ПРОБЛЕМИ ТА ШЛЯХИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ДЛЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ДСНС УКРАЇНИ

Кальченко Є.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: yehor.kalchenko@nure.ua

Abstract

The State Emergency Service of Ukraine (SES) is a key entity responsible for performing essential functions for the state and society. The Information and Communication System (ICS) of the SES – which includes Data Processing Centers (DPCs) and the Departmental Information and Communication System (DICS-DPC) – is a target of constant and deliberate cyberattacks. Proper functioning of the SES ICS requires protection in accordance with the provisions of the Laws of Ukraine "On Information Protection in Information and Communication Systems" and "On Personal Data Protection". The purpose of this work is to analyze the key problems identified during the processing of cyber incidents within the SES ICS and to determine priority directions for building a resilient, efficient, and automated Cybersecurity Incident Management System (CSIMS).

Актуальність побудови та вдосконалення системи управління кіберінцидентами підтверджується історичними деструктивними кібероперaціями. Наприклад, у 2022 році Державна служба України з надзвичайних ситуацій (далі - ДСНС) виявила, що інформація в понад 20 системах в адміністративній будівлі та певній кількості систем у Головних управліннях (ГУ) була стерта за допомогою шкідливого програмного забезпечення Wiper [1]. Зловмисник, що, ймовірно, належить до угрупування UNC3666 або APT28, міг мати доступ до мережі ДСНС принаймні з жовтня 2019 року. Це демонструє необхідність не лише реагування, але й проактивного захисту та мінімізації негативних наслідків тривалих вторгнень.

Аналіз результатів розслідування кіберінцидентів та внутрішніх планів ДСНС виявляє низку системних проблем, які необхідно усунути для підвищення кіберстійкості.

1. Залежність від застарілих та вразливих систем. Первинне ураження мережі ДСНС було здійснено через встановлення бекдору Metasploit на застарілий внутрішній сервер Windows [1]. Крім того, зловмисники використовували вразливості, пов'язані зі скомпрометованим мережним обладнанням (наприклад, 243 одиниці мережного обладнання було скомпрометовано, включаючи маршрутизатори Cisco). Неоновлене програмне забезпечення (ПЗ) та грубі помилки адміністраторів залишаються ключовими загрозами, оскільки хакери експлуатують вразливості протягом лічених годин після їх розголошення.

2. Проблеми з контролем доступу та безпекою облікових записів. Злам облікових записів є критичним вектором. Під час вторгнення було скомпрометовано 78 облікових записів [1]. Зловмисники використовували викрадені облікові дані для доступу до системи VoIP PBX («Вільха») та скомпрометували поштові скриньки. Однією з передумов ускладненого реагування була відсутність централізованої системи керування користувачами та комп'ютерами.

3. Недостатня централізація та автоматизація виявлення. Хоча ДСНС залучала партнера - Національний координаційний центр кібербезпеки (далі – НКЦК) для реагування, відсутність централізованого моніторингу ускладнювала стримування [1]. Це включає нестачу централізованого збору логів та моніторингу мережної активності для своєчасного виявлення підозрілої діяльності.

4. Ризики, пов'язані з інформацією з обмеженим доступом (далі – ІзОД). Існує потреба у проведенні регулярних перевірок на виявлення фактів можливої обробки ІзОД та персональних даних

на не атестованих засобах обчислювальної техніки. Прикладами конфіденційної інформації, до якої зловмисники отримали доступ, є бази даних контактів та інформація про співробітників, включно з номерами телефонів.

5. Слабка стійкість та відновлення. Деструктивні атаки (Wiper) підкреслили критичну залежність від надійних планів резервного копіювання та відновлення. У випадку критичних інцидентів (як атака на державні реєстри Мін'юсту у 2024 році [2]) потрібен перегляд стратегій резервування та підвищення стійкості.

Так, відповідно до аналітики інцидентів, опрацьованих Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та SOC Державного центру кіберзахисту Держспецзв'язку за 2024 рік спостерігається зростання загальної кількості кіберінцидентів [4] (таблиця 1, рис.1).

Табл. 1. Загальна кількість інцидентів у 2024 році

Перше півріччя 2024 року	Друге півріччя 2024 року	Приріст кількості інцидентів, (%)
1739	2576	+48%

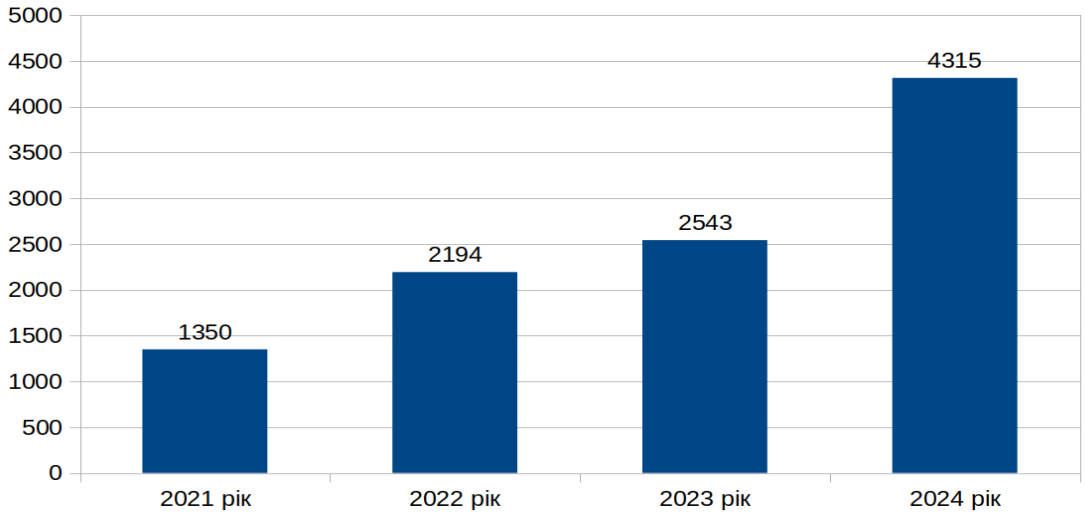

Рис. 1. Результати розподілу виявлених кіберінцидентів за роками

Побудова ефективної системи управління кіберінцидентами для інформаційно-комунікаційної системи (ІКС) ДСНС має бути реалізована через комплекс організаційно-технічних заходів, спрямованих на проактивне виявлення, швидку локалізацію та забезпечення стійкості (відновлення).

1. Розбудова платформи виявлення та автоматизації (Detection and Automation). Ключовим шляхом є розширення функціональних можливостей підходів управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) на базі ArcSight Enterprise. Необхідні заходи:

– інтеграція та кореляція: налаштування та інтеграція консолі керування агентів кінцевих пристроїв Palo Alto Cortex XDR (EDR) з ArcSight SIEM для отримання та аналізу телеметрії з кінцевих робочих станцій. Створення та вдосконалення правил кореляції ArcSight з адаптацією до нових видів атак;

– автоматизація реагування (SOAR): проведення заходів щодо налаштування ArcSight SOAR для ефективної автоматизації процесів реагування, включаючи інтеграцію з Cisco Firewall Management Center;

– централізоване логування: налаштування окремого сервера для централізованого зберігання журналів подій (логів) із мережного обладнання (з використанням rsyslog та syslog nginx) для постійного моніторингу.

2. Впровадження суворих процедур реагування та пріоритезації: дії реагування мають бути пропорційними рівню загрози, що класифікуються за чотирма рівнями критичності (0–3):

Табл. 2. Рівні критичності ймовірних кіберінцидентів

Категорія (Рівень)	Загроза та Наслідки	Часовий проміжок реагування	Ключова дія
Рівень 3 (Високий / Червоний)	Безпосередньо загрожує сталому функціонуванню Ресурсів захисту; **порушується захищеність** інформації; виникають потенційні загрози впливу на інші суб'єкти кібербезпеки.	**Миттєва реакція (0–15 хвилин)**.	**Термінове відключення (ізоляція) зовнішніх каналів зв'язку** скомпроментованої системи.
Рівень 2 (Середній / Жовтий)	Створюються **передумови для порушення захищеності** інформації (конфіденційності, цілісності, доступності); виникають передумови для припинення виконання функцій ДСНС.	**Миттєва реакція (0–15 хвилин)**.	**Термінове відключення (ізоляція) від ВІКС-ЦОД** окремого хосту, сегмента або всієї мережі підрозділу **без погодження та уточнення даних**.
Рівень 1 (Низький / Зелений)	Існує ймовірність загрози сталому функціонуванню, але без прямої загрози захищеності інформації.	**Швидке реагування до 30 хвилин** (на першочерговий запит) та **до 40 хвилин** (при глибокому розслідуванні).	Уточнення інформації; у випадку підтвердження – **локалізація (ізоляція) загрози**.
Рівень 0 (Некритичний / Білий)	Штатні або позаштатні інциденти (планові роботи, технічні проблеми, аварії в мережі).	За узгодженням часу (в екстрених випадках — без).	Відключення відбувається з попередженням про відсутність доступу.

Проведений аналіз категорій кіберінцидентів дозволив співвіднести основні типи загроз [3] з рівнями критичності (0–3) відповідно до їх потенційного впливу на конфіденційність, цілісність та доступність інформаційних систем.

Інциденти, що належать до категорії образливого або небажаного контенту (Код 01), у переважній більшості класифікуються як некритичні (Рівень 0), оскільки не спричиняють технічних порушень. Підвищення рівня можливе лише у разі переходу до фішингу або використання персональних даних.

Загрози, пов'язані зі шкідливим програмним кодом (Код 02), здебільшого належать до Рівня 2, а у разі ураження критичних ресурсів або ексфільтрації даних – до Рівня 3. Особливо небезпечними є rootkit-, ransomware- та botnet-інциденти.

Категорії збирання інформації (Код 03) та спроб втручання (Код 04) здебільшого мають Рівень 1–2, залежно від потенціалу ескалації. Експлуатація 0-day вразливостей або успішний доступ до критичних систем віднесено до Рівня 3.

Інциденти групи втручання (Код 05) становлять найбільшу загрозу. Компрометація привілейованих облікових записів завжди класифікується як Рівень 3, тоді як компрометація систем та застосунків – як Рівень 2–3, залежно від масштабів.

Порушення доступності (Код 06) у вигляді DoS/DDoS відносяться до Рівня 2, а навмисні деструктивні дії – до Рівня 3. Технічні збої без ознак атаки визначаються як Рівень 0–1.

Порушення конфіденційності та цілісності інформації (Код 07) здебільшого належать до Рівня 2–3, оскільки впливають на основні властивості інформаційної безпеки.

Категорії шахрайства (Код 08) та відомих вразливостей (Код 09) визначаються як Рівень 1–2, у той час як інциденти, що не підпадають під чітку класифікацію (Код 10), первинно оцінюються як Рівень 1 з подальшим уточненням.

Миттєва ізоляція: Для інцидентів високого (Рівень 3) та середнього (Рівень 2) критичності необхідна миттєва реакція (0–15 хвилин). У випадку виявлення стороннього втручання до ЦОД

(Рівень 3) або DDoS-атаки/розповсюдження вірусів (Рівень 2), ключовою дією є термінове відключення (ізоляція) зовнішніх каналів зв'язку скомпроментованої системи або сегмента мережі.

Підготовка до відновлення: налаштування резервних ПК (не менше п'яти в ГУ) з безпечно налаштованою операційною системою (ОС), агентом захисту та встановленим VPN-клієнтом для забезпечення доступу до ІКС ДСНС у випадку ізоляції локальної мережі підрозділу.

Оперативна взаємодія: постійна взаємодія з основними суб'єктами забезпечення кібербезпеки (Держспецзв'язку, CERT-UA, СБУ, НКЦК). У разі фіксації шкідливих програм або загроз слід НЕГАЙНО інформувати CERT-UA [4].

3. Посилення превентивного кіберзахисту (Hardening): Необхідно зосередитися на усуненні векторів атак, які використовувалися раніше:

– управління доступом та сегментація: впровадження Port Security (BIND за принципом IP+MAC+Port) на мережному обладнанні. Обмеження доступу до інформаційних ресурсів та мережного обладнання через адміністративні порти (SSH, RDP) лише з визначених IP-адрес робочих станцій адміністраторів. Впровадження окремих VLAN-ів для адміністраторів, MGMT та серверного сегменту;

– безпека облікових записів: зміна адміністративних паролів на складні та унікальні (мінімум 12–16 символів). Створення нових індивідуальних облікових записів для адміністраторів з подальшим видаленням стандартних облікових записів типу "admin" або "root". Ввімкнення багатофакторної автентифікації (MFA) для служб, що підключаються до Інтернету.

– управління вразливостями: забезпечення своєчасного оновлення програмного забезпечення серверів, сервісів та мережного обладнання до актуальних версій з урахуванням усіх патчів безпеки. Проведення регулярного сканування вразливостей (pentest) мережі.

– контроль трафіку: адміністрування міжмережних екранів Cisco FirePower з метою блокування трафіку, пов'язаного з TOR мережами, Telegram, Viber, AnyDesk та torrent.

4. Забезпечення стійкості та резервного копіювання:

– регулярне копіювання: проведення позачергового резервного копіювання конфігурацій мережного обладнання та інформаційних систем з обов'язковим зберіганням на окремих зовнішніх носіях. Створення резервних копій має відбуватися з дотриманням вимог щодо їх захисту, цілісності та конфіденційності.

– плани: актуалізація та затвердження планів резервного копіювання серверів, сервісів та мережного обладнання.

Таким чином побудова ефективної системи управління кіберінцидентами для ІКС ДСНС є невідкладним завданням, що вимагає переходу від традиційного реагування до проактивної кіберстійкості. Ключові шляхи вирішення проблем включають централізацію виявлення загроз (SIEM/SOAR/XDR), сувору сегментацію мережі, посилення політик керування привілейованими обліковими записами та впровадження багатофакторної аутентифікації, а також безумовну миттєву ізоляцію скомпрометованих сегментів (0–15 хвилин). Ці заходи, у поєднанні з регулярним оновленням ПЗ та взаємодією з CERT-UA та СБУ, мінімізують вікно атаки та забезпечать належний рівень захисту критичних інформаційних ресурсів ДСНС.

Література

1. Лист ДСНС України від 05.08.2022 №16-5114/163-1 "Про розслідування кіберінцидентів у ДСНС та звітування з виконання заходів за напрямом кіберзахисту" на 18 арк.

2. Публікація Державної служби спеціального зв'язку та захисту інформації України про російські кібер-операції "Аналітика за II півріччя 2024 року". URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=68769&embedded=true&a=bi (дата звернення: 02.09.2025).

3. Спільний документ ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs). URL: https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf (дата звернення: 02.09.2025).

4. Лист Генерального штабу Збройних Сил України від 10.11.2022 № 300/1/С/4888 щодо заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури на 4 аркушах.