної безпеки; розробка застосунку контролю та виявлення інцидентів інформаційної безпеки в мережі; тестування та дослідження розробленого застосунку.

# КАЛЕНДАРНИЙ ПЛАН

## виконання дипломної роботи

| № п/п | Етапи виконання дипломної роботи | Термін виконання етапів | Примітка |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 16.04.2021 | *Виконано* |
| 2 | Аналіз методів, моделей, систем обробки інцидентів інформаційної безпеки в ІКС | 10.05.2021 | *Виконано* |
| 3 | Обґрунтування вибору рішення | 11.05.2021 | *Виконано* |
| 4 | Розробка застосунку контролю та виявлення інцидентів інформаційної безпеки в мережі | 15.05.2021 | *Виконано* |
| 5 | Тестування та дослідження розробленого застосунку | 20.05.2021 | *Виконано* |
| 6 | Оформлення і друк пояснювальної записки | 30.05.2021 | *Виконано* |
| 7 | Оформлення презентації | 01.06.2021 | *Виконано* |
| 8 | Отримання відгуку керівника | 02.06.2021 | *Виконано* |
| 9 | Отримання рецензії | 05.06.2021 | *Виконано* |
| 10 | Перевірка на антиплагіат | 07.06.2021 | *Виконано* |

Здобувач вищої освіти _____ Д.Я. Махачек

(підпис, дата)

Керівник дипломної роботи _____ В.А. Лахно

(підпис, дата)

# РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків, загальний обсяг роботи складає 78 сторінок, має 19 рисунків, 21 таблицю та 8 сторінок додатків. Список використаних джерел містить 62 найменування і займає 7 сторінок.

Метою дипломної роботи є підвищення ефективності управління інцидентами інформаційної безпеки шляхом розробки програмного застосунку контролю та виявлення інцидентів.

В дипломній роботі розглянуті питання аналізу методів та моделей, контролю та виявлення. Проаналізовано та запропоновано метод контролю та виявлення інцидентів інформаційної безпеки.

Запропоновано метод виявлення інцидентів інформаційної безпеки, за рахунок якого можна буде спрогнозувати настання інцидентів інформаційної безпеки.

Запропонований метод може використовуватися у реальних практичних СЗІ для моніторингу інцидентів інформаційної безпеки в ІКС.

Ключові слова: контроль, виявлення, інциденти інформаційної безпеки, методи та моделі, інформаційно-комунікаційні системи.

# ЗМІСТ

# ВСТУП

**Актуальність.** Протягом останніх років спостерігається тенденція до підвищення уразливості інформаційних систем (ІС) до інцидентів інформаційної безпеки. Тому актуальним є пошук ефективних методів контролю та виявлення інцидентів в ІС. Разом з тим збільшилась кількість досліджень у питаннях контролю та виявлення інцидентів, які принципово відрізняються від існуючих, традиційних методів контролю, виявлення та прогнозування. Методи моніторингу у галузі інформаційної безпеки, що застосовуються на сучасному етапі, мають деякі недоліки і не завжди враховують нові причини, через які можуть виникнути інциденти в ІС і як їх можна попередити. Тому, актуальним є дослідження методів контролю та виявлення інцидентів інформаційної безпеки і створення нового методу контролю та виявлення інцидентів інформаційної безпеки в ІС.

Інцидент – будь-яка не прогнозована або небажана подія, яка може порушити діяльність або інформаційну безпеку.

В роботі сучасних систем моніторингу інцидентів виділяються наступні етапи: встановлення інциденту; надання інформації про виникнення інциденту; фіксація та реєстрація інциденту; мінімізація наслідків і усунення причин інциденту; дослідження витоків інциденту; реалізація дій, що застерігають повторне виникнення інциденту. Основною метою є розробка системної моделі моніторингу інцидентів.

**Метою дипломної роботи** є підвищення ефективності управління інцидентами інформаційної безпеки шляхом розробки програмного застосунку контролю та виявлення інцидентів.

Досягнення мети потребує розв’язання таких **задач**:

- проведення аналізу методів та засобів прогнозування та моніторингу інцидентів інформаційної безпеки в ІС;

- розробка програмного застосунку на основі методу контролю та виявлення інцидентів інформаційної безпеки;
- тестування та дослідження розробленого застосунку.

**Об'єкт дослідження:** процес виявлення інцидентів інформаційної безпеки в ІС.

**Предмет дослідження:** методи та засоби контролю та виявлення інцидентів інформаційної безпеки в ІС.

**Галузь застосування.** Даний застосунок контролю та виявлення інцидентів інформаційної безпеки в ІС може використовуватися на підприємствах для підвищення ефективності управління інцидентами.

**Новизна.** Набула подальшого розвитку розробка програмних засобів управління інцидентами ІБ, за рахунок використання методу контролю та виявлення інцидентів, що дозволяє проводити моніторинг інцидентів інформаційної безпеки, прогнозувати їх вплив на складові інформаційно-комунікаційних систем і обирати відповідні превентивні заходи.

**Практична цінність** полягає у тому, що за допомогою запропонованого метода створена можливість у реальних практичних системах захисту інформації визначити необхідні заходи щодо ліквідації наслідків кожного виду інцидентів інформаційної безпеки; сформувати цілі паралельної ліквідації можливих видів інцидентів інформаційної безпеки, здійснити їх синхронізацію, ранжування; втілити реалізацію паралельних стратегій цілей, забезпечити синхронізацію і взаємодію залучених сил і засобів; сформувати можливий набір паралельних оперативних впливів, провести їх диспетчеризацію, синхронізацію і здійснити маневрування силами і засобами в динаміці управління кіберінцидентами; забезпечити попередження виникнення інцидентів інформаційної безпеки.

# Розділ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1. Аналіз систем моніторингу

### JSOC: Моніторинг інцидентів:

В сучасних умовах жоден комплекс програмно-технічних засобів, що підтримується відповідним штатом фахівців з інформаційної безпеки не здатний забезпечити ефективне функціонування системи захисту інформації. Дане питання вимагає системного підходу та розробки комплексних систем управління безпекою, в яких мають брати безпосередню участь всі співробітники організації. Задачами системи управління інформаційною безпекою є систематизація процесів забезпечення захисту інформації, розташування пріоритетів організації в галузі захисту інформації, забезпечення адекватності системи існуючим ризикам тощо. В роботі сучасних систем моніторингу інцидентів в виділяються наступні етапи: визначення інциденту; сповіщення про виникнення інциденту; реєстрація інциденту; усунення наслідків і причин інциденту; розслідування інциденту; реалізація дій, що застерігають повторне виникнення інциденту. Основною метою є розробка системної моделі моніторингу інцидентів. Згідно з переліком функції системи управління інцидентами її можна віднести до систем моніторингового типу, отже для розробки математичної моделі її функціонування можна використати методи ідентифікації систем відповідного класу [1].

Об’єктами системи моніторингу інцидентів є:

- апаратні засоби (комутатори, маршрутизатори, сканери, UTM пристрої);
- програмні комплекси (операційні системи, антивірусні шлюзи, персональні антивірусні системи, підсистеми обробки даних, доступні служби та сервіси);

- інформаційні ресурси (бази даних, файли користувачів доступні в мережі тощо);
- дії користувачів корпоративної мережі [2].

У загальному вигляді система моніторингу структується на декілька рівнів прийняття рішень. На нульовому рівні проводиться спостереження, збір, первинна обробка даних, формування системи знань. На першому, другому і третьому рівнях послідовно здійснюється обробка даних, з проходженням всіх етапів, передбачених моделлю. Виконання робіт на даних етапах здійснюється системним аналітиком з метою отримання експертної оцінки поточного і прогнозованих станів об'єктів моніторингу. На цих етапах поповнюються динамічні знання системи. На четвертому рівні особа, що приймає рішення, на основі оцінок стану системи, генерує рішення по управляючій дії на об'єкти моніторингу і системи спостереження [1].

Також на даний час популярними інструментами моніторингу інцидентів стали сервіси JSOC. JSOC – один перших комерційних центрів моніторингу та реагування на інциденти ІБ. Він є провайдером сервісів безпеки (MSSP), таких як виявлення, реагування та розслідування інцидентів в цілодобовому режимі; аналіз і пріоритизація вразливостей як елементів базової інфраструктури, так і коду бізнес-додатків; відображення цільових APT-атак; виявлення заражених хостів мережі таргетованим шкідливим ПЗ і захист web-додатків в тому числі від DDoS.

На всіх етапах моніторингу і реагування на інциденти ІБ здійснюється забезпечення захист клієнтських даних. Забезпечення безпеки реалізовано як на фізичному, так і на інформаційному рівні за допомогою засобів розмежування доступу, аудиту роботи фахівців JSOC, контролю цілісності та захисту даних при передачі. JSOC сертифікований за вимогами PCI DSS, що підтверджує зрілість процесів забезпечення безпеки.

Уже більше десятка клієнтів отримують аутсорсингові послуги JSOC. Перший сервіс з моніторингу інцидентів був запущений в 2013 році, та став

одним з перших комерційних центрів. Зараз в штаті JSOC більше 30 фахівців чергової зміни, аналітиків і експертів, які обробляють понад 75 000 подій з підозрою на інциденти в рік.

JSOC – це набір сервісів ІБ для моніторингу інцидентів і протидії сучасним загрозам.

JSOC: Моніторинг інцидентів – це сума технологій і практик виявлення інцидентів, гарантований SLA розбору інцидентів і кваліфікований персонал, що працює 24x7.

JSOC надає сервіси, починаючи з довготривалого зберігання подій ІБ до моніторингу та розслідування інцидентів, виявлених за допомогою кореляційних правил. При цьому моніторинг інцидентів ведеться як в базовій інфраструктурі, так і на рівні додатків і користувачів з використанням відомостей про виявлені цільових атаках і zero-day кіберзагрози.

Платформа моніторингу інцидентів JSOC базується на відмовостійкій конфігурації системи HP ArcSight ESM, до якої додатково підключені джерела даних про недовірених IP, URL і бот-мережах. Компанія Solar Security має партнерські відносини з провідними лабораторіями, що займаються виявленням атак і протидією кіберзлочинності: Kaspersky Lab, Group-IB, а також організований інформаційний обмін з комерційним ресурсом CERT. Така співпраця дозволяє агрегувати інформацію про погрози, виявляти більше інцидентів і виявляти zero-day атаки в найкоротші терміни.

**Використання «JSOC: Моніторинг інцидентів» необхідно, якщо в організації:**

- Складна інфраструктура, що має критичні бізнес-системи, що знаходяться під загрозою зовнішніх і внутрішніх порушників ІБ.
- Безліч систем безпеки залишаються без належної уваги на реєстровані в них події ІБ.
- Відсутня можливість виділити команду для оперативного реагування та розбору інцидентів.

- Рідко вдається знайти порушників, відповідальних за виникнення інцидентів.
- Розроблено регламенти та політики ІБ, але не проводиться технічний контроль їх виконання.

**Проблеми, які вирішує «JSOC: Моніторинг інцидентів»:**

- Більшість серйозних інцидентів залишається непоміченою вчасно.
- Про інцидент стає відомо за непрямими ознаками або за зверненнями з боку клієнтів і партнерів.
- Значний період налаштування і введення в експлуатацію свого SOC, відсувають початок отримання від нього користі.
- Відсутнє розуміння варіантів інцидентів, можливих в інфраструктурі і додатках.

**Переваги «JSOC: Моніторинг інцидентів»:**

- Моніторинг та розбирання інцидентів в режимі 24x7 при повному дотриманні гарантованого рівня SLA.
- Швидкий старт, опрацювання сценаріїв інцидентів і підключення до центру моніторингу протягом 4 тижнів.
- Агрегація власної аналітики при хакерських угрупованнях, бот-мережах і недовірених IP-адреси з даними від декількох зарубіжних і російських лабораторій.
- Більше 1500 кореляційних правил, об'єднаних в 174 націлених сценаріїв інцидентів ІБ, розроблених для компаній різних галузей російського ринку.
- Організовано інформаційний обмін та співробітництво з провідними CERT і аналітичними центрами Kaspersky Lab і Group-IB для оперативної протидії кіберзлочинності.
- Перехресне інформування схожих по інфраструктурі клієнтів про виявлені атаках.
- Довгострокове розподіл інвестицій в ІБ з можливістю гнучкого масштабування послуг під актуальні потреби бізнесу.

**Склад послуги:**

- Підключення до JSOC систем ІБ, ІТ-сервісів, робочих станцій привілейованих співробітників і серверів СУБД і додатків в якості джерел подій ІБ.
- Розробка конекторів під нетипові системи, збір і довготривале зберігання подій ІБ з метою проведення розслідувань і виконання нормативних вимог.
- Вибір з каталогу JSOC і моніторинг релевантних сценаріїв інцидентів в базовій інфраструктурі.
- Профілювання активності користувачів і додатків для виявлення аномалій.
- Аналіз програм, роботи користувачів і адміністраторів з точки зору бізнес-процесів, розробка унікальних сценаріїв інцидентів під кожного клієнта.
- Виявлення zero-day атак шляхом зіставлення агрегованих даних про кіберзагрози і подій ІБ клієнтів.
- Моніторинг 24x7 інцидентів і реагування відповідно до прийнятого SLA.
- Розбір інцидентів, фільтрація помилкових спрацьовувань, встановлення первинних причин їх виникнення.
- Підготовка звіту про інцидент.
- Подальше проведення розслідувань із збиранням цифрових доказів.
- Перехресне оновлення сценаріїв інцидентів після виявлених векторів загроз в клієнтах JSOC[4].

**Аналіз сучасного програмного забезпечення по управлінню інцидентами ІБ:**

Сучасний ринок автоматизованих систем та програмних комплексів щодо виявлення й управління інцидентами є досить насиченим. Усі продукти різняться своїм функціоналом та можливостями але більшості систем

притаманні такі основні недоліки, як висока вартість програмного продукту, різні програмні платформи, відсутність шаблонів тощо.

Основними програмними продуктами, які мають попит на сучасному ринку є:

1. **EnCase Enterprise** – мережеве програмне забезпечення, що використовується для проведення власного аудиту, віддаленого всередині корпоративного розслідування інцидентів з використанням комп'ютерного обладнання, розслідування діяльності співробітників компанії або будь-яких інцидентів, пов'язаних з несанкціонованим доступом до комп'ютерної інформації [5].

2. **OTRS ITSM** – програмне забезпечення для управління інцидентами; мінімізації негативних впливів на бізнес і забезпечує ефективну реєстрацію і обробку інцидентів, використовуючи, в тому числі, інтегровану конфігураційну базу даних для аналізу інцидентів та інтелектуальні засоби автоматизації для якнайшвидшого відновлення працездатності IT [6].

3. **BPMonline Service Desk** – рішення, яке володіє всіма перевагами системи управління бізнес-процесами (BPM) і повністю відповідає рекомендаціям бібліотеки ITIL. Робота BPMonline Service Desk полягає у веденні обліку інцидентів, подій, які впливають на якість реалізованих товарів або послуг, що надаються [7].

4. **NetForensics** – система управління інформаційною безпекою, якапризначена для роботи з гетерогенним середовищем продуктів забезпечення інформаційної безпеки і реалізує безперервний збір, обробку і відображення подій безпеки [8].

5. **SysAid Pro** – це комплексне і разом з тим спрощене рішення для довідкових служб IT, яке допоможе ефективно обробляти запити на послуги, точніше управляти ресурсами і автоматизувати всі IT-процеси підприємства[9].

6. **Axios Assyst 7 –** програмний продукт, який має особливість вбудованого редактора потоків робіт, що дозволяє описати життєвий цикл стандартних змін і запитів на обслуговування в залежності від їх типу [10].

7. **BMC Remedy ITSM Suite 7.5 –** клієнт-серверна середовище для побудови додатків, що розробляється компанією BMC Software (спочатку розроблялася Remedy Corporation). Спершу орієнтувалася на розробку тікет-систем, але успішно застосовується для створення додатків будь-яких типів. ARS використовує зовнішню базу даних (DB2, MS SQL Server, Oracle, і ін.) для зберігання даних і вихідного коду програми (workflow). Найбільш поширений в США і Європі [11].

8. **HP Service Manager 7 –** програмний додаток, який характеризується: розвиненим функціоналом автоматизації ITSM-процесів; вміщує в собі документована процесну модель; наявність розвиненого Web-інтерфейсу [12].

9. **Naumen Service Desk** – програмне забезпечення, яке дозволяє реалізувати сервісний підхід в різних службах підприємств, а також – автоматизувати процеси обслуговування в сервісних компаніях, що працюють за моделлю аутсорсингу. Основними перевагами є: настройка шаблонів інцидентів і запитів на обслуговування, класифікація щодо ієрархічної структури сервісів і угод, а також щодо конфігураційних одиниць у володінні користувача, контрольований доступ до записів по всіх інцидентах і запитах на обслуговування [13].

Аналіз та порівняння програмних продуктів, які мають попит на сучасному ринку представлено в табл. 1.1.

*Таблиця 1.1*

Аналіз сучасного програмного забезпечення по управлінню інцидентами ІБ

| № п/п | Назва | Вартість | | Сумісність з ОС | Статистика, звіти | Моніторинг мережі | Категоризація | Журнал зміни | Надання пріоритету | Багатомовний інтерфейс | Шаблони e-mail оповіщень | Моніторинг IP та мак-адреси, з якої |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | демо | Ліцензовані ПЗ | | | | | | | | | |
| **1** | **BPMonline Service Desk Concurrent** | + | 300€ | -Microsoft Windows - UNIX. | + | + | + | + | + | - | - | - |
| **2** | **OTRS IT Service Management** | + | 500€ | Linux; - UNIX, такі як OpenBSD, FreeBSD - Windows. | + | - | - | + | - | - | - | - |
| **3** | **EnCase Enterprise** | + | 350€ | Windows, UNIX, Linux, Solaris, Mac OS X, NetWare. | + | + | + | - | + | + | - | - |
| **4** | **nFX Log One** | - | 200€ | Windows XP/2005 MS SQL Server 2005. | +- | - | + | - | - | - | + | - |
| **5** | **SysAid** | + | 320€ | Linux, UNIX. | - | - | - | + | + | + | + | - |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **6** | **BMC Remedy ITSM Suite 7.5** | + | 850 | Windows XP/2005, Linux та ін. | - | - | + | + | - | + | + | - |
| **7** | **Axios Assyst7.5** | - | $400 | Windows. | + | - | + | - | + | + | - | - |
| **8** | **HP Service Manager 7.10** | + | $800 | Linux, UNIX, FreeBSD, Windows. | - | + | + | - | + | - | - | - |
| **9** | **Naumen Service Desk** | + | $900 | Windows, UNIX, Linux, Mac OS X. | + | + | + | + | + | + | + | - |

*Продовження табл.1.1*

**Моніторинг подій і виявлення інциденту інформаційної безпеки з використанням SIEM-систем**

Забезпечення інформаційної безпеки (ІБ) є важливим завданням для різних організацій. Виконання цієї нетривіальної задачі вимагає значних фінансових і трудових витрат. Важливо розуміти, що ці витрати зроблені даремно, якщо система захисту інформації при цьому діє недостатньо швидко і продуктивно. Тому останнім часом все більш актуальною стає проблема моніторингу подій ІБ (далі – подій), а також виявлення та обробка виникаючих інцидентів ІБ (далі – інцидентів) в мінімальні терміни.

Ключовим поняттям в даній області є «подія інформаційної безпеки», для якого в сучасному законодавстві прийнято наступне визначення:

Подія – ідентифіковане поява певного стану системи, сервісу або мережі, що вказує на можливе порушення політики ІБ або відмова захисних заходів, або виникнення невідомої раніше ситуації, яка може мати відношення до безпеки [14, 15].

Моніторинг подій проводиться на основі даних, отриманих з різних джерел, до яких відносяться:

- IDS / IPS-системи;
- засоби антивірусного захисту;
- журнали подій;
- сканери вразливостей;
- DLP-системи,
- мережеве обладнання;
- інші джерела.

Кількість джерел подій зростає з ростом організації, тобто з ростом числа серверів, автоматизованих робочих місць, мережевого обладнання та інших об'єктів інфраструктури. Інформація з різних джерел зберігається окремо, має різні формати, і, як наслідок, ніяк не пов'язана між собою. Для великих організацій важко обробляти досить швидко і ефективно такий потік подій обмеженим персоналом підрозділу, відповідального за моніторинг. Це проявляється в низькій швидкості виконання аналізу подій, його якості і невиявлених взаємозв'язків між подіями, які є симптомами інциденту [16].

Проблеми моніторингу подій негативно впливають на виявлення інцидентів.

Інцидент – поява одного або декількох небажаних або несподіваних подій, з якими пов'язана значна ймовірність компрометації бізнес-операцій і створення загрози ІБ [14].

Інцидент – будь непередбачене або небажана подія, яка може порушити діяльність або інформаційну безпеку [15].

Інцидент – подія або комбінація подій, яка вказує на доконаний, що вживаються або ймовірну реалізацію загрози ІБ, результатом якої є:

- порушення або можливе порушення роботи засобів захисту інформації в складі СОІБ організації;
- порушення або можливе порушення вимог законодавства, нормативних актів і розпоряджень регулюючих і наглядових органів, внутрішніх документів організації БС РФ в області забезпечення ІБ, порушення або можливе порушення у виконанні процесів СОІБ організації;
- порушення або можливе порушення у виконанні банківських технологічних процесів організації;
- нанесення або можливе нанесення збитку організаціїі (або) її клієнтам [17, 18].

Визначення вище розрізняються, але всі вони, так чи інакше, вказують на заподіяння негативних наслідків процесу, інформаційній системі, організації в результаті виникнення інциденту. Таким чином, своєчасне виявлення інциденту мінімізує втрати організації.

В умовах децентралізації інформації про події з багатьох джерел виявлення інциденту стає складною і не завжди вирішуваною завданням. Після виявлення інциденту необхідно ідентифікувати постраждалі активи, зрозуміти причини інциденту, оцінити його ступінь тяжкості, пріоритет, вжити заходів щодо реагування. При виконанні цих операцій виконавці часто стикаються з тією ж проблемою розрізненості джерел інформації. Це проявляється в неналежному реагуванні або його відсутності, що тягне за собою збитки організації.

SIEM-система дозволяє уникнути зазначених вище проблем. Вона вирішує завдання зі збору та зберігання інформації з різних джерел, аналізувхідних подій, їх кореляції і обробці за правилами, виявлення інцидентів, їх пріоритетності та автоматичного оповіщення. Крім того, SIEM-

системи часто мають можливість проведення перевірки на відповідність стандартам.

Типова структура SIEM-систем:

- агенти – встановлюються на інформаційну систему і передають дані з неї на сервер, до складу агентів можуть включатися модулі для перетворення даних;
- сервер-колектор – збирає події від безлічі джерел;
- сервер-коррелятор – збирає і обробляє інформацію від колекторів і агентів;
- сервер баз даних – зберігає журнали подій [19].

SIEM-система збирає інформацію з різних джерел за допомогою агентів і серверів-колекторів в централізоване сховище даних, що дозволяє згодом аналізувати події в цілому. Також це дозволяє уникнути розрізненої і, в переважній кількості випадків, неконтрольованої конфігурації засобів аналізу подій. Негативним моментом такого побудови системи є зростання навантаження на мережу організації [20].

Після збору інформації SIEM-система починає аналіз подій ІБ, що потребується для виявлення інциденту. Для цього застосовуються 2 основні методи кореляції: сигнатурний (тобто на основі правил) і бесігнатурний, що визначає аномальну поведінку інформаційної системи. За результатами аналізу SIEM-система показує виявлені інциденти ІБ.

Для того щоб SIEM-система ефективно виконувала свої завдання в конкретній організації, потрібно правильна конфігурація кореляційних механізмів і постійна їх модифікація. Внаслідок цього SIEM-системи починають окупати себе значно пізніше її впровадження, особливо при застосуванні бесігнатурних методів кореляції, які вимагають накопичення статистичних даних. Налаштуванням SIEM-системи організації, як правило, займається експерт, який пройшов спеціальні курси і має певний досвід в цій області [21].

Крім основного завдання з моніторингу подій і виявлення інцидентів на основі даних про критичність активів організації і небезпеки загрози SIEM-системи можуть пріоритезувати інциденти, автоматично оповіщати про інцидент, видавати заздалегідь підготовлені рекомендації щодо негайного реагування на інцидент, зберігати дані про інцидент для подальшого розслідування.

На даний момент на ринку SIEM-систем можна виділити наступні продукти:

- HP ArcSight.
- McAfee Nitro.
- IBM QRadar.
- Splunk SIEM.
- RSA Security Analytic.
- LogRhythm.

Застосування SIEM-системи не є обов'язковим при побудові комплексної системи захисту інформації та в багатьох випадках недоцільно. Основним замовником таких систем є великі організації, в яких потрібно безперервний контроль за забезпеченням ІБ і журнал пов'язаних з цим подій [22, 23].

**Реєстрація інцидентів з використанням кнопки допомоги ITSM**

Для якісного та швидкого реагування на інциденти та їх автоматичну реєстрації можна використовувати кнопку допомоги ITSM [24].

Автоматична реєстрація інцидентів з використанням Кнопки Допомоги ITSM (раніше: Червона Кнопка ITSM) – це повна або часткова автоматизація процесів реєстрації, кваліфікації, маршрутизації і діагностики інциденту. Інциденти можуть генеруватися як безпосередньо за допомогою кнопки Допомоги ITSM (пряма реєстрація інцидентів), так і системою моніторингу на підставі скарг користувачів (реєстрація агрегованих інцидентів). Спрощена схема прямої реєстрації інцидентів показана на малюнку (див. рис. 1.1).


Рис. 1.1. Спрощена схема прямої реєстрації інцидентів

**1. Пряма реєстрація інцидентів.**

**Автоматична реєстрація інцидентів для підтримки бізнес-додатків:**

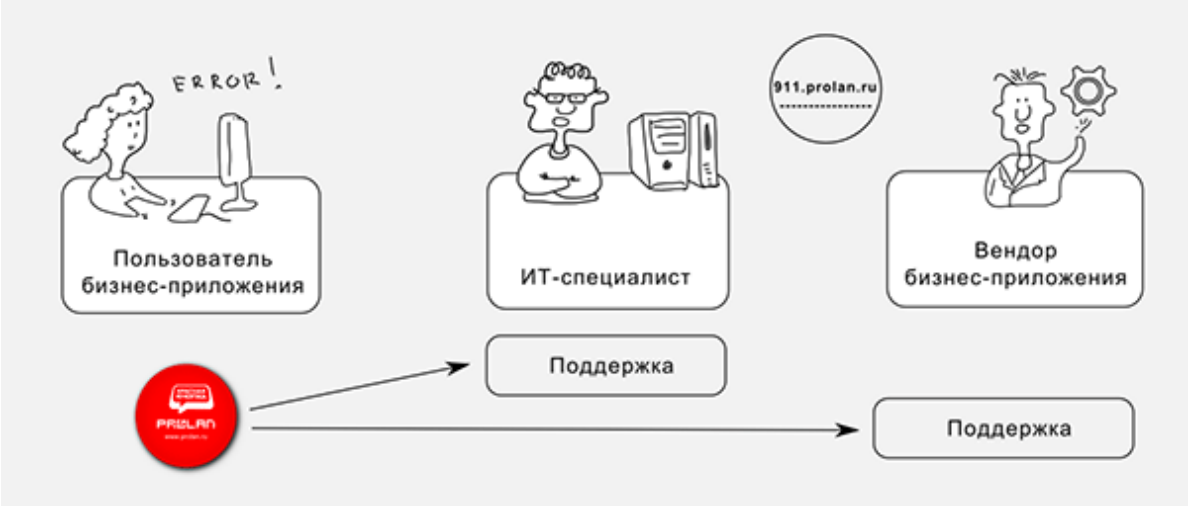



Рис. 1.2. Схема застосування Кнопки Допомоги ITSM для підтримки бізнес-додатків

Кнопка Допомоги ITSM встановлюється на комп'ютер кінцевого користувача бізнес-додатки. Кнопка Допомоги ITSM – це програма EPM-Agent Plus і, опціонально, апаратна кнопка – USB-девайс ProLAN-101. Для зв'язку з Service Desk - системою використовуються протоколи SMTP або HTTP. Якщо постачальник сервісу використовує систему моніторингу, Кнопка Допомоги

ITSM може відсилати повідомлення також в систему моніторингу (див. рис. 1.2).

**Реєстрація інциденту:**

Користувач натискає «червону кнопку» при виникненні інциденту – події, яка не є частиною нормальної роботи IT-сервісу, здатного привести до повного припинення функціонування сервісу або зниження рівня його якості (ITIL v.3).

Кнопка Допомоги ITSM збирає інформацію про оточення (робить скріншот, отримує заголовок вікна переднього плану, змінні середовища і т.п.) і відкриває діалогове вікно, в якому користувач вибирає бажану дію («Зареєструвати інциденту») і вказує тип інциденту. Додаток і бізнес-операція, яку виконував користувач вже визначені [25].

Після натискання кнопки «ОК» і автоматичного виконання тематичних перевірок (залежних від зазначеного додатка, бізнес-операції і типу інциденту) Кнопка Допомоги ITSM формує Знімок Інциденту і реєструє інцидент в Service Desk з використання протоколів SMTP або HTTP(див. рис. 1.3).

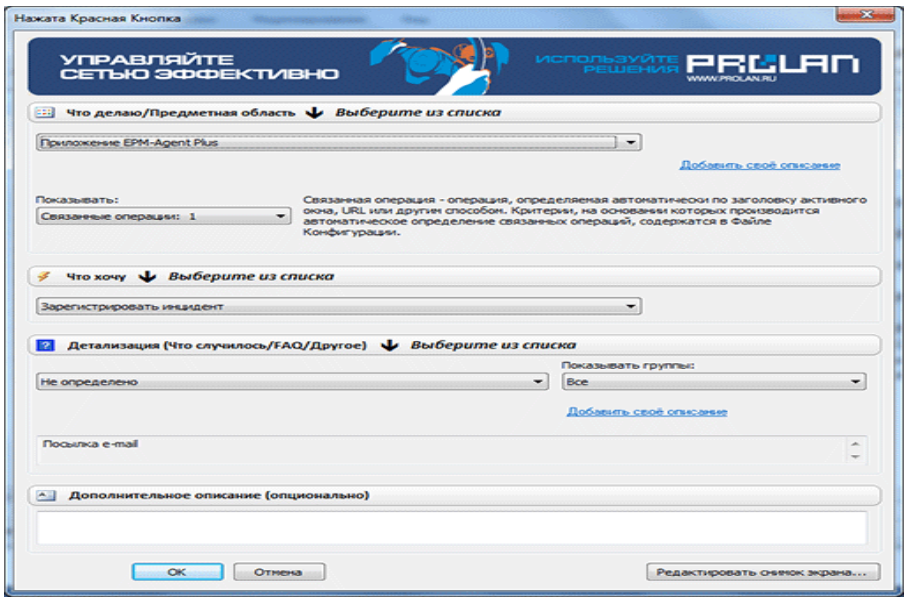



Рис. 1.3. Реєстрація інциденту в Service Desk

**Класифікація інциденту:**

Зазвичай, щоб повідомити службі Service Desk про інцидент, користувачеві потрібно зателефонувати, написати електронного листа або заповнити веб-форму, але отриманої інформації часто буває недостатньо. Тому

оператор першої лінії підтримки, отримавши повідомлення про інцидент, зазвичай повинен задати користувачеві ряд уточнюючих питань. Час, що витрачається на отримання адекватних відповідей, залежить від безлічі факторів, зокрема, від комунікативних навичок користувача. Знімок Інциденту, який передається за допомогою кнопки Допомоги ITSM в Службу підтримки, як правило, включає досить інформації для кваліфікації інциденту.

**Маршрутизація інциденту:**

Кнопка допомоги ITSM маршрутизує знімок Інциденту потрібного фахівця в залежності від програми, в якому стався інцидент, бізнес-операції і типу інциденту. Можлива також автоматична маршрутизація Знімка Інциденту в різні Service Desk - системи.

**Діагностика інциденту:**

Кнопка Допомоги ITSM автоматично збирає ряд діагностичних даних з боку користувача, які можуть бути корисні в діагностиці інциденту:

- скріншот екрану (доступний для редагування користувачем щоб уникнути витоку конфіденційної інформації);
- назва процесу і заголовок вікна переднього плану;
- виконувана бізнес-операція;
- облікові дані користувача;
- змінні середовища;
- результати контекстних перевірок (залежать від програми, бізнес-операції і типу інциденту).

Повний набір діагностичних даних, що характеризують інцидент з боку користувача, називається знімки Інциденту.

Велика частина діагностичних даних збирається без будь-якої участі користувача, ще до відкриття діалогового вікна. Контекстні перевірки виконуються після відкриття діалогового вікна і вказівки типу інциденту.

**Автоматична реєстрація інцидентів для підтримки IT-інфраструктури:**

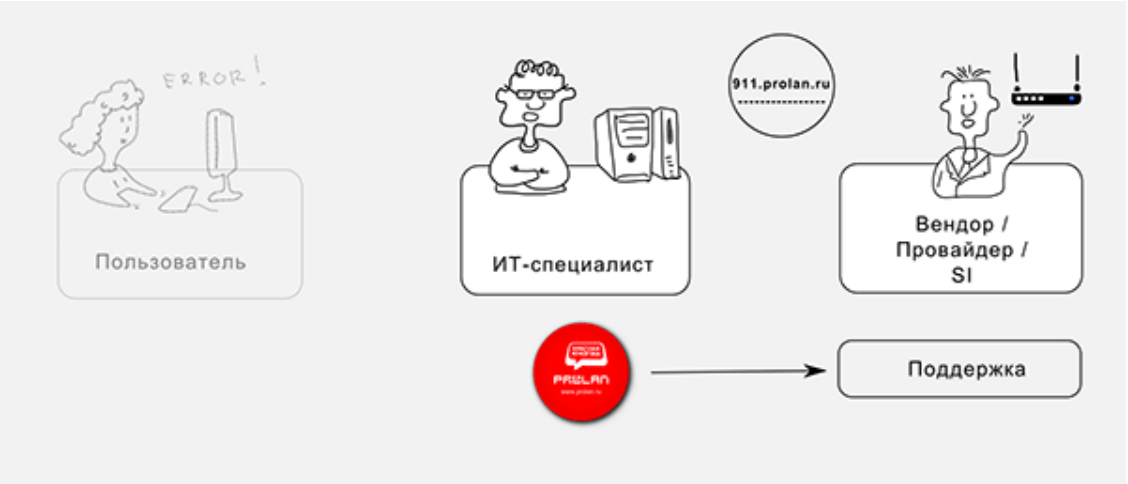



Рис. 1.4. Схема застосування Кнопки Допомоги ITSM для підтримки IT-інфраструктури

Автоматична реєстрація інцидентів для підтримки IT-інфраструктури відрізняється від автоматичної реєстрації інцидентів для підтримки бізнес-додатків (див. рис. 1.4).

Одержувачем підтримки виступає не кінцевий користувач, а системний адміністратор або інший IT-фахівець, відповідальний за працездатність мережі. Кнопка Допомоги ITSM покликана надати йому допомогу тоді, коли власних навичок адміністратора виявляється недостатньо для діагностування і вирішення складних проблем. Кнопка Допомоги ITSM пов'язує його зі службою підтримки Вендора обладнання, Провайдера, Системного інтегратора або IT-служби головного офісу компанії (для розподіленої IT-служби) [26].

У рішенні для підтримки IT-інфраструктури Кнопка Допомоги ITSM автоматизує наступні операції.

**Збір діагностичної інформації:**

Після відкриття діалогового вікна Кнопка Допомоги ITSM додатково запрошувати у адміністратора імена об'єктів IT-Інфраструктури, що підлягають перевірці (перелік усіх об'єктів в мережі створюється в процесі початкового налаштування Кнопки Допомоги ITSM). Отримавши їх, Кнопка Допомоги ITSM виконує ряд перевірок щодо саме цих пристроїв, обумовлені їх типом і зазначеним адміністратором типом інциденту.

**Реєстрація та маршрутизація:**

Реєстрація та маршрутизація Знімка Інциденту щодо IT-інфраструктури аналогічна реєстрації та маршрутизації Знімка Інциденту щодо бізнес-додатків.

**2. Реєстрація агрегованих інцидентів за скаргами користувачів.**


Рис. 1.5. Реєстрація агрегованих інцидентів за скаргами користувачів

Реєстрація агрегованих інцидентів – це реєстрація інцидентів, які автоматично формуються Агрегатором Інформації системи моніторингу на підставі скарг користувачів.

В реєстрації агрегованих інцидентів беруть участь Кнопка Допомоги ITSM і система моніторингу. Передбачається, що використовується система моніторингу ProLAN. Спрощена схема реєстрації агрегованих інцидентів показана на малюнку (див. рис. 1.5).

**Скарга користувача:**

Вводиться розрізнення інциденту і скарги користувача. Інцидент – це порушення в роботі IT-сервісу, що вимагає, з точки зору користувача, негайного реагування Служби підтримки. Скарга – це наслідок зниження якості IT-сервісу нижче комфортного для користувача рівня, але ще не вимагає негайного реагування Служби підтримки.

Скарга не реєструється безпосередньо в Service Desk, але приймається Агрегатором Інформації системи моніторингу і використовується для відстеження якості IT-сервісів і формування агрегованого Інцидентів.

Скарга користувача генерується при тривалому (близько 2 секунд) натисканні «червоної кнопки», в той час як Знімок Інциденту – при звичайному (короткому) натисканні. Відправка Скарги користувача простіше, ніж відправка Знімка Інциденту, і здійснюється повністю в автоматичному режимі (без відкриття діалогового вікна).

**Метрики продуктивності і доступності IT-сервісу і Агреговані Інциденти:**

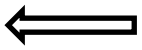
Експертна система агрегатор Інформації групує отримані від «червоних кнопок» скарги по географічному положенню користувача, по бізнес-процесам, що виконуються користувачами в момент натискання «червоної кнопки», по підрозділу, до якого належить користувач. На підставі цього угруповання формуються метрики продуктивності і доступності IT-сервісів, які оцінюються і відслідковують системою моніторингу так само, як метрики здоров'я IT-інфраструктури. Метрики продуктивності і доступності IT-сервісів оцінюються за п'ятибальною шкалою.

Для кожної метрики продуктивності і доступності IT-сервісів встановлюється мінімальна оцінка, падіння нижче якої означає критичне зниження якості IT-сервісу, що вимагає негайного втручання служби підтримки. При зниженні оцінки метрики в даний момент часу нижче мінімальної оцінки система моніторингу автоматично формує Агрегований Знімок Інциденту і відправляє його в Service Desk, де він реєструється поряд зі звичайними Знімками Інциденту (див. табл. 1.2) [27, 28].

*Таблиця 1.2*

Приклад таблиці порогових значень метрики продуктивності і доступності IT-Сервісів

| **Оцінка якості (колір «індикатора»)** | >/< | **Порогове значення** |
|---|---|---|
| Погано (червоний) | > | 4 |
| На межі (миготливий червоний) | > | 3 |
| Потребує уваги (жовтий) | > | 2 |
| Припустимо (миготливий жовтий) | > | 1 |
| Добре (зелений) | < | 1 |



Порогове значення Оцінювання Якості для відправки агрегованих Знімка Інциденту в Service Desk

**Значення агрегованого Інцидентів:**

Значення агрегованого Інциденту в тому, що він дозволяє виявляти критичне погіршення роботи IT-сервісу тоді, коли для кожного окремого користувача робота сервісва ще представляється терпимою. IT-сервіс може продовжувати працювати, і жодного інциденту з цього IT-сервісу ще зареєстровано не було, але кількість скарг на якість IT-сервісу перевищила допустиме значення – тоді і формується Агрегований Інцидент [29].

**Призначення і переваги:**

Основне призначення автоматичної реєстрації інцидентів – скоротити, з одного боку, трудовитрати на реєстрацію, кваліфікацію, маршрутизацію і діагностику інциденту, з іншого (з боку користувача) – скоротити час, витрачений користувачем на реєстрацію інциденту (простий). Є й інші призначення і переваги [30].

## 1.2. Аналіз методів моніторингу

Зростання загроз безпеки інформаційного простору, в тому числі і загроз внутрішнього походження, ставить перед фахівцями в області захисту інформації завдання пошуку їх джерел. Одним з напрямків вирішення цього завдання виступає реалізація моніторингу інформаційного простору.

Моніторингом називають систему спостережень і контролю, що проводяться регулярно за певною програмою для оцінки стану контрольованого середовища, аналізу процесів, що відбуваються в ній і своєчасного виявлення тенденцій її змін[31].

Істотним атрибутом моніторингу, який вирізняє його від інших видів спостереження іконтролю, наприклад від аудиту, є те, що моніторинг проводиться в режимі реальногочасу [32]. Цей фактор має вирішальне значення при організації моніторингу вінтересах забезпечення безпеки інформації, оскільки затримки у виявленні загрозможуть мати серйозні наслідки.

Реалізація моніторингу інформаційного простору можлива при наявностіапаратно-програмних комплексів, орієнтованих на сканування простору зметою виявлення «слабких» місць (вразливостей) або ознак аномальної діяльностіоб'єктів безпеки. Такі комплекси отримали назву «сенсори» [33]. Очевидно, щовеликий масштаб інформаційного простору вимагає наявності безлічі подібнихкомплексів, кожному з яких виділяється деяка частина простору для моніторингу, що наведено в рисунку 1.6.

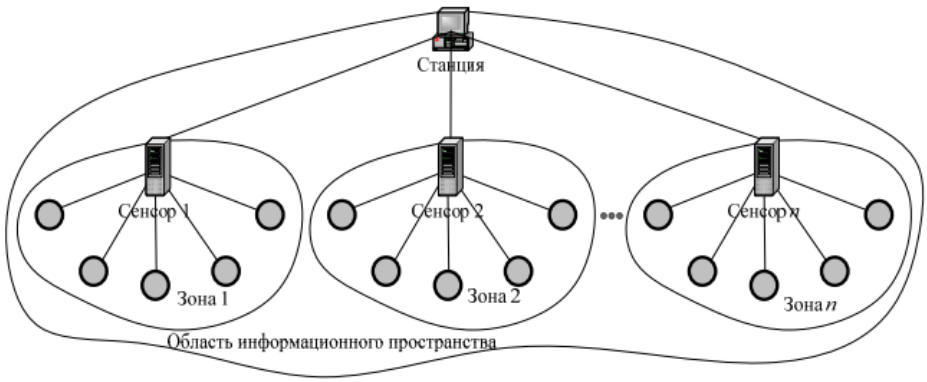



Рис.1.6. Структура системи моніторингу інформаційного простору

Дані моніторингу підлягають обробці на деяких вузлах (станціях), які

здійснюють збір інформації від декількох сенсорів. При виявленні ознак загрозбезпеки ці станції вирішують задачу пошуку мішеней в своїй зоні інформаційногопростору з метою попереднього обґрунтування рішення адміністратора безпекина застосування інструментальних засобів виявлення і нейтралізації виявленихджерел загроз.

**Метод розміщення компонентів системи моніторингу інформаційного простору:**

Побудова системи моніторингу інформаційного простору, що здійснюється з метою пошуку джерел внутрішніх загроз безпеки, вимагає визначення числа і місць розміщення компонентів цієї системи. До найбільш важливих і численних компонентів слід віднести сенсори. Насичення інформаційного простору великою кількістю сенсорів призводить до істотного збільшення вартості системи моніторингу. З іншого боку, зниження їх числа відносно деякого значення, здатне привести до збільшення часу збору і обробки інформації моніторингу. В такій ситуації виникає необхідність вирішення завдання розміщення сенсорів в інформаційному просторі.

Ця задача належить до класичних задач розміщення з дискретним

простором рішень - задач про покриття множин, тобто визначення числа і місць розміщення деяких об'єктів [34]. Її формулювання виглядає наступним чином:

знайти

$$\min C = \sum_{j=1}^{n} c_j f_j \qquad (1.1)$$

при обмеженнях

$$\sum_{j=1}^{n} k_{ij} \ f_j \geq 1, i = 1...m, \qquad (1.2)$$

$$f_j = (0,1), \ j = 1...n. \qquad (1.3)$$

де $k_{ij}$ – коефіцієнт покриття, причому $k_{ij} = 1$, якщо $i$-й вузол інформаційного простору розташовується в межах $j$-ї зони і $k_{ij} = 0$ в іншому випадку; $f_j = 1$,

якщо в $j$-й зоні розташований деякий сенсор і $f_j = 0$ в іншому випадку. зазначені обмеження вимагають, щоб кожен з m вузлів потрапляв в зону відповідальності, принаймні, одного з $n$ сенсорів. У цьому випадку мета полягає в тому, щоб забезпечити потрапляння вузлів в зону відповідальності з мінімальними витратами, причому $c_j$ – витрати на розміщення сенсора в $j$-й зоні.

При цьому $i$-й вузол вважається «покритим» зоною відповідальності $j$-го сенсора ( $j$-й зоною), якщо час отримання інформації $j$-м сенсором від $i$-го вузла не перевищує деякого допустимого значення $t_0$, тобто $t_{ij} \le t_0$.

Вже згадана задача являється задачею цілочисельного лінійного програмування і може бути з допомогою будь-якого прийнятного методу [34-36]. Однак для її рішення розроблений ряд методів, таких як методи неявного перебору, методи січної площини, методи відсікання і евристичні методи [34].

Зазвичай завдання про покриття множини при вирішенні проблеми розміщення об'єктів полягає у визначенні мінімальної кількості зазначених об'єктів, які задовольняють потреби множини споживачів. У цьому випадку завдання (1.1-1. 3) зводиться до задачі про повне покриття. Для цього вважають $c_j = 1, j = 1...n.$

У загальній постановці рішення задачі про покриття безлічі полягає у визначенні мінімальної кількості сенсорів, необхідних для задоволення (покриття) потреб деякої заданої множини користувачів. Тоді таку задачу можна вважати задачею про повне покриття. На практиці не завжди можливо розмістити в мережі таку кількість сенсорів, яка повністю задовольняла б потреби всіх вузлів (наприклад, через обмеження на вартість системи моніторингу). Зазвичай реальна кількість сенсорів здатна задовольнити тільки деяку підмножину вузлів. Тоді доцільно вести мову про часткове покриття.

Якщо задача про повне покриття полягає у визначенні мінімального числа і місць розміщення сенсорів, при якому своєчасно задовольняються потреби всіх вузлів, то задача про часткове покриття пов'язана з визначенням

розміщення заданого сенсорів, при якому своєчасно задовольняються потреби максимального числа вузлів. Математичний опис цього завдання видається в наступному вигляді:

знайти

$$\max Z = \sum_{i=1}^{m} \max k_{ij} f_i, 1 \le j \le n, \quad (1.4)$$

при обмеженнях

$$\sum_{j=1}^{n} f_j \le K, \quad (1.5)$$

$$f_j = (0,1),\ j = 1...n. \quad (1.6)$$

де $K$ – максимальна кількість сенсорів, що підлягають розміщенню.

У вираженні для цільової функції $\max k_{ij} f_i$ означає, що якщо деяке місцерозміщення вузла інформаційного простору накривається більш ніж одним сенсором, то при обчисленні $Z$ враховується тільки максимальна величина $k_{ij}$. Обмеження показують, що в кращому випадку можна використовувати $K$ сенсорів для розміщення. Якщо $Z$ дорівнює $m$-числу вузлів, це означає, що величина $K$ досить велика, щоб задоволені були всі споживачі (вузли). Таким чином, задача про повне покриття може бути зведена до задачі про часткове покриття для різних значень $K$. У цьому випадку рішення задачі (1.4-1.6) з найменшим значенням величини $K$ для якого $Z = m$, буде оптимальним рішення [37,38].

**Методика побудови системи моніторингу інформаційного простору:**

Завдання побудови системи моніторингу інформаційного простору МНС Росії по своїй суті є завданням синтезу, спрямованої на відшукання структури і параметрів названої системи в залежності від її характеристик, значення яких визначаються вимогами щодо оперативності видачі результатів моніторингу. Система моніторингу інформаційного простору відноситься до класу складних систем. Таке становище зобов'язує ретельно підходити до вибору методів її синтезу, оскільки суворі формальні методи не завжди можуть бути застосовні в силу того, що вони мають обмежену область використання, що пов'язано з їх

орієнтацією на вузьке коло завдань малої розмірності з повністю формалізуються характеристиками. Основна проблема вирішення завдань синтезу складних систем полягає в їх неоднозначності. Це пояснюється необхідністю отримання двох груп характеристик, перша з яких описує структуру системи, а друга – параметри її елементів. Така неоднозначність породжується в результаті взаємозалежності характеристик обох груп. Для її усунення, тобто для виділення деякої альтернативи серед інших використовується принцип оптимальності. Останнє означає, що з допустимих варіантів вирішення завдання один визнається кращим, ніж інші [39]. Правило переваги задається критерієм оптимальності, формування якого саме по собі є нетривіальною завданням. Відомі вимоги, що пред'являються до критерію оптимальності, носять загальний характер і мають високу ступінь невизначеності [40]. Критерій оптимальності повинен відображати різні фактори, що впливають на ефективність функціонування системи. Число цих факторів може бути досить великим. Виділення безлічі значущих чинників в принципі може виявитися нереалізованим. Не менш складним завданням є ранжування факторів за їх важливості. В результаті обидва завдання вирішуються на основі досвіду, знань та інтуїції. Але навіть якщо виділення значущих чинників можливо, то наслідком цього є 30 чергова проблема. Якщо кожен подібний фактор розглядати як критерій, то завдання синтезу стає багатокритеріальним, методи вирішення якої далекі від повного пророблення [41]. Тому на практиці такі завдання прагнуть звести до однокрітеріальним, що досягається скаляризації векторного критерію. До теперішнього часу відомі багато способів скаляризації. Однак відсутні суворі правила їх вибору, відповідно успіх рішення завдання не завжди очевидний. Рішення завдання побудови системи моніторингу інформаційного простору за допомогою точних математичних методів, наприклад, методів математичного програмування, може зустріти суттєві труднощі в силу двух причин. По-перше, це висока розмірність завдання, що визначається необхідністю врахування великої кількості факторів. По-друге, неможливість вичерпної формалізації ряду

факторів і, як наслідок, ризик отримання рішення, що не орієнтованого на конкретну обстановку. У такій ситуації раціональним є використання підходу, відомого під назвами «ітеративний синтез» або «синтез через аналіз» [39]. Традиційний спосіб вирішення завдань синтезу через аналіз передбачає побудову ітеративної процедури. У кожній ітерації крім розрахунку величини критерію проводиться модифікація чергового варіанта побудови системи, після чого варіант піддається оцінці.

### 1.3. Аналіз моделей моніторингу

**Модель для оцінки системи моніторингу інформаційного простору:**

Оскільки моніторинг повинен здійснюватися в реальному часі, домінуючоювластивістю системи моніторингу визнається оперативність. Цю властивість можна оцінити через сумарні тимчасові затримки в реалізації процедур контролю, які складаються з наступних складових:

- Затримки при передачі запитів від сенсорів до вузлів інформаційного простору.
- Затримки при виконанні операцій на вузлах (сканування портів, читання системних журналів і т.п.).
- Затримки при первинній обробці даних на сенсорах.
- Затримки при обробці даних на станціях моніторингу.

Ці величини залежать від безлічі факторів і, отже, євипадковими величинами. Такий стан призводить до необхідності розглядупроцесу моніторингу як випадкового і дослідження його в рамках теорії ймовірностей ітеорії масового обслуговування.

Стохастична мережа масового обслуговування (СеМО), визначається наступною сукупністю характеристик:

1) Множиною систем масового обслуговування (СМО) $\{S1, S2, ..., Sn\}$, що утворюють мережу.

2) Числом каналів $K1, K2, ..., Kn$ в системах $S1, S2, ..., Sn,$ відповідно.

3) Матрицею траєкторій руху заявок $R = \|rij\|$, де $rij$ – номер СМО, на яку переходить заявка, яка рухається по $i$-му шляху на $j$-й фазі обслуговування придетермінованій процедурі маршрутизації, або матрицею ймовірностей переходу заявок з однієї СМО в іншу $P = \|pij\|$|, де $pij$ – імовірність того, що заявка, яка залишає $Si$, надходить в $Sj$.

4) Числом заявок, що циркулюють в замкнутій мережі ($Z$).

5) Інтенсивністю джерел заявок в розімкнутої мережі $\wedge = \{\lambda i\}$, де $ip$ – адреса джерела заявки.

6) Законами розподілу часу $F1(t), F2(t), ..., Fn(t)$ і дисциплінами обслуговування заявок в системах $S1, S2, ..., Sn$.

Системи $S1, S2, ..., Sn$ і зв'язки між ними визначають структуру мережі. Інтенсивність джерел заявок, інтенсивність обслуговування, довжини черг і режим роботи приладів характеризують навантаження і продуктивність СеМО.

Елементами, які беруть участь у моніторингу та представляють різні СМО,є (див. рис. 1.7):

- Сенсори (СМО 1).
- Станції моніторингу (СМО 2).
- Вузли інформаційного простору (СМО 3).
- Канали передачі даних (СМО 4).

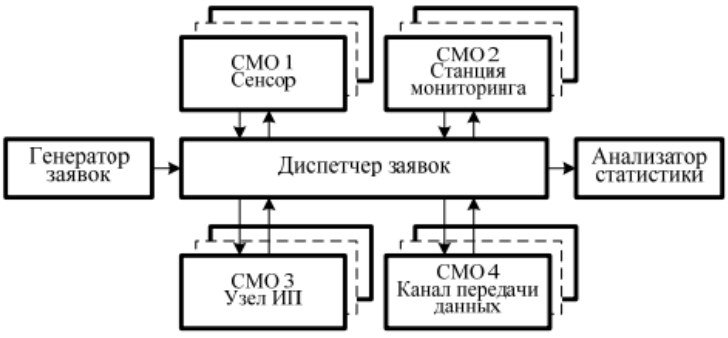



Рис.1.7. Представлення процесу моніторингу у вигляді обслуговування заявок в СеМО

Модель, представлена у вигляді СеМО, може бути досліджена аналітичним іімітаційним методами. Порівняльний аналіз показує, що метод імітаційногомоделювання при дослідженні розробленої моделі є кращимз наступних причин:

1) Велика розмірність задачі, виступає критичним фактором при побудові аналітичних моделей.

2) Порушення властивостей стаціонарності, ординарності і відсутності післядіївхідного потоку в процесі обслуговування заявок в СМО, що утворюють СеМО, призводить дотого, що вхідний потік заявок на черговий фазі обслуговування в мережі (за винятком початкової) відрізняється від найпростішого.

В результаті моделювання можливе одержання ймовірнісно-часових характеристик комплексу операцій, пов'язаних з моніторингом інформаційногопростору. Це дозволяє оцінити відповідність досліджуваної системи вимогам, а при виявленні невідповідності – визначити можливі напрями модифікації системи [42].

## 1.4. Методи прогнозування та класифікація прогнозів

Допоміжними методами для моніторингу виступають також методи прогнозування.

**Методи прогнозування:**

- Експертні методи;

Область застосування таких методів – економічна кон'юнктура, розв'язання проблем науково-технічного прогресу, розвиток об'єктів великої складності.

Вони призначені для об'єктів, розвиток яких не піддається предметному опису, математичній формалізації. Також використовуються в умовах відсутності достовірної статистики, що характеризує об'єкт управління, в умовах великої невизначеності, за відсутності ЕОМ, в екстремальних ситуаціях.

Особливості застосування: за експертними оцінками 7-9 фахівців. Вироблення колективної думки групи експертів. Потребує багато часу для опитування і обробки даних [43].

- Методи евристичного прогнозування;

Застосовуються в науково-технічні об'єктах і проблемах, розвиток яких погано піддається формалізації.

Призначені для знаходження оптимальних способів створення проектованих систем (модернізованих), прогнозування великих і складних систем, виявлення об'єктивізованого уявлення про перспективи розвитку вузької області.

Особливості застосування: математичний апарат (метод) непридатний. Спеціально обробляються прогнозні оцінки об'єкта шляхом систематизованого опитування експертів у вузькій сфері науки, техніки, виробництва. Інформаційний масив створюється із заповнених експертами таблиць [44].

- Колективна генерація ідей;

Застосовуються для отримання блоку ідей з прогнозування і прийняття рішень.

Призначені для визначення всього можливого кола варіантів розвитку керованого об'єкта, визначення альтернативного кола чинників, що впливають на об'єкт прогнозу та отримання сценарію розвитку об'єкта управління.

Особливості застосування: синтез об'єкта прогнозу, мультифакторний аналіз подій, аналіз подій зі сторони детермінуючих чинників [45].

- Морфологічний аналіз;

Застосовується в умовах малого обсягу інформації про проблеми, що вивчаються, для отримання систематизованої інформації по всі можливі варіанти її рішення.

Призначення даного методу в прогнозуванні можливого результату фундаментальних досліджень, а також при відкритті нових ринків, формуванні нових потреб.

Особливості застосування: структурні взаємозв'язки між об'єктами, явищами і концепціями. Загальність припускає їй використання повної сукупності знань про об'єкт. Необхідною вимогою є повна відсутність попередніх думок. Містить такі етапи: формулювання проблеми; аналіз параметрів; побудова «морфологічного ящика», що включає всі рішення; вивчення всіх рішень.

- Прогнозні графи і «дерево рішень»;

Застосовується в структурному прогнозуванні (знаходження розв'язання проблеми при збереженні функцій, але зміною структури об'єкта).

Вирішує задачі прогнозу розвитку об'єкта в цілому, формулювання сценарію досягнення прогнозованої мети, рівня мети, критерію.

Особливості застосування: вибір графи, що визначається сутністю відносин, які вона повинна виразити [46].

- Математичні методи параметричного прогнозування;

Застосовуються для визначення тенденцій розвитку об'єктів, що мають кількісні статистичні дані, які характеризують їх минулий і сьогоднішній стан.

Вирішують задачі прогнозної екстраполяції.

Дані методи можуть застосовуватися:

- за умов, коли вихідні статистичні дані відповідають вимогам, пред'явленим де конкретних математичний методів;
- за наявності кількісної інформації;
- якщо значення часу (глибини) упередження укладаються в рамках одного з циклів об'єкта прогнозування.

Також вирішують задачі методу найменших квадратів.

Застосування можливе, якщо за час упередження функціональна структура об'єкта прогнозування не змінюється (можуть змінюватися тільки значення параметрів) [47, 51].

- Прогнозування за аналогією;

Застосовуються для розв'язання проблемних ситуацій, звичних для осіб, що приймають рішення.

Вирішуються ситуаційні управлінські задачі [48].

**Класифікація прогнозів:**

- Цільовий.

Визначає можливості реалізації цілі управління. Дозволяє уточнити ціль організації і сформулювати її місію. Визначаються критерії досягнення мети.

- Пошуковий.

Виявляє закономірність тенденцій у розвитку керованого об'єкта. Встановлення стану прогнозованого об'єкта в сьогоденні і майбутньому. Враховується в процесі розробки стратегічних рішень.

- Нормативний.

Визначає шляхи, етапи реалізації цілей управлінського рішення. На його основі рекомендується використовувати відповідні методи управління: планові, програмні і т. п [49].

- Програмний.

Досліджує вплив чинників на різних етапах досягнення мети організації. Формулює гіпотези взаємовпливу різних факторів на об'єкт прогнозування і визначення ймовірнісних термінів досягнення проміжних цілей в процесі досягнення головної.

- Проектний.

Отримання матеріалу, що забезпечує цільову спрямованість концепцій проектів, їхнього життєвого циклу, критеріїв оцінки інвестиційних проектів. Результати проектного прогнозу використовуються при розробці інвестиційних і фінансових рішень [50].

## 1.5. Висновки до першого розділу

В першому розділі було розглянуто та проаналізовано існуючі методи, моделі та системи моніторингу та прогнозування в галузі інформаційної

безпеки. За допомогою аналізу різних джерел було визначено принципи їх роботи, в яких випадках застосовуються, переваги та недоліки. Проаналізовано які з методів чи моделей є дієвішими та яку приносять користь.

Підводячи підсумки, можна сказати, що для створення свого методу моніторингу інцидентів в ІКС потрібно розглядати та аналізувати вже існуючі методи та моделі, адже з них ми можемо взяти переваги, виправити недоліки задля створення кращого та більш функціонального методу мережево-центричного моніторингу інцидентів інформаційної безпеки в ІКС.

# Розділ 2. МЕТОД КОНТРОЛЮ ТА ВИЯВЛЕННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖІ

## 2.1. Мереживо – центричний моніторинг

З огляду на динаміку розвитку та глобалізацію інформаційно-комунікаційних технологій (ІКТ), процес впровадження та використання ІКТ у більшості сфер сьогоденного суспільного життя набув неабиякої актуальності [1]. Цей процес включає в себе: розвиток засобів інтерактивної комунікації та інформаційного обміну (соціальні мережі; електронний поштовий обмін; обмін миттєвими повідомленнями; відеозв’язок та Інтернет-телефонія); інформатизація та автоматизація виробничих процесів і більшості сфер суспільного життя (побудова локальних (корпоративних) обчислювальних мереж; систематизація інформації в базах даних; платформи для сумісної роботи користувачів; загальний доступ до ресурсів; VoIP та відеозв'язок; електронний документообіг; система управління взаємовідносинами з клієнтами (CRM); система планування ресурсів підприємства (ERP); система управління інформаційної безпекою; контроль та управління доступом); послуги Інтернет-банкінгу, електронна комерція, миттєве переведення коштів тощо. Усі зазначені процедури, функціонування яких забезпечується ІКТ, є доволі критичними навіть для пересічного громадянина, в першу чергу, з точки зору інформації, яка в них циркулює. Виникнення інцидентів інформаційної безпеки і, як наслідок, порушення штатного режиму функціонування всієї системи можуть призвести до значних матеріальних збитків. Під кіберінцидентом відповідно до [52] будемо розуміти подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі). Процеси виявлення, ідентифікації, оброблення та розслідування інцидентів інформаційної безпеки відповідно до міжнародного стандарту [53].

На сьогодні відомо багато робіт присвячених дослідженню систем виявлення несанкціонованих дій в ІКТ, наприклад, в деяких роботах проведено порівняльний аналіз систем виявлення вторгнень (IntrusionDetectionSystems, IDS) з використанням віртуальних приманок (Honeypot) останнього покоління HoneynetGenIII (Autograph, PADS, PAYL, COVERS, DIRA, DOME, Minos, Paid, Vigilante, HoneyStat тощо), що мають різні механізми виявлення атак та працюють з різними вхідними даними. Інші роботи містять ґрунтовний аналіз систем та засобів управління кризовими ситуаціями у різних галузях, що включає в себе прогнозування, ідентифікацію, оцінку кризових ситуацій та реагування на них. Хоча більшість розглянутих систем і базуються на застосуванні датчиків (сенсорів) і зібраної статистики, проте такі системи не можливо використовувати в кіберпросторі з метою управління інформаційною (кібернетичною) безпекою, так як вони не оперують з реальними параметрами кіберпростору. З огляду на це, не є можливим прогнозування враження кіберінцидентами і конкретних складових ІТС (які теж є компонентами кіберпростору) і, як наслідок, не можливе управління протидією (контрзаходами) та ліквідацією наслідків різних категорій інцидентів інформаційної безпеки.

Мережево-центрична (Network-centric) концепція управління виникла у військовому середовищі не стільки в процесі теоретичних досліджень [54-55], скільки внаслідок систематичного аналізу результатів впровадження в збройні сили нових бойових засобів і підвищення рівня освіченості особового складу. Останнім часом термін «мережево-центричний» все частіше використовується в різних галузях, пов'язаних з використанням мережевих комп'ютерних технологій у сфері управління, наприклад у роботі [56] пропонується мережево-центричне управління кластерами ІКТ, у роботі [57] розроблено універсальне програмоване комп’ютерне середовище мережево-центричного управління, а в [58] розглядається мережево-центричний підхід до ліквідації наслідків надзвичайних ситуацій.

Протидія виникненню та ліквідації наслідків інцидентів інформаційної безпеки за допомогою засобів, об'єднаних інформаційними мережами в єдину систему включає в себе:1) постійний комп'ютерний моніторинг потенційно небезпечних місць та об'єктів для визначення необхідних заходів щодо ліквідації наслідків кожного виду можливих інцидентів інформаційної безпеки; 2) здійснення необхідних заходів з підготовки до боротьби з наслідками можливих груп інцидентів інформаційної безпеки; 3) формування цілей паралельної ліквідації можливих видів інцидентів інформаційної безпеки, їх синхронізацію, узгодження і ранжування; 4) реалізація паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних ресурсів; 5) формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування ресурсами в динаміці управління.

У широкому розумінні моніторинг – це систематичне накопичення та обробка даних про стан і динаміку зміни параметрів аналізованого об'єкта або процесу і представлення результатів у зручному для керівника або експерта вигляді [58]. Завданням моніторингу при комплексному управлінні підготовкою до ліквідації наслідків різних категорій інцидентів інформаційної безпеки є своєчасна оцінка виникнення загроз кожної категорії інцидентів інформаційної безпеки, аналіз динаміки їх розвитку та їх комплексна оцінка. У динаміці це збір та аналіз даних про втрати від інцидентів інформаційної безпеки. Мережево-центрична система моніторингу об'єднує засоби моніторингу всіх рівнів і напрямків управління в єдине ціле. Вона повинна забезпечувати доведення всієї необхідної інформації до адресатів в реальному часі або близькому до нього в міру її отримання та, що дуже важливо, використовуючи інформацію, отриману на всіх рівнях і напрямах управління. Такий підхід дозволяє різко поліпшити розуміння сформованої ситуації керівниками усіх ступенів, підвищити рівень взаємодії і здійснювати синхронізацію зусиль по горизонталі і вертикалі управління.

Необхідно зазначити, що порушення хоча б одного з перерахованих принципів може привести до серйозних ускладнень. Мережево-центрична

концепція орієнтована не тільки на ефективне управління наявними технічними, фінансовими та іншими засобами, а й на досягнення інформаційної переваги в економіці, політиці, соціальній сфері і т.д., забезпечуючи здатність системи оперативно адаптуватися до швидкоплинної обстановки і переносити функції стратегічного та оперативного управління по вертикалі і горизонталі відповідно до потреб сформованої обстановки. Для цього мережево-центричний моніторинг повинен забезпечувати в реальному часі комплексний багаторівневий аналіз потоків окремих малоінформативних, а часто і суперечливих, первинних відомостей про появу нових об'єктів або процесів. Система повинна вміти змінювати логіку аналізу сформованої обстановки в міру зміни джерел інформації та отриманих нових даних про ситуацію. Вихід з ладу однієї або кількох локальних підсистем моніторингу не повинен призвести до колапсу всього мережево-центричного моніторингу.

## 2.2. Метод контролю та виявлення інцидентів інформаційної безпеки в інформаційно-комунікаційних системах

Згідно з [59] інформаційно-телекомунікаційна система (ІТС) – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. Згідно [60] типовий склад ІТС:

1) серверне обладнання (комп’ютери з підвищеною продуктивністю та технічними характеристиками; зазвичай призначені для надання одного або декількох специфічних сервісів, на кшталт електронного поштового обміну, баз даних, IP-телефонії, файлового сховища тощо);

2) середовище передачі даних (оптоволоконні лінії, кабелі типу «звита пара», телефонні кабелі, бездротові канали передачі даних (Wi-Fi, Wi-MAX, Bluetooth));

3) активне мережеве обладнання і обладнання зв’язку (комутатори, маршрутизатори, модеми, бездротові точки доступу, телефонія), а також

пристрої захисту (міжмережеві екрани, системи виявлення/попередження вторгнень тощо);

4) автоматизовані робочі місця співробітників (АРМ) (стаціонарні комп'ютери, ноутбуки, мобільні пристрої).

Складові ІТС є середовищем в якому можуть виникнути інциденти інформаційної безпеки. Оскільки розглядається комплексне планування проведення заходів протидії прогнозованим кіберінцидентам, то залежно від сформованих умов повинні відслідковуватися параметри, що характеризують ті види інцидентів інформаційної безпеки, які можуть відбутися.

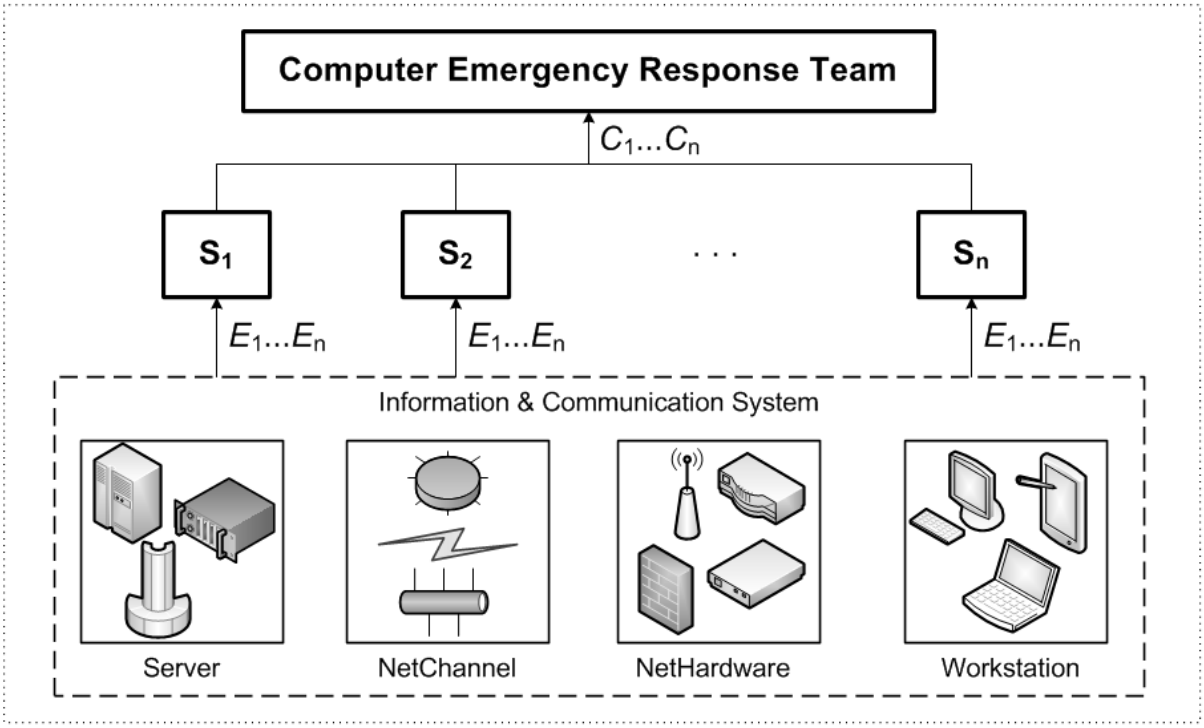



Рис. 2.1. Схема роботи команди реагування на інциденти

В ІКС відбувається певна подія $E$, що надходить на сенсори $S$, які її вловлюють і виявляють кіберінцидент, що надходить до команди реагування на інциденти (див. рис. 2.1).

Відповідно до найбільш розповсюджених видів сучасних комп'ютерних загроз за даними CERT-UA [60] визначимо види інцидентів інформаційної безпеки:

1) пошкодження ІТС небезпечним програмним забезпеченням (Malware)*(один із найбільш розповсюджених способів ураження є drive-by*

*завантаження – ураження комп'ютера при відвідуванні користувачем шкідливого веб-сайту)* Віруси: мережеві хробаки (networm) – підклас вірусів, що інфікують комп'ютери та шукають способи для розповсюдження по мережі, створюючи свої копії; троянські програми (trojan) програми, призначенні для прихованого (під виглядом чогось іншого) проникнення до системи, зазвичай, зі зловмисними намірами; руткіти (rootkit) пакети програм, призначених для приховування факту «присутності» зловмисників у системі (комп'ютері); клавіатурні шпигуни (keylogger) забезпечують фіксацію всіх переривань, що надходять у систему вводу під час натискання клавіш на клавіатурі; рекламні системи (adware) шкідливе програмне забезпечення, призначене для нав'язування реклами, шляхом, як приклад, блокування дій користувача за допомогою «випливаючого вікна», що містить рекламні матеріали);

2) реалізація Інтернет-шахрайства (Internet Fraud) (фішинг (phishing) атака полягає у спонуканні користувача ввести свої автентифікаційні дані (логін, пароль, банківську інформації) та іншу інформацію шляхом запевнення останніх щодо достовірності та справжності хибних (спеціально створених для цього) мережевих ресурсів (в тому числі просто посилань, за якими потрібно перейти), таких як пошта, веб-сайти, призначені для Інтернет-банкінгу, сторінки авторизації у соціальних мережах тощо; вішинг (vishing) вид шахрайства, що полягає в отриманні у користувача під час телефонної розмови, шляхом використання різних методів переконання, необхідної зловмиснику інформації. Один із різновидів «соціальної інженерії»);

3) несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем (Unauthorized Access)(цілеспрямована хакерська атака – дії, що спрямовані на порушення штатного режиму функціонування системи, порушення доступності її сервісів (компонентів), отримання несанкціонованого доступу до конфіденційної інформації, порушення цілісності інформації тощо; дефейс атака полягає у зміні змісту головної сторінки веб-сайту, в результаті чого при його відвідуванні замість звичного

контенту відображається щось інше (написи «Hacked By», нецензурні або провокаційні фрази/малюнки тощо);

4) бот-мережі (Botnet)(сукупність комп'ютерів, уражених шкідливим програмним забезпеченням, ресурси яких (як інформаційні, так і виробничі) через спеціальні командно-контрольні сервери (C&C) несанкціоновано використовуються зловмисниками (ZeuS, SpyEye, Carberp, Rustock, Kelihos, Pandora, BlackEnergy));

5) реалізація DDoS-атаки (DDoS) (розподілена мережева атака, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів);

6) крадіжка коштів (Money Theft);

7) «крадіжка особистості» (Identity Theft) (несанкціоноване заволодіння персональними даними особи, що дозволяє зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами тощо) від її імені (як один із механізмів підтвердження автентичності особи може використовуватись електронний цифровий підпис))(див. рис. 2.2).

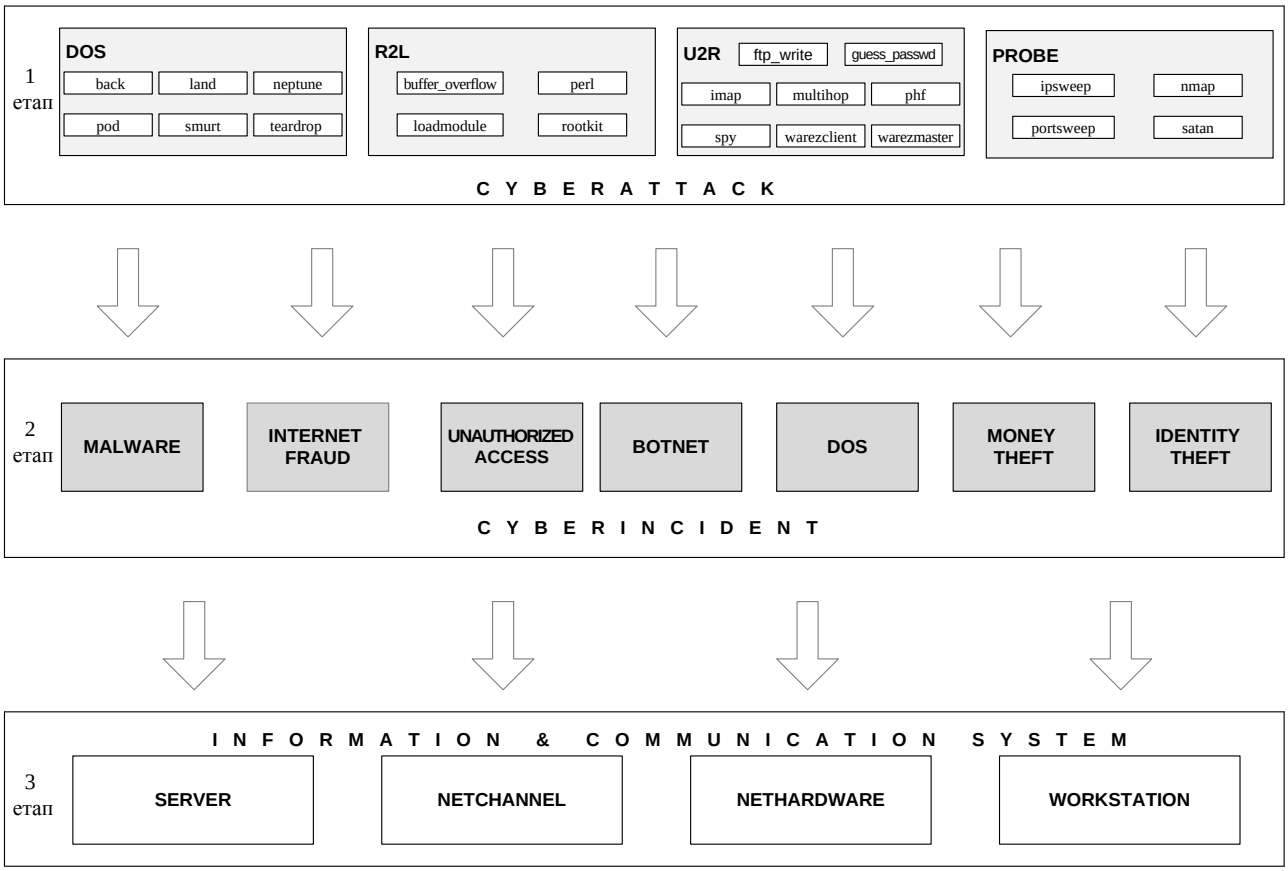



Рис. 2.2. Схема реалізації методу мереживо – центричного моніторингу інцидентів інформаційної безпеки в ІКС

Варто враховувати те, що інциденти інформаційної безпеки можуть мати комбінований характер, наприклад враження ІКС шкідливим програмним забезпеченням може призвести, через не великий часовий термін, до «крадіжки особистості» та іншого.

Основними джерелами загроз є: ресурси мережі Інтернет; електронна пошта; знімні носії інформації (USB-flash, CD/DVD); соціальні мережі; загрози, пов’язані з інсайдерською діяльністю, тощо.

Метод мережево-центричнго моніторингу інцидентів інформаційної безпеки реалізується у 2 етапи:

1 етап – моніторинг і оцінка ситуації на основі завчасного прогнозу базуючись на оціночних характеристиках можливих інцидентів інформаційної безпеки;

2 етап – моніторинг і оцінка ситуації на основі оперативних даних про інциденти інформаційної безпеки;

Зазначені етапи включають відповідну організацію і використовувані засоби.

Джерелами надходження інформації при проведенні моніторингу можуть бути: системи виявлення вторгнень IDS/IPS, міжмережеві екрани, honeypot системи, операційні системи, різні додатки (у тому числі спеціалізовані системи виявлення інцидентів інформаційної безпеки), антивірусні системи, звернення користувачів тощо.

При одночасній обробці кількох інцидентів необхідно розставляти пріоритети. Обгрунтуванням для призначення пріоритету служить рівень важливості помилки для бізнесу і для користувача. На основі діалогу з користувачем і відповідно до положень Угод про Рівень Послуг (Service Level Agreements - SLAs) служба Service Desk призначає пріоритети, що визначають порядок обробки інцидентів. При ескалації інцидентів на другу, третю або більшу лінії підтримки, той же пріоритет повинен бути дотриманий, але іноді він може бути скорегований за погодженням із Службою Service Desk[61].

Звичайно, кожен користувач буде вважати, що його інцидент має найвищий пріоритет, але думки користувачів часто бувають суб'єктивними. Для об'єктивної оцінки пріоритету в діалозі з користувачем вживаються наступні критерії:

- **ступінь впливу інциденту:** ступінь відхилення від нормального рівня надання послуги, що виражається в кількості користувачів або бізнес-процесів, які зазнали впливу інциденту;
- **терміновість інциденту:** прийнятна затримка дозволу інциденту для користувача або бізнес-процесу.

Пріоритет визначається на основі терміновості і ступеня впливу. Для кожного пріоритету визначається кількість фахівців і обсяг ресурсів, які можуть бути спрямовані на вирішення інциденту. Порядок обробки інцидентів однакового пріоритету може бути визначений відповідно до зусиль, необхідних

для вирішення інциденту. Наприклад, інцидент який легко вирішується може бути оброблений перед інцидентом, що вимагає великих зусиль.

При управлінні інцидентами існують способи зниження ступеня впливу і терміновості, такі, як перемикання системи на резервну конфігурацію, перенаправлення черги друку та ін. (див. рис. 2.3).

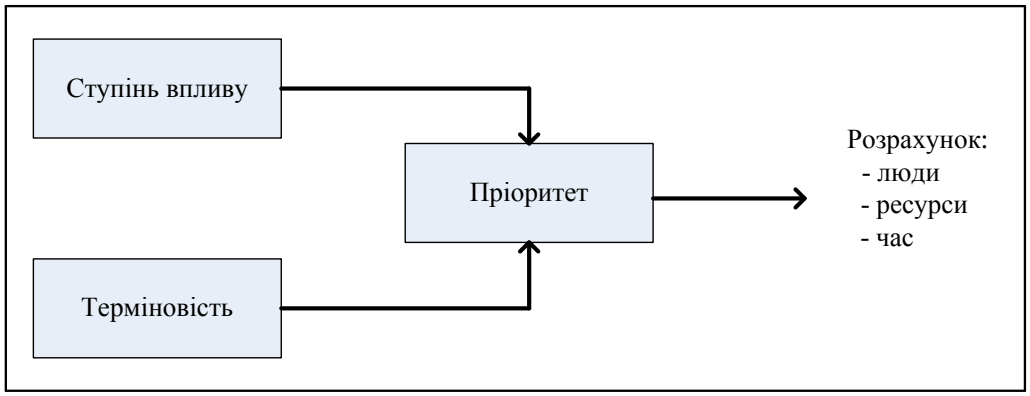



Рис. 2.3. Визначення ступеня впливу, терміновості і пріорітету

Ступінь впливу і терміновість також можуть самі змінюватися у часі, наприклад при зростанні кількості користувачів, які зазнали впливу інциденту або в критичні моменти часу. Ступінь впливу і терміновість можуть бути об'єднані в матрицю, наприклад, як показано в табл. 2.1.

*Таблиця 2.1*

Приклад системи кодування пріоритетів

**Ступінь впливу**

| **Терміновість** | **Пріорітет / Час вирішення** | **Високий** | **Середній** | **Низький** |
|---|---|---|---|---|
| | **Висока** | Критичний / < 1 години | Високий / < 8 годин | Середній / < 24 годин |
| | **Середня** | Високий / < 8 годин | Середній / < 24 годин | Низький / < 48 годин |
| | **Низька** | Середній / < 24 годин | Низький / < 48 годин | Планування / Заплановано |

**Ескалація**

Якщо інцидент не може вирішитися першою лінією підтримки за узгоджений час, необхідне залучення додаткових знань або повноважень. Це називається ескалацією, яка відбувається відповідно до розглянутих вище

пріоритетів і, відповідно, часу дозволу інциденту. Розрізняють функціональну і ієрархічну ескалацію: 

- **Функціональна ескалація (горизонтальна) –** означає залучення більшої кількості фахівців або надання додаткових прав доступу для вирішення інциденту; при цьому, можливо, відбувається вихід за межі одного структурного IT-підрозділу.
- **Ієрархічна ескалація (вертикальна)** – означає вертикальний перехід (на більш високий рівень) в рамках організації, так як для вирішення інциденту недостатньо організаційних повноважень (рівня влади) або ресурсів.

Завданням Керівника Процесу Управління інцидентами є завчасне резервування можливостей для функціональної ескалації в рамках лінійних підрозділів організації так, щоб вирішення інцидентів не вимагало регулярної ієрархічної ескалації. У будь-якому випадку, лінійні підрозділи повинні надати для цього процесу достатню кількість ресурсів.

**Перша, друга та n-лінія підтримки**

Вище була викладена маршрутизація інциденту, або функціональна ескалація. Маршрутизація визначається необхідним рівнем знань, повноважень і терміновістю. Першою лінією підтримки (підтримкою 1-го рівня) зазвичай є Служба Service Desk, другою лінією – підрозділи, які здійснюють Управління IT-інфраструктурою, третя – відділи розробки та архітектури програмного забезпечення, і четверта – постачальники.Чим менше організація, тим менше в ній рівнів ескалації. У великих організаціях Керівник Процесу Управління інцидентами може призначити Координаторів інцидентів у відповідних підрозділах для підтримки своєї діяльності. Наприклад, координатори можуть виконувати роль інтерфейсу між процесною діяльністю і лінійними організаційними підрозділами. Кожен з них координує діяльність своїх груп підтримки.

На 1 етапі основною задачею моніторингу є загальна оцінка можливих видів інцидентів інформаційної безпеки, які можуть виникнути, і побудова

завчасного прогнозу ситуації. Для цього використовуються дані про складові ІТС, які були отримані в нормальних умовах функціонування ІТС.

Для загальної оцінки можливих видів інцидентів інформаційної безпеки з використанням наявних даних моніторингу про складові ІТС комп'ютерна система, погоджуючи суб'єктивні оцінки керівників і експертів, формує таблицю 2.2.

*Таблиця 2.2*

Оцінка впливу інцидентів інформаційної безпеки на складові ІТС

| Складові ІТС | Оцінки за видами інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| Серверне обладнання | 2 | 3 | 2 | 1 | 1 | 4 | 4 |
| Середовище передачі даних | 3 | 4 | 4 | 2 | 2 | 4 | 4 |
| Активне мережеве обладнання і обладнання зв’язку | 3 | 4 | 3 | 3 | 3 | 3 | 3 |
| Автоматизовані робочі місця співробітників | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Атаки поділяються на: 1. Відмову систем від обслуговування (DOS); 2. Одержання суб’єктом впливу несанкціонованого доступу до інформації управління (R2L); 3. Несанкціоноване розширення повноважень суб’єкта впливу (U2R); 4. Сканування портів з метою одержання конфіденційної інформації (PROBE). Розглянемо можливість реалізації атаки R2L і, як наслідок виникнення 7 видів інцидентів інформаційної безпеки в ІТС. Список складових для оцінки видів інцидентів інформаційної безпеки стандартний, зберігається в

БД. Табл. 2.3 складається комп'ютерною системою шляхом опитування експертів і керівників та узгодження їх оцінок шляхом використання методів попарного порівняння, експертного оцінювання та ранжирування [62].

*Таблиця 2.3*

Оцінювання впливу атак на складові ІКС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Серверне обладнання | – | = | < | < | 8 | 3 |
| 2. Середовище передачі даних | = | – | < | < | 8 | 3 |
| 3. Активне мережеве обладнання і обладнання зв'язку | > | > | – | < | 5 | 2 |
| 4. Автоматизовані робочі місця співробітників | > | > | > | – | 3 | 1 |

Потім система просить експертів визначити значимість («вагу») кожного критерію та погоджує її. Визначення «ваги» може бути здійснено методом парних порівнянь. «Вага» критерію дуже важлива для оцінки виду інциденту інформаційної безпеки. У мережево-центричних системах складність може полягати в тому, що на різних рівнях і напрямках управління «ваги» критеріїв можуть бути різними, і це вимагатиме окремого розрахунку оцінок для кожного виду інциденту інформаційної безпеки у різних середовищах. Але на цьому в нашому прикладі зупинятися не будемо. Розглянемо спрощений варіант. Система показує експертам і керівникам таблицю типу табл. 2.3 і просить її

заповнити, тобто поставити в кожній клітинці один із знаків: «важливіше», «менш важливий» і «еквівалентний» (тобто >, <, =).

У таблиці 2 кожного $k$-го експерта система замінює знаки співвідношення на значення $r_{ij}^k$ за правилом:

$$r_{ij}^k = \begin{cases} 1, \textit{якщо } a_i > a_j, \\ 2, \textit{якщо } a_i = a_j, \\ 3, \textit{якщо } a_i < a_j. \end{cases} \quad (2.1)$$

Система підраховує бал кожного критерію як суму $r_{ij}^k$ (може бути і якийсь інший алгоритм, важливо, щоб він відображав «ваги» критеріїв, зазначених експертами або керівником при парних порівняннях критеріїв). Після цього система проводить узгодження матриць кожного експерта $R^k$, в результаті формується зведена матриця колективної переваги [58]. Узгодження може проводитися за різними алгоритмами. У таблиці 2.3 використовувалася трибальна шкала (<, >, =). Можуть бути використані шкали більшої бальності. У разі порушення транзитивності переваг може виникнути ситуація, коли матриця $R^*$ не є ранжуванням, тобто не дозволяє визначити переваги. Тоді система будує таке ранжування $R$, яке є найближчим до групової думки. Позначивши через $d(R, R^*)$ відстань між $R$ і $R^*$, отримаємо вимога $d(R, R^*)\min$. Груповий вибір $R^*$ визначається умовою

$$\sum_{k=1}^{K} d(R^*, R^k) = \min_{R \in R(n)} \sum_{k=1}^{K} d(R\ , R^k) \quad (2.2)$$

Нарешті, завершальним кроком є визначення порівняльної значущості можливого збитку, який може призвести кожен вид інцидентів інформаційної безпеки відповідно до значень кожного критерію (табл. 1) і їх «ваги» (див. табл. 2.3).

Це важливо для диспетчеризації стратегій і оперативних впливів. Оцінка порівняльної значущості може бути підрахована за простою формулою (хоча існують і дуже складні):

$$Q_j = \sum_{i=1}^{I} a_i x_{ij},\ j = \overline{1, J}, \quad (2.3)$$

де $x_{ij}$ - значення $i$-го критерію $j$-го виду інцидентів інформаційної безпеки;

$a_i$ –«ага» $i$-го критерію в таблиці 2.3. При використанні значень критеріїв з таблиці 2 чим менше значення $Q_j$, тим більшу небезпеку становить вид інцидентів інформаційної безпеки. Тоді для виду інциденту інформаційної безпеки «Malware» за співвідношенням (2.2) отримуємо:

$$Q_1 = 8 \times 2 + 8 \times 3 + 5 \times 3 + 3 \times 1 = 58,$$

для виду інциденту інформаційної безпеки «Internet Fraud»:

$$Q_2 = 8 \times 3 + 8 \times 4 + 5 \times 4 + 3 \times 1 = 79,$$

для виду інциденту інформаційної безпеки «Unauthorized Access»:

$$Q_3 = 8 \times 2 + 8 \times 4 + 5 \times 3 + 3 \times 1 = 66,$$

для виду інциденту інформаційної безпеки «Botnet»:

$$Q_4 = 8 \times 1 + 8 \times 2 + 5 \times 3 + 3 \times 1 = 42,$$

для виду інциденту інформаційної безпеки «DDoS»:

$$Q_5 = 8 \times 1 + 8 \times 2 + 5 \times 3 + 3 \times 1 = 42,$$

для виду інциденту інформаційної безпеки «Money Theft»:

$$Q_6 = 8 \times 4 + 8 \times 4 + 5 \times 3 + 3 \times 1 = 82,$$

для виду інциденту інформаційної безпеки «Identity Theft»:

$$Q_7 = 8 \times 4 + 8 \times 4 + 5 \times 3 + 3 \times 1 = 82.$$

Нормовані оцінки видів інцидентів інформаційної безпеки:

$$r_j = \frac{Q_j}{\sum_j Q_j},\ r_1 = 0.13,\ r_2 = 0.18,\ r_3 = 0.15,\ r_4 = 0.09,\ r_5 = 0.09,\ r_6 = 0.18,\ r_7 = 0.18.$$

Таким чином, при реалізації атаки R2L найбільшу небезпеку несуть інциденти інформаційної безпеки DDoSта Botnet потім інцидент інформаційної безпеки Malware, далі інцидент інформаційної безпеки Unauthorized Access і тільки потім інциденти інформаційної безпеки Internet Fraud, Money Theft та Identity Theft.

Різниця в значеннях $Q_j$ дозволяє вважати отримане ранжирування ступеня небезпеки видів інцидентів інформаційної безпеки досить близьким до істини.

Якщо виникає декілька інцидентів паралельно тоді ми маємо шаблони впливу різних інцидентів на складові ІТС і в залежності від рівня критичності складової ІТС можна провести пріоритезацію інцидентів з метою адекватного реагування.

*Таблиця 2.4*

Вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації атак

| Атака | Вагові коефіцієнти виникнення інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| DOS | 2 | 1 | 2 | 4 | 2 | 2 | 3 |
| R2L | 3 | 2 | 2 | 1 | 4 | 2 | 3 |
| U2R | 2 | 3 | 3 | 1 | 1 | 3 | 2 |
| PROBE | 2 | 3 | 1 | 3 | 3 | 1 | 4 |

*Таблиця 2.5*

Оцінювання впливу інциденту інформаційної безпеки Malware на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | = | < | < | 8 | 3 |
| 2. Netchannel | = | – | > | < | 6 | 2 |
| 3. Nethardware | > | > | – | = | 4 | 1 |
| 4. Workstations | < | > | = | – | 6 | 2 |

$Q_1 = 8 \times 2 + 6 \times 3 + 4 \times 2 + 6 \times 2 = 54,$

*Таблиця 2.6*

Оцінювання впливу інциденту інформаційної безпеки Internet Fraud на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | > | > | = | 4 | 1 |
| 2. Netchannel | = | – | = | < | 7 | 3 |
| 3. Nethardware | < | = | – | < | 8 | 4 |
| 4. Workstations | = | > | < | – | 6 | 2 |

$Q_2 = 4 \times 1 + 7 \times 2 + 8 \times 3 + 6 \times 3 = 60,$

*Таблиця 2.7*

Оцінювання впливу інциденту інформаційної безпеки Unauthorized Access на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | = | > | < | 6 | 1 |
| 2. Netchannel | = | – | < | < | 8 | 2 |
| 3. Nethardware | < | > | – | = | 6 | 1 |
| 4. Workstations | < | < | = | – | 8 | 2 |

$Q_3 = 6 \times 2 + 8 \times 2 + 6 \times 3 + 8 \times 1 = 54,$

*Таблиця 2.8*

Оцінювання впливу інциденту інформаційної безпеки Botnet на складові ІТС

| № складової ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|

| Складові ІТС | | | | | | |
|---|---|---|---|---|---|---|
| 1. Server | – | = | > | < | 6 | 2 |
| 2. Netchannel | = | – | < | = | 7 | 3 |
| 3. Nethardware | > | > | – | < | 5 | 1 |
| 4. Workstations | < | = | < | – | 8 | 4 |

$$Q_4 = 6 \times 4 + 7 \times 1 + 5 \times 1 + 8 \times 3 = 60,$$

*Таблиця 2.9*

Оцінювання впливу інциденту інформаційної безпеки DDoS на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | = | < | < | 8 | 4 |
| 2. Netchannel | = | – | > | = | 5 | 1 |
| 3. Nethardware | < | > | – | < | 7 | 3 |
| 4. Workstations | < | = | > | – | 6 | 2 |

$$Q_5 = 8 \times 2 + 5 \times 4 + 7 \times 1 + 6 \times 3 = 61,$$

*Таблиця 2.10*

Оцінювання впливу інциденту інформаційної безпеки Money Theft на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | > | = | = | 5 | 2 |
| 2. Netchannel | < | – | = | < | 8 | 4 |
| 3. Nethardware | = | = | – | < | 7 | 3 |
| 4. Workstations | > | = | > | – | 4 | 1 |

$$Q_6 = 5 \times 2 + 8 \times 2 + 7 \times 3 + 4 \times 1 = 51,$$

*Таблиця 2.11*

Оцінювання впливу інциденту інформаційної безпеки Identity Theft на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | < | = | < | 8 | 3 |
| 2. Netchannel | > | – | = | > | 4 | 1 |
| 3. Nethardware | = | = | – | > | 5 | 2 |
| 4. Workstations | < | > | > | – | 5 | 2 |

$Q_7 = 8 \times 3 + 4 \times 3 + 5 \times 2 + 3 \times 4 = 58.$

Нормовані вагові коефіцієнти виникнення інцидентів інформаційної безпеки:

$$r_j = \frac{Q_j}{\sum_j Q_j},\ r_1 = 0.135,\ r_2 = 0.151,\ r_3 = 0.135,\ r_4 = 0.151,\ r_5 = 0.153,\ r_6 = 0.128,\ r_7 = 0.145.$$

Таким чином, при реалізації атаки R2L найбільшу небезпеку несе інцидент інформаційної безпеки Money Theft потім в приблизно рівних значеннях інциденти інформаційної безпеки Unauthorized Access та Malware, далі інцидент інформаційної безпеки Identity Theft, наступні інциденти інформаційної безпеки Botnet та Internet Fraud і найменшу небезпеку представляє інцидент інформаційної безпеки DDoS.

На 2 етапі задачею моніторингу є збір оперативних даних про інциденти інформаційної безпеки та спираючись на результати 1 етапу внести коректування в початковий прогноз.

Крім того, мереживо – центричний моніторинг визначається тим, що для кожної системи менеджменту інцидентів інформаційної безпеки формується мережа агентів (джерело інформації, сенсори (рис.2.1)), так загальну систему менеджменту інцидентів інформаційної безпеки регіону чи держави можна

відобразити як складну мережу взаємопов’язаних центрів кампусного типу, кожен з яких має можливість:

- мати чітко сформульовану мету функціонування;
- діяти відповідно до закладених при його створенні правил і алгоритмів;
- керувати базою даних, що містить необхідну йому інформацію;
- вміти використовувати результати моніторингу, реагуючи на них своїми діями;
- проявляти власну ініціативу;
- посилати і отримувати повідомлення від інших СМКІ і вступати з ними у взаємодію.

Побудована таким чином мереживо – центрична інфокомунікаційна система дозволяє зв'язати в єдиний інтерфейс управління, моніторингу і вироблення управляючих рішень всіх абонентів (посадових осіб), що входять до її складу структурних підрозділів, програмні продукти, Web сторінки, мультимедіа дані, а також необхідні персональні дані для їх використання різними програмними додатками незалежно від місцезнаходження абонентів мережі особливо спеціального призначення

Основні принципи мереживо – центричного управління:

- всі елементи системи прив'язані до єдиного координатно-тимчасового поля, тобто діють в єдиному просторі станів;
- дані для спільного використання надаються своєчасно і безперебійно;
- постійна підтримка систематичності спостережень за станом системи та потенційно-небезпечними об'єктами, що можуть викликати КС;
- забезпечення своєчасності отримання, комплексності оброблення та використання поточної інформації, що надходить і зберігається;
- система повинна бути самоорганізуючою, тобто здатна підтримувати, відновлюватись і адаптувати до нових умов свою структуру і

поведінку, зокрема бути стійкою до часткових відмов вузлів мережі і ліній зв'язку;

- система повинна бути відкритою, тобто обмінюватися ресурсами з середовищем;

Підатака категорії R2L , що описується певним набором параметрів ініціює виникнення одного (або декількох) з 7 типів інцидентів, що негативно впливають на певні компоненти ІТС – тобто можна моніторити зміни ідентифікуючих параметрів і прогнозувати негативний вплив на компоненти ІТС, а рівень цього впливу можна визначити експертним оцінюванням.

## 2.3. Висновки до другого розділу

В другому розділі було проаналізовано мереживо – центричний моніторинг. Згідно з CERT-UA визначено типовий склад ІТС та види інцидентів інформаційної безпеки. Було створено схему реалізації методу мереживо – центричного моніторингу інцидентів інформаційної безпеки в ІКС. Також прораховано оцінку впливу інцидентів інформаційної безпеки на складові ІТС та оцінку впливу атак на складові ІКС.

Роблячи висновки, можна сказати, що для експериментального дослідження методу мереживо – центричного моніторингу інцидентів інформаційної безпеки в ІКС потрібно розробити програмний додаток, який за допомогою взятих з бази KDD 99 сигнатур атак зможе швидко виявити яку саме складову ІКС потрібно захищати та надасть рекомендації для уникнення настання інцидентів інформаційної безпеки.

# Розділ 3. ТЕСТУВАННЯ ТА ДОСЛІДЖЕННЯ РОЗРОБЛЕНОГО ЗАСТОСУНКУ

## 3.1. Тестування розробленого методу контролю та виявлення інцидентів інформаційної безпеки

Програмний засіб тестування розробленого методу мереживо – центричного моніторингу інцидентів інформаційної безпеки в ІКС написаний на мові програмування C#. Запускається від імені адміністратора.

Система тестування складається з:

- випадаючого списку сигнатур атак, взятого з бази KDD99;
- чотирьох атак;
- інцидентів інформаційної безпеки та балів, які виставлені їм шляхом експертного оцінювання та попарного порівняння;
- складових ІКС та виставленими балами для них;
- вкладки з рекомендаціями щодо захисту обраної складової ІКС.

Програмний засіб працює таким чином: спочатку рандомно обирається з бази KDD99 сигнатура атаки, яка відноситься до певної частинки атаки (див. рис. 2.2). Потім визначається який саме вид атаки може бути здійснено і вона підсвічується. Далі розраховуються вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації певної атаки (див. табл. 2.4).Обирається найменший коефіцієнт і підсвічується інцидент інформаційної безпеки, який несе найбільшу небезпеку. Далі оцінюється вплив інциденту інформаційної безпеки на складові ІТС (див. табл. 2.5-2.11) і підсвічується складова з найменшим значенням, тобто та, яка є найнебезпечнішою для системи. Завершальним етапом є видача рекомендацій по захисту складової ІКС задля уникнення настання певного виду інциденту інформаційної безпеки в подальшій роботі системи.

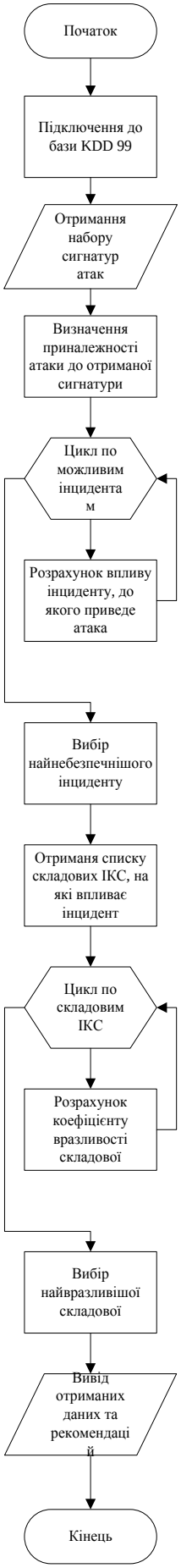



Рис. 3.1. Алгоритм роботи програмного засобу тестування методу

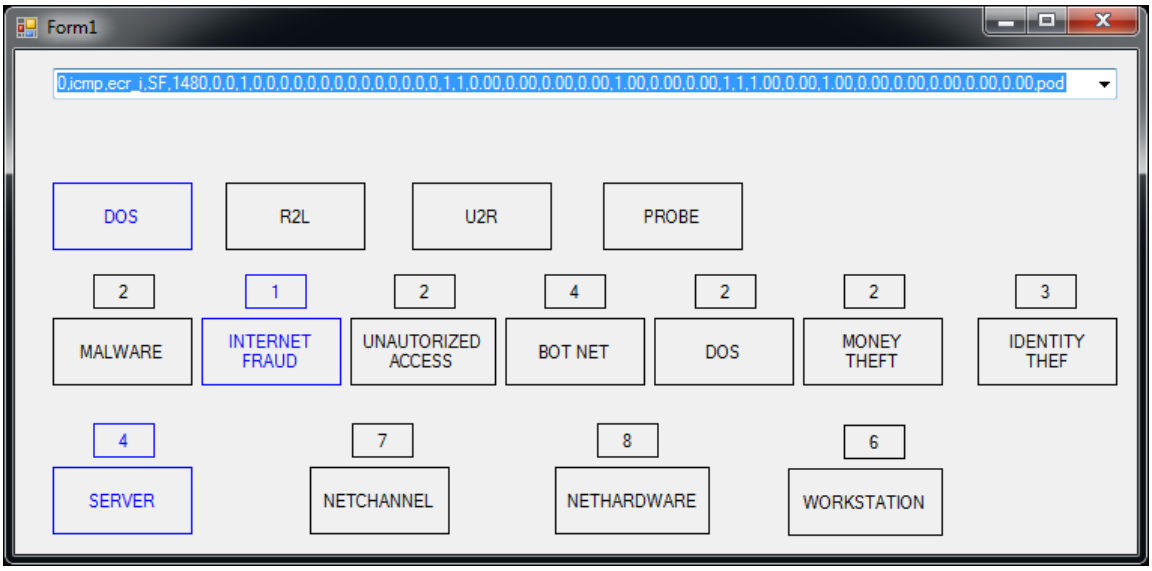



Рис. 3.2. Враження складової ІКС Server

*Таблиця 3.1*

Вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації атаки DOS

| Атака | Вагові коефіцієнти виникнення інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| DOS | 2 | 1 | 2 | 4 | 2 | 2 | 3 |

*Таблиця 3.2*

Оцінювання впливу інциденту інформаційної безпеки Internet Fraud на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | > | > | = | 4 | 1 |
| 2. Netchannel | = | – | = | < | 7 | 3 |
| 3. Nethardware | < | = | – | < | 8 | 4 |
| 4. Workstations | = | > | < | – | 6 | 2 |

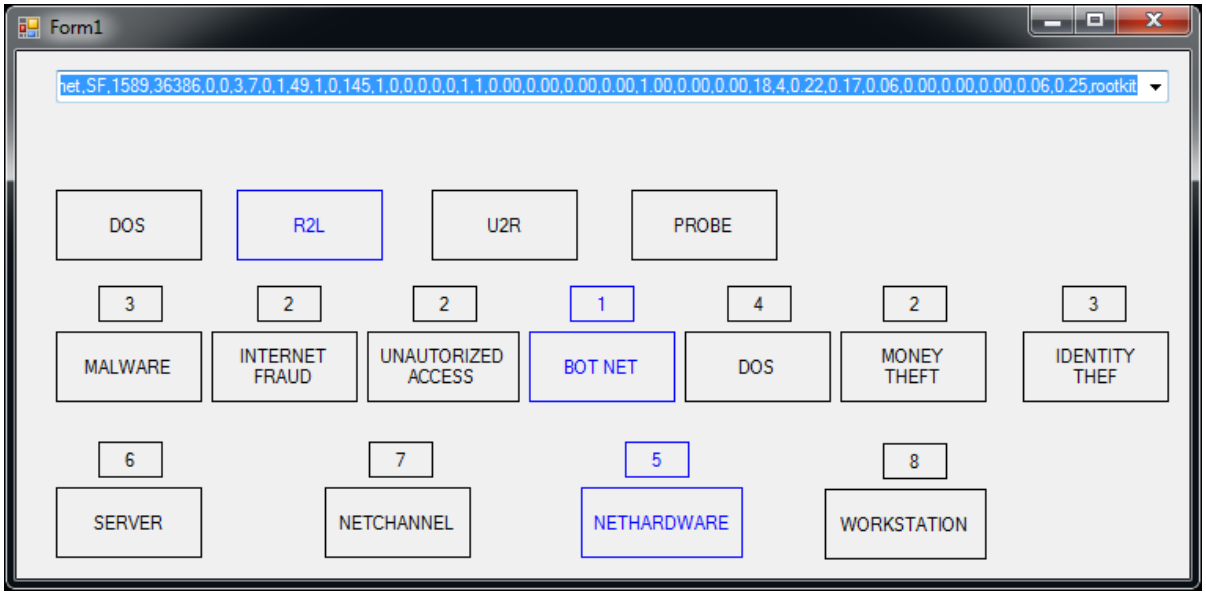



Рис. 3.3. Враження складової ІКС Nethardware

*Таблиця 3.3*

Вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації атаки R2L

| Атака | Вагові коефіцієнти виникнення інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| R2L | 3 | 2 | 2 | 1 | 4 | 2 | 3 |

*Таблиця 3.4*

Оцінювання впливу інциденту інформаційної безпеки Botnet на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | = | > | < | 6 | 2 |
| 2. Netchannel | = | – | < | = | 7 | 3 |
| 3. Nethardware | > | > | – | < | 5 | 1 |
| 4. Workstations | < | = | < | – | 8 | 4 |

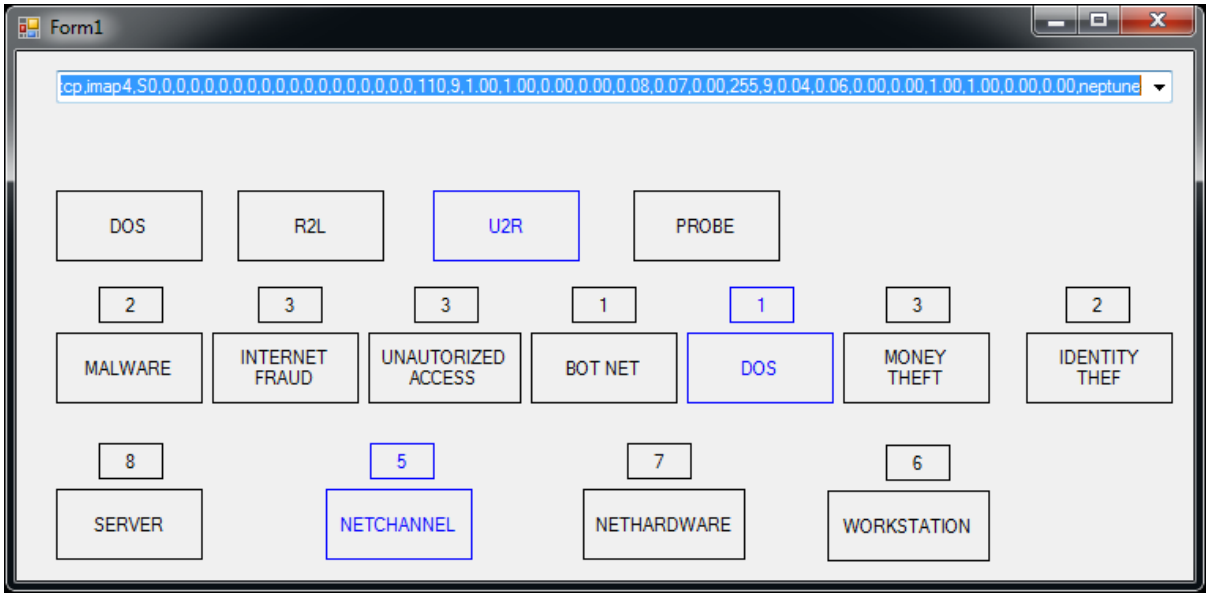



Рис. 3.4. Враження складової ІКС Netchannel

*Таблиця 3.5*

Вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації атаки U2R

| Атака | Вагові коефіцієнти виникнення інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| U2R | 2 | 3 | 3 | 1 | 1 | 3 | 2 |

*Таблиця 3.6*

Оцінювання впливу інциденту інформаційної безпеки DDoS на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | = | < | < | 8 | 4 |
| 2. Netchannel | = | – | > | = | 5 | 1 |
| 3. Nethardware | < | > | – | < | 7 | 3 |
| 4. Workstations | < | = | > | – | 6 | 2 |

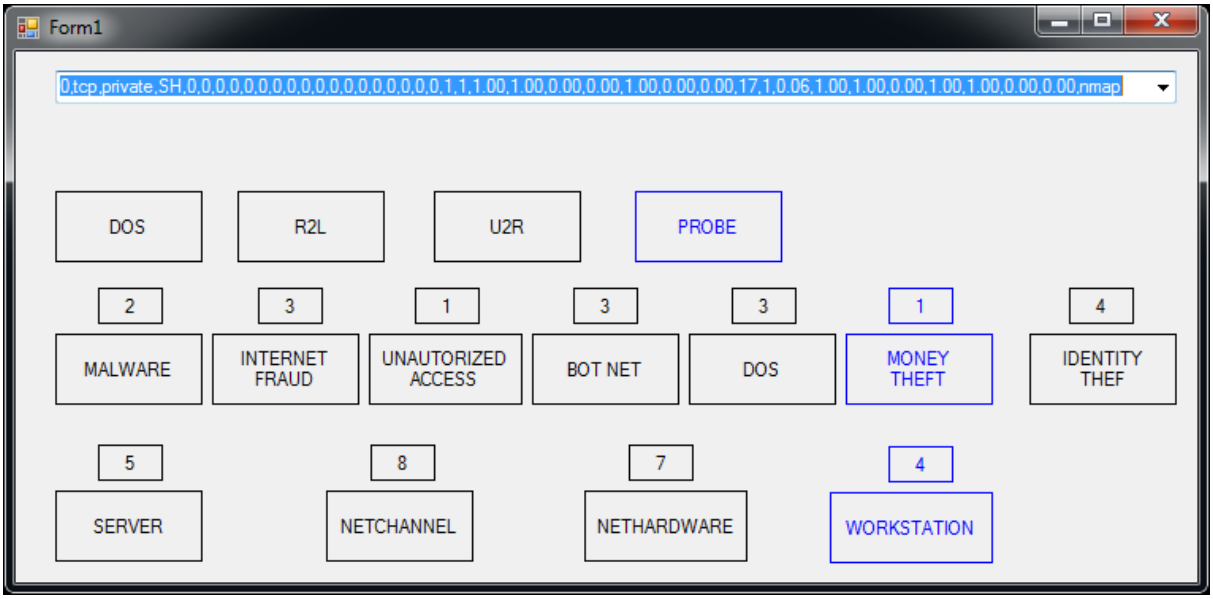



Рис. 3.5. Враження складової ІКС Workstation

*Таблиця3.7*

Вагові коефіцієнти виникнення інцидентів інформаційної безпеки при реалізації атаки PROBE

| Атака | Вагові коефіцієнти виникнення інцидентів інформаційної безпеки | | | | | | |
|---|---|---|---|---|---|---|---|
| | Malware | Internet Fraud | Unauthorized Access | Botnet | DDoS | Money Theft | Identity Theft |
| PROBE | 2 | 3 | 1 | 3 | 3 | 1 | 4 |

*Таблиця 3.8*

Оцінювання впливу інциденту інформаційної безпеки Money Theft на складові ІТС

| № складової ІТС / Складові ІТС | 1 | 2 | 3 | 4 | Бал, «вага» критерію | Місце критерію в ранжуванні |
|---|---|---|---|---|---|---|
| 1. Server | – | > | = | = | 5 | 2 |
| 2. Netchannel | < | – | = | < | 8 | 4 |
| 3. Nethardware | = | = | – | < | 7 | 3 |
| 4. Workstations | > | = | > | – | 4 | 1 |

### 3.2. Рекомендації щодо захисту складових в ІС

З метою уникнення настання інцидентів інформаційної безпеки було розроблено низку рекомендацій для кожної складової ІС.

**Основні рекомендації щодо захисту серверного обладнання (Server):**

- Слідкувати за оновленням операційної системи та іншого програмного забезпечення, що використовується.
- Використовувати програмний між мережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.
- Використовувати стійкі паролі, забезпечувати їх регулярну зміну; не зберігати автентифікаційні дані в легкодоступних місцях. Дотримуватися політики «чистого екрану» та «чистого робочого місця».
- Здійснювати резервне копіювання даних шляхом їх збереження на знімних носіях інформації (CD/DVD, HDDтощо); налаштувати функцію «відновлення системи».
- При користуванні послугами Інтернет-банкінгу, електронної пошти тощо, у разі необхідності введення автентифікаційних даних впевнитись у тому, що використовується захищене з'єднання HTTPS.

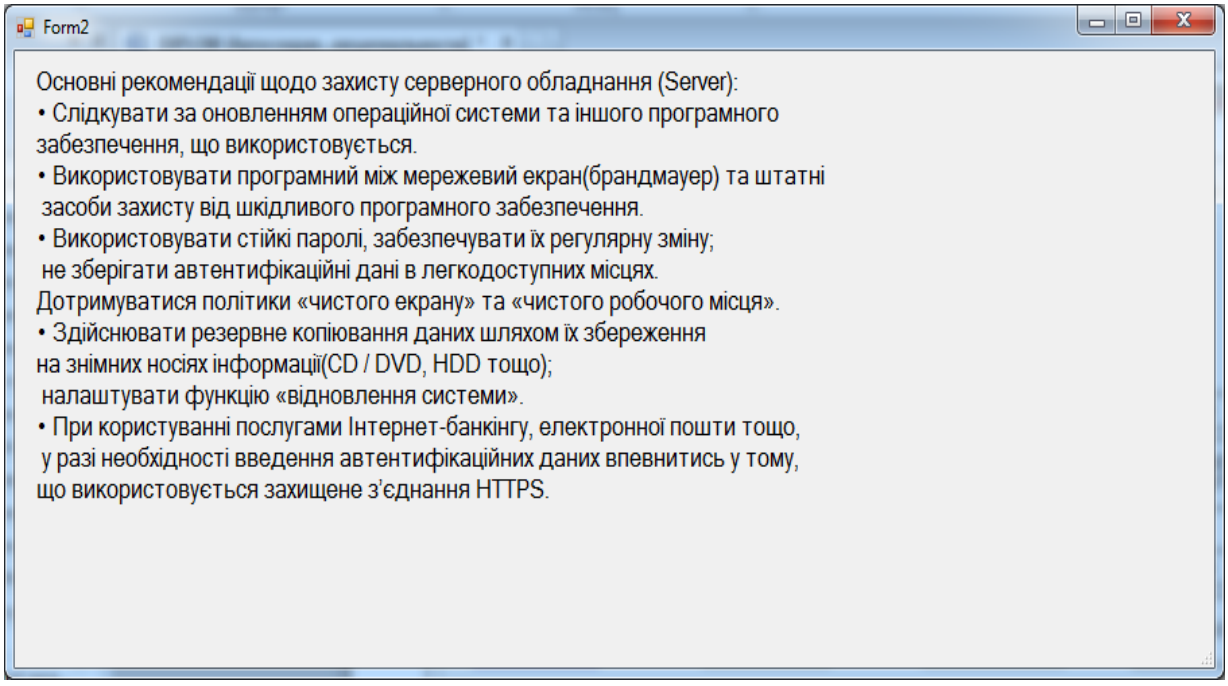



Рис. 3.6. Рекомендації для Server

**Основні рекомендації щодо захисту середовища передачі даних (Netchannel):**

- Не підключатись до загальнодоступних (незахищених) бездротових мереж; за необхідності використання таких бездротових мереж (в кафе, барах, аеропортах) ні в якому разі не вводити свої автентифікаційні дані (при доступі до електронної пошти, Інтернет-банкінгу тощо).

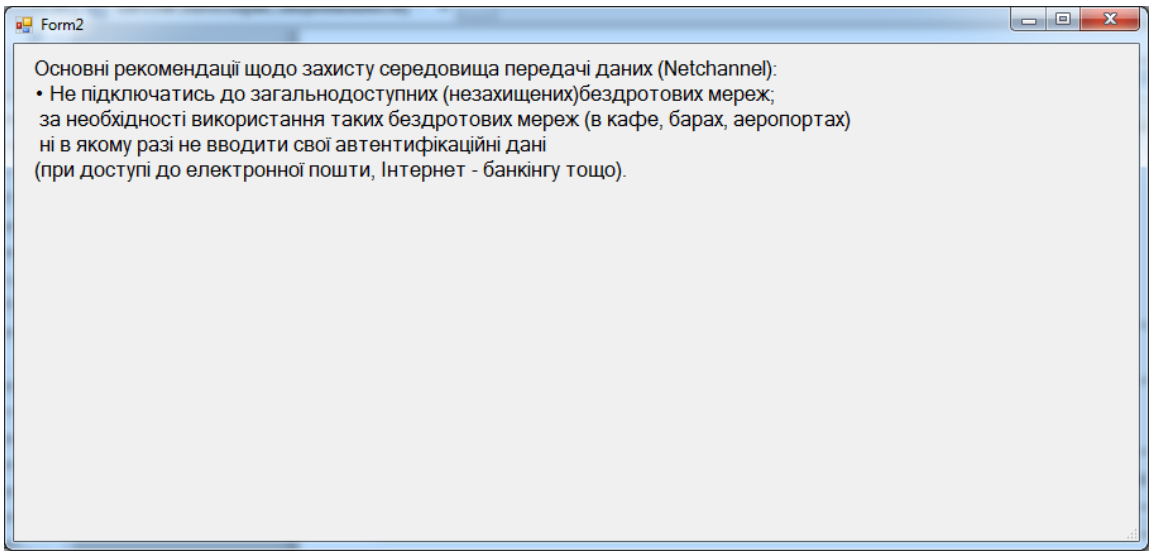



Рис. 3.7. Рекомендації для Netchannel

**Основні рекомендації щодо захисту автоматизованих робочих місць співробітників (Workstation):**

- Слідкувати за оновленням операційної системи та іншого програмного забезпечення, що використовується.
- Використовувати програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.
- Користуватися антивірусним програмним забезпеченням та регулярно оновлювати бази даних сигнатур вірусів.
- Працювати на АРМ під обліковим записом користувача, що не має адміністративних привілеїв. Не залишати АРМ «без нагляду» –блокувати сеанс роботи за допомогою комбінації клавіш «Win+L».
- Використовувати стійкі паролі, забезпечувати їх регулярну зміну; не зберігати автентифікаційні дані в легкодоступних місцях. Дотримуватися політики «чистого екрану» та «чистого робочого місця».

- При підключенні змінних носіїв інформації до АРМ забезпечувати їх автоматичну перевірку на наявність шкідливого програмного забезпечення; відключити автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

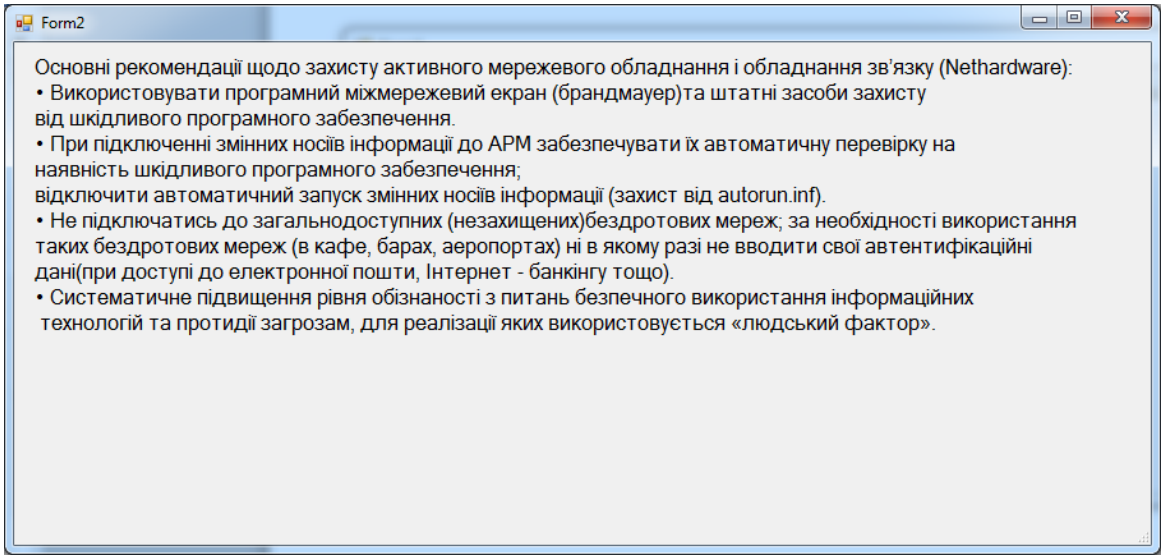



Рис. 3.8. Рекомендації для Workstation

**Основні рекомендації щодо захисту активного мережевого обладнання і обладнання зв'язку (Nethardware):**

- Використовувати програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.
- При підключенні змінних носіїв інформації до АРМ забезпечувати їх автоматичну перевірку на наявність шкідливого програмного забезпечення; відключити автоматичний запуск змінних носіїв інформації (захист від autorun.inf).
- Не підключатись до загальнодоступних (незахищених) бездротових мереж; за необхідності використання таких бездротових мереж (в кафе, барах, аеропортах) ні в якому разі не вводити свої автентифікаційні дані (при доступі до електронної пошти, Інтернет-банкінгу тощо).

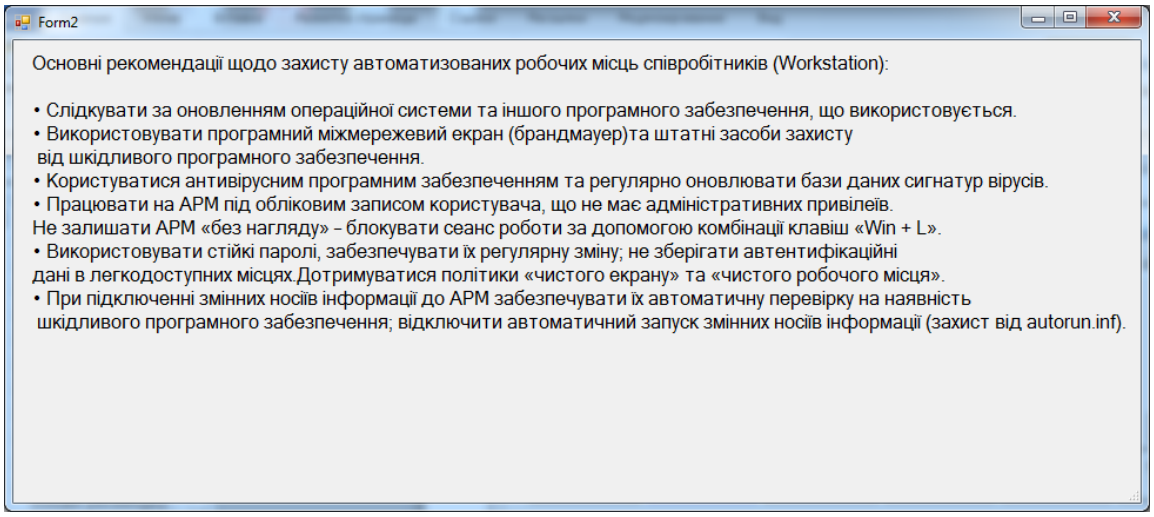



Рис. 3.9. Рекомендації для Nethardware

### 3.3. Висновки до третього розділу

У третьому розділі було експериментально досліджено розроблений метод мереживо – центричного моніторингу інцидентів інформаційної безпеки в інформаційно-комунікаційних системах за рахунок створення програмного засобу тестування, який на виході визначає складову ІКС, яка найбільш вражена і видає рекомендації по її захисту. Також наведено алгоритм роботи програмного засобу, який описує його покрокову роботу. Розраховані всі значення, за якими програмний засіб визначає виникнення можливих інцидентів інформаційної безпеки.

Роблячи висновок, можна сказати, що експериментальне дослідження запропонованого методу підтвердило можливість його застосування у реальних системах захисту інформації для визначення необхідних заходів щодо ліквідації наслідків кожного виду інцидентів інформаційної безпеки; формування цілей паралельної ліквідації можливих видів інцидентів інформаційної безпеки, їх синхронізацію, ранжирування; реалізацію паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних сил і засобів; формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування силами і засобами в динаміці управління кіберінцидентами; попередження виникнення інцидентів інформаційної безпеки, як наслідок зниження затрат на їх ліквідацію.

# ВИСНОВКИ

Результатом виконаної роботи являється розроблений програмний застосунок метод контролю та виявлення інцидентів інформаційної безпеки.

У процесі виконання роботи було отримано такі результати:

1. Проведено аналіз існуючих методів, моделей і систем обробки прогнозування та моніторингу інцидентів ІБ в інформаційно-комунікаційних системах, що дозволило виявити їх недоліки і формалізувати завдання щодо розробки методу мережево-центричного моніторингу інцидентів ІБ.
2. Запропоновано програмний застосунок управління інцидентами ІБ, за рахунок використання методу контролю та виявлення інцидентів, що дозволяє проводити моніторинг інцидентів інформаційної безпеки, прогнозувати їх вплив на складові інформаційно-комунікаційних систем і обирати відповідні превентивні заходи.
3. Проведено експериментальне дослідження розробленого застосунку, що підтвердило можливість його застосування у реальних системах захисту інформації для визначення необхідних заходів щодо ліквідації наслідків кожного виду інцидентів ІБ; формування цілей паралельної ліквідації можливих видів інцидентів ІБ, їх синхронізацію, ранжирування; реалізацію паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних сил і засобів; формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування силами і засобами в динаміці управління інцидентами ІБ; попередження виникнення інцидентів ІБ, як наслідок зниження затрат на їх ліквідацію.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гнатюк С. О., Кищенко В. В., Котелянець В. В., Бауиржан М. Мережево-центричний моніторинг інцидентів кібербезпеки у секторах критичної інфраструктури держави. Кібербезпека: освіта, наука, техніка. № 2 (2), 2018. С. 80-89.

2. Образцов Е.С. Мониторинг как средство защиты информации/Е.С. Образцов // Перспективы развития информационных технологий . 2012. №9.

3. Израэль Ю.А. Глобальная система наблюдений. Прогноз и оценка окружающей природной среды. Основы мониторинга / Ю.А. Израэль // Метеорология и гидрология. 1974, 7. – С. 3-8.

4. Управление инцидентами [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://solarsecurity.ru/products/jsoc/monitoring/.

5. EnCase Enterprise[Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://www.guidancesoftware.com.

6. OTRS ITSM [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: https://www.otrs.com/software/otrsitsm-features/?lang=ru.

7. BPMonline Service Desk [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://www.terrasoft.ru/products/service_desk/bpmonlinesd.

8. NetForensics[Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://www.osp.ru/cw/2004/47/83746.

9. SysAid Pro [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://rutracker.org/forum/viewtopic.php?t=3398446.

10. Axios Assyst 7 [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://www.osp.ru/data/275/142/1239/1-18.pdf.

11. BMC Remedy ITSM Suite[Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://ru.wikipedia.org/wiki/BMC_Remedy_Action_Request_System.

12. HPServiceManager 7 [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL:http://www.terrasoft.ua/industry/telecom.

13. Naumen Service Desk [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://www.naumen.ru/products/service_desk/?utm_source=google&utm_medium=cpc&utm_campaign=google.

14. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности: ГОСТ Р ИСО/МЭК ТО 18044—2007. Введ. 2008.07.01. – М. :ИПК «Издательство стандартов», 2008. – 2 с.

15. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования: ГОСТ Р ИСО/МЭК 27001—2006. Введ. 2006.12.27. – М. :ИПК «Издательство стандартов», 2006. – 2 с.

16. Попов, С.В. О влиянии состояний функционирования средств защиты информации на эффективность мониторинга инцидентов информационной безопасности банка / С.В. Попов, В.Н. Шамкин // Вест. Тамб. гос. техн. ун-та. – 2011. – Т. 17, № 2. – С. 297–303.

17. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положення: СТО БР ИББС-1.0-2014. – 9 с.

18. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности : ГОСТ Р ИСО/МЭК ТО 18044–2007.Введ. 2007–12–27. – М. : Стандарт- информ. – 2009. – 46 с.

19. Попов С.В. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности / С.В. Попов, В.Н. Шамкин // Вестник ТГТУ . 2012. №1

20. Miller D.R. Security Information and Event Management (SIEM) / Sh. Harris, A.A.Harper, S.VanDyke, Ch. Black // Implementation. McGraw–Hill Companies. 2011. – 430 p.

21. Попов, С.В. Факторы, влияющие на эффективность мониторинга инцидентов информационной безопасности в автоматизированной банковской системе / С.В. Попов, В.Н. Шамкин // Науч.-техн. вестн. Поволжья. – 2010. – № 1 – С. 145–148.

22. IT-Grundschutz Catalogues, Bundesamt für Sicherheit in der Informationstechnik, 2005, URL: https://www. bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_ node.html.

23. Григорьев А.Н.. InfoStream. Мониторинг новостей из Интернет: технология, система, сервис: научно-методическое пособие. / А.Н. Григорьев, Д.В Ландэ, С.А. Бороденков, Р.В. Мазуркевич, В.Н. Пацьора - Киев: ООО "Старт-98", 2007. - 40 с.

24. Мониторинг компьютерной сети сети [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8.

25. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных інфраструктурах / *И.В.* Котенко, И.Б. Саенко, О.В. Полубелова О, А.А. Чечулин. – Труды СПИИРАН. 2012. Вып. 20. С. 27-56.

26. Котенко И.В. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников / И.В. Котенко, М.В. Степашкин, В.С. Богданов //Проблемы информационной безопасности. Компьютерные системы. 2006, №. 2, С.7–24.

27. Моніторинг бюджету - кому вигідно [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://uabudget.blogspot.com/2010/05/blog-post_14.html.

28. Макашова В.Н. Современные аспекты распространения киберэкстремистской идеологии в молодежной ИТ-среде / В.Н. макашова, Е.В. Чернова, И.И. Боброва // Фундаментальные исследования . 2014. №12-6.

29. Гладыш С.В. Иммунокомпьютинг в управлении инцидентами информационной безопасности / С.В. Гладыш // Штучний інтелект. — 2008. — № 1. — С. 123-130.

30. Автоматическая регистрация инцидентов с использованием кнопки помощи ITSM [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://911.prolan.ru/applying/registration.html.

31. Артамонов В.С. Информационное обеспечение государственной пожарно-спасательной службы в условиях чрезвычайных ситуаций / В.С. Артамонов, В.Е. Кадулин, Р.Н. Козленко // Вестник Санкт-Петербургского университета ГПС МЧС России. 2003. № 3. С.58–59.

32. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев . – СПб.: БХВ- Петербург, 2003. 752 с.

33. Лукацкий А.В. Обнаружение атак /А.В. Лукаций// 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2003. 608 с.

34. Моудер Дж. Исследование операций: в 2 т: пер. с англ. / Под ред. Дж. Моудера, С. Элмаграби. М.: Мир, 1981.

35. Куватов В.И. Исследование операций / В.И. Куватов, Г.А. Величко //Петродворец.: ВМИРЭ, 2000. 374 с.

36. Тушавин В. А. Использование теории ограничений для совершенствования менеджмента инцидентов / В.А. Тушавин // Молодой ученый. — 2011. — №6. Т.1. — С. 110-112.

37. Таха Х. Введение в исследование операцій / Х. Таха; в 2 кн: пер. с англ. - М.: Мир, 1985.

38. Котенко И.В. Методика выбора контрмер в системах управления информацией и событиями безопасности / И.В. Котенко, Е.В. Дойникова // Информационно-управляющие системы . 2015. №3 (76).

39. Иванов А.Ю. Военно-технические основы построения и математическое моделирование перспективных средств и комплексов автоматизации / А.Ю. Иванов, С.П. Полковников С, Г.Б. Ходасевич. - СПб.: ВАС, 1997. 419 с.

40. Системный анализ в управлении: учеб. пособ. / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; под ред. А.А. Емельянова. М.:Финансы и статистика, 2002. 368 с.

41. Бусленко Н.П. Моделирование сложных систем / Н.П. Бусленко – М.: Наука, 1978. 399 с.

42. Урзов А.Ю. Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности / А.Ю. Урзов, С.К. Варлатая //Доклады ТУСУР . 2013. №2 (28).

43. Кошельок Г. В. Статистичні методи прогнозування грошових потоків підприємства / Г. В. Кошельок // Економіка підприємства: сучасні проблеми теорії та практики. Матеріали четвертої міжнародної науково-практичної конференції (м. Одеса, 18 вересня 2015 року). – Одеса: Атлант, 2015. – С. 273-274.

44. Размещение компонентов системы мониторинга информационного пространства [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://essuir.sumdu.edu.ua/bitstream/123456789/28595/1/automated%20control.pdf.

45. Шевчук Н. С. Методи прогнозування кредитоспроможності підприємств / Н. С. Шевчук // Вісник соціально-економічних досліджен: збірник наукових праць / гол. ред. М. І. Звєряков ; Одеський держ. екон. ун-т. - Одеса: ОДЕУ, 2007. – Вип. 26. – С. 387-391.

46. Нікуліна Т. М. Основні напрямки та переваги сучасних інформаційно-аналітичних систем прогнозування економічних ситуацій / Т. М. Нікуліна // Вісник соціально-економічних досліджень : зб. наук. пр. / голов. ред. М. І. Звєряков; Одеський держ. екон. ун-т. – Одеса, 2010. – Вип. 40. - С. 279-282.

47. Мацкул В. М. Моделювання та прогнозування надходжень пдв на мікро- та макроекономічних рівнях / В. М. Мацкул, Л. О. Кирилова // Вісник соціально-економічних досліджень: зб. наук. пр. / голов. ред. М. І. Звєряков; Одеський нац. екон. ун-т. – Одеса, 2013. – Вип. 2 (49), Ч. 2. – С. 53-59.

48. Рзаєв Г.І. Використання Інтернет-ресурсів у менеджменті конкурентоспроможності підприємств/ Г.І. Рзаєв // Вісник Національного університету "Львівська політехніка". Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку, 2009. - Т 647. - С. 596-600.

49. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью/И.В. Котенко – Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Т.41, Москва, URSS, 2009. С.74–103.

50. Казакова Н.Ф. Метод системного багаторівневого прогнозування / Н. Ф. Казакова, А. М. Кушер А.М. // Матеріали II Міжнар. наук.-практ. конф. «Обробка сигналів і негаусівських процесів» (Черкаси, 25-29 травня 2009 г.) – Черкаси: ЧДТУ, 2009.

51. Янковий О.Г. Вдосконалення планування на підприємстві за допомогою математико-статистичних методів прогнозування / О.Г. Янковий, О.Л. Гура // Актуальні проблеми економіки. – 2009. – №1(91). – С. 229–238.

52. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // В.О.Гнатюк / Безпека інформації. – №3 (19). – 2013. – С. 175-180.

53. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности: ISO/IEC 27035:2011. Введ. 2011.09.01. – М.: ИПК «Издательство стандартов», 2011. – 78 с.

54. Синявский В.К. Влияние содержания и принципов «сетецентрической войны» на процессы управления войсками (силами) / В.К. Синявский // Наука и военная безопасность. – 2010. – №4.

55. Парадигма сетецентрического управления и ее влияние на процессы управления войсками [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://agat.by/pres/statia%20nayka-3.pdf.

56. Network centric warfare and wireless communications: [Электронний ресурс]. – Режим доступа:World Wide Web. – URL: http://www.meshdynamics.com/military-mesh-networks.html.

57. Затуливетер, Ю.С.Компьютерный базис сетецентрического управления / Ю.С. Затуливетер // Труды российская конференции с международным участием "Технические и программные средства в системе управления, контроля и измерения". - Москва, 18-20 октября 2010 г. - С.17-37.

58. Трахтенгерц Э.А. Сетецентрические методы компьютерной поддержки управления ликвидацией последствий чрезвычайных ситуаций /Шершаков В.М., Трахтенгерц Э.А.,Камаев Д.А. - М.: ЛЕНАНД, 2015. - 160 с.- ISBN 978-5-9710-1557-4.

59. Про захист інформації в інформаційно-телекомунікаційних системах [Текст] : Закон України № 80/94-ВР від 5 липня 1994 р. / Верховна Рада України // Відомості Верховної Ради України. – 1994. - №31. – Ст.286.

60. CERT-UA [Электронний ресурс]. – Режим доступа:WorldWideWeb. – URL: http://cert.gov.ua/.

61. Пархоменко Ю.О. Метод мережево-центричного моніторингу інцидентів інформаційної безпеки в інформаційно-комунікаційних системах / Ю.О. Пархоменко, В.О. Гнатюк //VI міжнародна науково-технічна конференція «ITSEC» (ITSEC-2016, 17-19 травня 2016 р.): тези доп. – К.: НАУ, 2016. – С. 26-27

62. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації – 2012. –№1.