

**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**

**ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В  
ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА**



**МІЖНАРОДНА  
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ  
«ЖИВУЧИСТЬ ТА РЕЗИЛЬЄНТНІСТЬ – 2023»  
(«SURVIVABILITY & RESILIENCE – 2023»)**

Збірник матеріалів конференції  
19 жовтня 2023 р.

Київ – 2023

УДК 004.052.2

Рекомендовано до друку Вченою радою  
Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України  
(протокол №8 від 28 вересня 2023 р.)

Програмний комітет:

***В.В. Мохор***, доктор технічних наук, член-кор. НАН України  
***О.Г. Додонов***, доктор технічних наук, професор,  
***О.Г. Корченко***, доктор технічних наук, професор,  
***С.Є. Саух***, доктор технічних наук, член-кор. НАН України  
***В.М. Різак***, доктор фіз.-мат. наук, професор,  
***О.А. Чемерис***, доктор технічних наук, професор,  
***А.М. Давиденко***, доктор технічних наук,  
***С.Я. Гільгурт***, доктор технічних наук,  
***В.О. Артемчук***, доктор технічних наук,  
***В.М. Білецький***, доктор технічних наук, професор,  
***Ю.М. Коростіль***, доктор технічних наук, професор,  
***В.Д. Самойлов***, доктор технічних наук, професор,  
***С.Д. Винничук***, доктор технічних наук, професор,  
***Б.В. Дурняк***, доктор технічних наук, професор,  
***О.В. Тимченко***, доктор технічних наук, професор,  
***А.В. Яцишин***, доктор технічних наук.

Організаційний комітет:

***А.М. Давиденко***, доктор технічних наук,  
***С.Я. Гільгурт***, доктор технічних наук,  
***М.Г. Кузнєцова***, кандидат технічних наук,  
***М.П. Пригара***, кандидат технічних наук,  
***О.В. Цуркан***  
***О.С. Потенко***

Survivability & Resilience – 2023 : collection of materials of the international scientific and practical conference, Kyiv, October 19, 2023, PIMEE of NAS of Ukraine. – 2023. – 153 p.

Живучість та резильєнтність критичної інфраструктури – 2023 : збірник матеріалів міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023 р., ПІМЕ ім. Г.Є. Пухова НАН України. – 2023. – 153 с.

© Автори публікацій, 2023

© Інститут проблем моделювання в енергетиці  
ім. Г.Є. Пухова НАН України, 2023

## ЗМІСТ

### **A. Yevdina, Y. Yevdin, S. Schantz**

Ensuring the survivability and resilience of the decision support system rodos at the federal office for radiation protection..... 8

### **Л.В. Ковальчук, М.С. Кондратенко**

Аналіз юридичного статусу смарт-контрактів та проблем, які виникають при узгодженні їх з законодавством України.....10

### **В.Ю. Зубок, Р.С. Драгунцов**

Визначення кіберстійкості в нормативно-правовому полі Європейського Союзу і України та застосування його до ІКТ під впливом енергетичних загроз.....13

### **О.Г. Додонов, О.С. Горбачик, М.Г. Кузнцова**

Живучість інформаційних систем та забезпечення резильєнтності критичних інфраструктур.....18

### **К.В. Клименко, Н.М. Ухналь**

Впровадження парадигми резильєнтності у забезпечення функціонування критичної інфраструктури України.....21

### **А.В. Давидюк**

Процес управління вразливостями як складова кіберстійкості критичної інфраструктури.....25

### **К.Д. Ніколаєв**

Забезпечення раціонального природокористування як складової національної безпеки України.....28

### **Г.П. Костенко, А.О. Запорожець**

Огляд метрик резильєнтності енергосистеми на різних стадіях життєвого циклу.....31

### **О.О. Ципляк, В.О. Артемчук**

Перспективи застосування нейронних мереж архітектури типу LLAMA для швидкого прийняття рішень у відновленні глобальної енергосистеми.....37

**Д.І. Швайка, А.І. Швайка**

Використання баз даних у IoT платформі ThingsBoard: переваги та недоліки різних підходів.....41

**Н.А. Куликовська, А.В. Тіменко, С.С. Грушко, М.Б. Ільяшенко**

Резильєнтність IoT систем в умовах забезпечення цілісності передачі даних.....44

**О.О. Огір**

ELECTRON Usecase1: defending against power grid cyber attacks – insights from Ukraine.....46

**С.С. Штаненко, Ю.Я. Самохвалов**

Програмовані логічні інтегральні схеми як основа підвищення живучості сучасних технологічних систем.....49

**Т.В. Потаніна**

Корозійна стійкість і живучість тепловиділяючих елементів активної зони ядерного реактора.....51

**О. Dzhyhun, PhD, А. Onyskova**

Flexibility of the energy system model.....55

**Л.Ю. Гальчинський, В.В. Личик**

Проблематика підбору метрик для оцінки кібервідмовостійкості.58

**К.Ю. Зандер, В.О. Гнатюк**

Моделі та архітектура медичних інформаційн системи України..62

**В.М. Зварич**

Деякі питання впливу технічного стану двигунів власних потреб на оцінку резильєнтності теплової електростанції.....67

**О. І. Старовойтов**

Забезпечення резильєнтності підприємства електронної комерції.....69

**О.С. Потенко**

Розробка методики оцінки профілів функціональних послуг захисту на базі оптимізаційних підходів.....71

**Chaikin M.M.**

Introduction of the nist cybersecurity framework into the regulatory framework of ukraine, as a basis for the introduction of cyber resilience and implementation of cyber resilience review.....72

**О.Г. Додонов, А.І. Кузьмичов, Ю.В. Чернецька**

Модель кількісного оцінювання стійкості системи (розподілу енергетичних ресурсів).....78

**В.В. Шкарупило, В.В. Душеба, А.В. Тіменко**

Огляд рівнів забезпечення резилієнтності у галузі енергетики.....80

**Ф.О. Корбейніков**

Резильєнтний підхід до побудови розподіленої системи забезпечення інформаційної безпеки.....82

**М.М. Худинцев, І.Л. Палажченко**

Показники відновлення критичної інформаційної інфраструктури.....85

**Ф. Сафаров, Д. Олефір, Ю. Привалов, І. Блінов**

Запровадження елементів «Demand Response» для забезпечення надійної роботи енергосистеми України під час проходження осінньо-зимового періоду.....88

**А.В. Бойченко, В.Р. Сенченко**

Дослідження взаємозв'язків об'єктів критичної інфраструктури..90

**Н.В. Заїка, В.С. Ракович, М.Ю. Комаров**

Запобігання та захист об'єктів критичної інфраструктури від атак БПЛА.....92

**К.Ю. Коноваленко**

Ієрархії скорочення для прискорення обчислення найкоротшого шляху.....95

**С.М. Пістюльга**

Підвищення стійкості комп'ютерних мереж об'єктів критичної інфраструктури шляхом використання захищеного зв'язку.....97

**І.І. Бударов**

Огляд сучасних методів та інструментів для роботи із  
3D-моделями.....98

**С.П. Купрієнко, В.О. Артемчук**

Роль комп'ютерного зору для забезпечення живучості  
автоматизованих систем відеоспостереження в авіаційній  
індустрії.....101  
101

**Р.М. Гамрецький, В.О. Гнатюк**

Роль якості програмного забезпечення у резильєнтності  
інформаційно-комунікаційних систем.....104

**Є.О. Галич, В.Г. Павленко, А.В. Ільєнко**

Сучасний стан забезпечення кібербезпеки та стійкості об'єктів  
критичної інфраструктури України.....106

**С.Р. Соловей**

Застосування технології блокчейн для підвищення живучості  
систем бронювання авіаквитків.....110

**М.М. Ларін**

Калькулятор шкоди на основі даних о вразливостях  
інформаційного забезпечення підприємства.....113

**М. Рябих**

Інструменти захисту від XSS-вразливостей.....116

**П.І. Котирло, О.О. Висоцька**

Використання спаму як способу поширення пропаганди в  
соціальних мережах.....120

**В.В. Скоробагатько**

Резервне копіювання критичних даних корпоративних  
застосунків.....122

**К.Р. Бурлака**

Аналіз засобів розпізнавання кібератак.....125

**Ю.І. Кучеренко**

Аналіз сучасних досліджень у сфері захисту онлайн-повідомлень.....129

**Я.М. Власюк**

Ефективність розподіленої архітектури відеоспостереження в аеропортах.....131

**Г.В. Волошин**

Виявлення недозволених предметів на зображеннях за допомогою нейронних мереж.....134

**Н.В. Нощенко**

Система моніторингу користувачів веб-застосунків з використанням технології SSO за геометрією обличчя.....138

**О.О. Білий**

Проблематика методів класифікації деструктивних даних.....142

**Д.В. Безгубенко**

Здійснення кібератаки на комп'ютерну мережу.....144

**А.М. Давиденко**

Резильєнтність операторів програмного забезпечення для функціонування критичної інфраструктури.....147

**С.Я. Гільгурт**

НРС та реконфігуровні засоби підвищення резильєнтності кіберфізичних систем .....149

A. Yevdina, Y. Yevdin, S. Schantz

## **ENSURING THE SURVIVABILITY AND RESILIENCE OF THE DECISION SUPPORT SYSTEM RODOS AT THE FEDERAL OFFICE FOR RADIATION PROTECTION**

The decision support system RODOS (Realtime Online Decision Support System) calculates future environmental contamination and expected doses for people affected by a radiation emergency. RODOS is part of the Integrated Measurement and Information System (IMIS) of the Federal Office for Radiation Protection (BfS) and is in operational use.

In emergency situations, it is important to provide rapid and clear forecasts of the radiological situation. These forecasts form the basis for radiological situation reports, which provide the competent authorities with justified recommendations for specific emergency measures, such as the evacuation of the population.

The RODOS calculations are based on the weather forecasts of the German Meteorological Service (Deutscher Wetterdienst, DWD) and on information on the composition and quantity of radioactive releases (sourceterm), which in case of an emergency are transmitted to the BfS by the operator of the affected nuclear power plant in Germany or abroad and by the remote monitoring of nuclear power plants (Kernreaktor-Fernüberwachung, KFÜ).

To ensure the reliability of this system, there are several ways to obtain the weather forecast and the meteorological and radiological measurements. The weather forecast is automatically updated every 3-6 hours (depending on the calculation domain), covers 72 hours and is stored for approximately one month. It is therefore possible to use previous weather forecasts in the event of a temporary loss of communication with the meteorological service.

In addition, automatic calculations are made for shutdown and operating nuclear power plants in Germany and neighbouring countries to provide an immediate initial assessment of potentially affected areas in case of an emergency. These forecasts are up to date within 48 hours and can be used independently of the availability of the RODOS system.

To ensure resilient operation of the decision support system, the Federal Office for Radiation Protection in Munich has two physical servers dedicated to RODOS, one as the main server and used as a production environment, and the other for development and testing. The data required for the calculations are stored independently or duplicated. If the main server fails, the second server can be used as a production server.

In order to maintain the survivability of the RODOS system, a backup IMIS system has been installed at another BfS site in Freiburg (and in the future also in Berlin). The main processes of loading, storing data, performing RODOS calculations, processing results and generating radiological situation reports have been installed



there and duplicate the processes of the main system. The backup system can be used if the system at the main site (in Munich) is not available for certain reasons (e.g. blackout).

This multi-level support for survivability and resilience ensures the stable operation of the RODOS system.

## **АНАЛІЗ ЮРИДИЧНОГО СТАТУСУ СМАРТ-КОНТРАКТІВ ТА ПРОБЛЕМ, ЯКІ ВИНИКАЮТЬ ПРИ УЗГОДЖЕННІ ЇХ З ЗАКОНОДАВСТВОМ УКРАЇНИ**

Розвиток цифрових технологій суттєво змінює принципи та інструменти, на яких базується функціонування фінансових ринків розвинутих країн. Однією з проривних технологій, яка зумовила напрямки подальших змін у багатьох галузях, стала блокчейн-технологія.

Саме завдяки виникненню і швидкому розвитку блокчейн-платформ виник новий тип договорів – так звані смарт-контракти, тобто «розумні угоди». Смарт-контракт – це формальна угода, яка створена у вигляді комп'ютерного коду і може бути укладена, змінена або припинена лише за допомогою конкретної комп'ютерної програми. Така угода виконується автоматично та безперервно, і не потребує участі третьої довіреної сторони. Вона також може функціонувати в умовах повної недовіри між сторонами.

Актуальність роботи зумовлена як стрімким поширенням використання смарт-контрактів у різних галузях, так і їх спроможністю вирішити широкий спектр нагальних питань (ведення державних реєстрів, захист від рейдерства, спрощення р2р-продажу електроенергії між домогосподарствами, тощо), за умови визначення їх юридичного статусу.

Смарт-контракти на блокчейн-платформі для операцій в електроенергетиці, на відміну від традиційних контрактів, мають кілька вагомих переваг:

1. Швидкі розрахунки, проводяться негайно після факту споживання електроенергії.
2. Зручний вибір параметрів тарифікації та управління трафіком.
3. Відсутність проблем з боржниками завдяки автоматизованій системі розрахунків.
4. Відмова від посередників, що призводить до зниження ціни на електроенергію на 5-10%.

Ці смарт-контракти ініціюються однією із сторін (споживачем, мережею або генеруючою компанією) і укладаються після узгодження всіх деталей.

Можна навести такі потенційні очікування від впровадження смарт-контрактів в енергетиці:

- зменшення витрат завдяки відмові від посередників;
- збільшення гнучкості у виборі тарифу та системи оплати;
- посилення ролі звичайних споживачів у плануванні обсягів споживання;
- можливість безпосередньо закуповувати електроенергію від виробників;
- захист учасників від недобросовісних маніпуляцій з показниками обліку;
- захист мережевих та генеруючих компаній від ризику банкрутства компаній-постачальників;
- захист споживачів від недостовірної інформації щодо відключень.

Концепція смарт-контрактів з першими належними згадками виникла у 1994 році, коли криптограф та правовий експерт Нік Сабо висловив думку, що застосовуючи електронний децентралізований реєстр, можна створювати контракти, які виконуються автоматично. Але на практиці ця ідея була повноцінно реалізована лише у 2008 році завдяки появі технології блокчейн. Зараз використання смарт-контрактів набуває суттєвого практичного значення. Особливо вважаємо за потрібне виділити такі сфери їх застосування як ведення каскадних державних реєстрів [1-2] та укладання різних угод щодо продажу «зеленої» електроенергії [3]. Але при цьому на шляху їх використання виникає багато юридичних питань і проблем. Деякі з них є реальними, і пов'язані в основному з тим, що смарт-контракти є досить новим інструментом, який ще не знайшов відображення у законодавствах переважної більшості країн. Деякі інші проблеми можна вважати більш надуманими, ніж реальними, вони пояснюються настороженим ставленням більшості людей до нових технологій, які є досить складними для розуміння звичайного громадянина, що не є спеціалістом у відповідній галузі.

З юридичної точки зору, смарт-контракт представляє собою цифрову ітерацію цивільно-правової угоди, виражену у вигляді програмного коду, що автоматично виконується в розподіленій мережі. За принципом, схожим на традиційний цивільно-правовий договір, смарт-контракт складається зі сторін, предмету договору та ключових умов. Законна діяльність смарт-контракту визначається його здатністю відповідати основним вимогам цивільно-правового договору, включаючи наміри сторін в установленні юридичних відносин, ясність умов контракту та забезпечення можливості примусового виконання. Важливими ризиками, пов'язаними з смарт-контрактами, є невизначеність щодо їх юридичного статусу, а також криптовалюти як засобу оплати, складність вираження умов контракту у математичному алгоритмі, потенційна помилка у програмному коді та загроза хакерських атак [4]. Щоб вирішити ці проблеми та забезпечити адекватне юридичне регулювання смарт-контрактів в Україні, необхідно внести зміни до законодавства, які визнають криптовалюту як засіб платежу та встановлюють смарт-контракти як форму цивільно-правової угоди. Необхідно забезпечити, щоб сторони договору були чітко ідентифіковані і підтвердили свою згоду з умовами договору, використовуючи цифровий електронний підпис. Крім того, смарт-контракт повинен супроводжуватися обов'язковим текстовим додатком, в якому будуть викладені ключові положення договору, які матимуть юридичну силу в разі судової суперечки. Окрім цього, важливим кроком є перехід державних реєстрів на технологію блокчейн з закріпленням юридичної можливості автоматичного внесення змін до реєстрів при виконанні смарт-контракту.

Аналізуючи юридичний статус смарт-контрактів у світі, можна зробити висновок, що найбільш розвинене правове регулювання смарт-контрактів у США. «Хоч розумні контракти можуть звучати по-новому, сама їхня концепція коріниться у базовому договірному праві. Зазвичай суд виносить рішення щодо

договірних суперечкам і забезпечує дотримання умов, але часто зустрічається й інший метод, особливо для міжнародних транзакцій. За допомогою розумних контрактів комп'ютерна програма забезпечує виконання контракту, вбудованого в код» (Звіт Комітету з економіки Сенату США, 2018).

Підсумовуючи проаналізовані дані, доцільно доповнити ЦК України статтею 636-1 «Смарт-договір» з таким змістом:

1. Смарт-договір – це угода, яка укладається у формі електронного документа та набуває чинності після компіляції програмного коду та його розміщення в Ethereum або іншій системі з використанням технології блокчейну.

2. Ідентифікація сторін у смарт-договорі вважається еквівалентною використанню цифрових підписів в системі.

3. Для укладення смарт-договору застосовуються загальноприйняті протоколи, і умови повинні бути конкретними, виконуваними та законними.

4. Якщо програмний код реалізує умови, що не відповідають змісту електронного документа, смарт-договір може бути визнаний недійсним.

5. Виконання зобов'язань, передбачених смарт-договором, автоматично відбувається шляхом виконання цифрових передач у визначеній послідовності при настанні зазначених в договорі обставин.

6. Криптовалюта є законним засобом оплати при виконанні смарт-договорів.

1. Кондратенко М.С. (2023). "Використання технології блокчейну для побудови ієрархічної структури на множині державних реєстрів з метою захисту від підробки інформації". Електронне моделювання, 3(23), 43–56. <https://www.emodel.org.ua/images/em/45-3/45-3-4.pdf>
2. Кондратенко М.С. (2023). Визначення кількості блоків підтвердження у блокчейні, в якому розміщено реєстр другого рівня у випадку, коли в обох блокчейнах використовується протокол консенсусу POS. XLI Науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Збірник матеріалів конференції, 188–190. <https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf>
3. Зелений тариф. (2023). Вікіпедія. Вільна енциклопедія. [https://uk.wikipedia.org/wiki/Зелений\\_тариф](https://uk.wikipedia.org/wiki/Зелений_тариф).
4. Смарт контракт: розумний код рулить. (2020). Na chasi. Crypto. <https://nachasi.com/crypto/2020/12/08/smart-kontrakt>.

## ВИЗНАЧЕННЯ КІБЕРСТІЙКОСТІ В НОРМАТИВНО-ПРАВОВОМУ ПОЛІ ЄВРОПЕЙСЬКОГО СОЮЗУ І УКРАЇНИ ТА ЗАСТОСУВАННЯ ЙОГО ДО ІКТ ПІД ВПЛИВОМ ЕНЕРГЕТИЧНИХ ЗАГРОЗ

На сьогодні добре відомі поняття кіберстійкості (cyber resilience) [1] та цифрової стійкості (digital resilience) [2]. Є різні підходи до тлумачення різниці між ними. Аналіз джерел дозволяє зробити висновок, що обидва мають відношення до управління безперервністю бізнес-процесу (business continuity management, або BCM). Втім, сфера застосування поняття cyber resilience ставить в середину концепції стійкості та відновлюваності інфокомунікаційних систем до кібератак, в той час як digital resilience – це більше про властивості та поведінку окремого індивіда, групи чи спільноти під впливом тих самих кіберзагроз [3].

Загальновідомо що кібербезпека тісно пов'язана із захистом інформації [4]. Однак в захисті інформації *поняття стійкості вже визначене в нормативних документах з технічного захисту інформації*, а саме [5]. «Стійкість до відмов» визначена як один з критеріїв доступності, що гарантує можливість використання інформації, окремих функцій або комп'ютерної системи в цілому після відмови її компонента. Рівні даної послуги ранжуються на підставі спроможності комплексу засобів захисту забезпечити можливість функціонування системи в залежності від кількості відмов, а також кількості послуг, доступних після відмови. Як бачимо, в цьому визначені *не йдеться про здатність до відновлення*. Це змушує відокремити поняття стійкості та резильєнтності по відношенню до захисту інформації.

В той же час, в Україні існує національна система стійкості (надалі – НСС) [6], призначена для забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національної безпеки, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, зокрема гібридних. Як бачимо, тут стійкість чітко асоційовано з процесом відновлення.

Впроваджувана НСС має забезпечити, зокрема, безпеку та захищеність об'єктів критичної інфраструктури, до яких в НСС віднесено в тому числі кібербезпеку; захищеність та безперебійне функціонування інформаційних та комунікаційних послуг. Таке розширення поняття критичної інфраструктури, попри свою узагальненість, співпадає з напрямками світового розвитку світових практик. Так, 16 січня 2023 року набула чинності Директива (ЄС) 2022/2555, відома як NIS2 [7]. Вона замінила Директиву (ЄС) 2016/1148, відому як просто NIS. Однією з головних відмінностей Директиви NIS2 у порівнянні з попередньою, відомою як просто NIS, є підвищення спільного рівня

кібербезпеки в усьому Союзі для подальшого покращення резильєнтності та можливостей реагування на інциденти як державного, так і приватного секторів та ЄС загалом. Переглянута директива спрямована на гармонізацію вимог кібербезпеки та впровадження заходів кібербезпеки в різних державах-членах. Щоб досягти цього, встановлюються мінімальні правила для нормативної бази та встановлює механізми для ефективної співпраці між відповідними органами в кожній державі-члені. Він оновлює перелік секторів і видів діяльності, на які поширюються зобов'язання щодо кібербезпеки, і передбачає засоби правового захисту та санкції для забезпечення виконання.

З цифрової резильєнтності додатково ще виокремлюють поняття *цифрової операційної резильєнтності* (digital operations resilience), описаної в положенні про цифрову операційну резильєнтність фінансового сектору (DORA) [8]. Цифрова операційна резильєнтність фокусується на спроможності ІКТ-ресурсів організації забезпечити BCM у випадку кризових подій. Директиву NIS2 було узгоджено з галузевим законодавством, зокрема з DORA і директивою щодо стійкості критично важливих організацій (critical entities resilience – CER). Механізм добровільного партнерського навчання (peer-learning) підвищить взаємну довіру та вивчення передових практик і досвіду в ЄС, тим самим сприяючи досягненню високого загального рівня кібербезпеки.

NIS2 починає діяти в жовтні 2023 року. Очікується також початок дії Закону про кіберстійкість (CRA) [9], який встановлює вимоги до кібербезпеки для ряду апаратних і програмних продуктів, що надходять на ринок ЄС, включаючи розумні колонки, ігри, операційні системи тощо. CRA, ймовірно, буде погоджено інституціями ЄС у 2024 році з зобов'язання почнуть застосовуватися в 2025 або 2026 роках.

З метою підвищення кіберстійкості CRA спрямований на такі задачі:

- забезпечити, щоб виробники покращували безпеку продуктів із цифровими елементами, починаючи з фази проектування та розробки та протягом усього життєвого циклу;
- забезпечити узгоджену структуру кібербезпеки, сприяючи відповідності для виробників обладнання та програмного забезпечення;
- підвищити прозорість властивостей безпеки продуктів із цифровими елементами;
- забезпечити можливість безпечного використання продуктів з цифровими елементами.

Для України чи не найголовнішим викликом з кіберстійкості є енергосистема – найважливіший компонент критичної інфраструктури держави, що зумовлює нормальне функціонування усіх галузей економіки та державних сервісів. Резильєнтність будь-якої інформаційно-комунікаційної системи (ІКС) напряму залежить від стабільної роботи енергосистеми держави. В той час, як найбільш імовірною загрозою резильєнтності конкретної ІКС під час моделювання загроз зазвичай вважається спорадичне відключення електропостачання на нетривалий термін з подальшим відновленням, загрози

військового характеру для енергосистеми держави несуть принципово інші ризики. Останні зумовлені систематичними вимкненнями електропостачання на об'єктах ІКС на відносно тривалій період, що супроводжуються коливаннями напруги в розподільчих мережах та можуть бути як передбачуваними (стабілізаційними), так і екстремними [10, 11].

Тривалі та систематичні відключення електропостачання на об'єктах ІКС зумовлюють ряд специфічних загроз для кіберстійкості системи та зокрема її кібербезпеки:

- припинення функціонування всієї системи, або окремих її частин на період що дорівнює або перевищує тривалість відключення;
- вихід з ладу обладнання ІКС внаслідок перепадів напруги, що спричиняє прямі збитки та відмову в обслуговуванні на тривалій період;
- неможливість своєчасного та гарантованого моніторингу стану розподіленої системи або окремих її компонентів;
- відключення засобів безпеки, що забезпечують захист компонентів системи, що продовжують функціонування;
- погіршення спостережності інфраструктури внаслідок необхідності моніторингу стану енергоживлення окремих компонентів системи;
- перевантаження команд SOC, NOC та CSIRT необхідністю розслідування недоступності компонентів, що зумовлені відключенням електроживлення;
- перебої у функціонуванні окремих компонентів системи внаслідок помилок десинхронізації.

Модель кризового реагування для забезпечення стійкості цільової функції, відповідно до [12], передбачає наступні фази стійкості:

- готовність та запобігання;
- реагування;
- відновлення (повернення до штатного функціонування).

Існуючі на даний момент підходи до усунення ризиків *на етапі готовності та запобігання*, пов'язаних з відключенням електропостачання на об'єктах ІКС виявляються ефективними під час нетривалих проблем в енергосистемі, але володіють рядом проблем при застосуванні під час глобальних кризових ситуацій. Короткий порівняльний аналіз наведено в [13].

Враховуючи викладені міркування, можемо дійти наступних висновків щодо впливу систематичних відключень електроживлення на кіберстійкість сучасних ІКС:

- основні ризики пов'язані з безпосередньою відмовою в обслуговуванні внаслідок відсутності електроживлення, однак ряд ризиків впливають напряму на кібербезпеку внаслідок дії ефектів другого порядку;
- існуючі підходи до усунення ризиків відключення електропостачання є ефективними лише частково по відношенню до систематичних та довготривалих відключення електропостачання;

Для точного визначення потенційного впливу руйнування енергосистеми на кіберстійкість конкретної інфраструктури як частини її резильєнтності, необхідне проведення моделювання загроз з залученням експертної оцінки архітектури системи.

Для усунення основних ризиків, пов'язаних з масовими відключеннями електропостачання та відповідного підвищення кіберстійкості необхідне застосування комбінації існуючих методів протидії загрозам такого типу у комбінації з істотним розширенням покриття інфраструктури моніторингом та специфічними контролями безпеки, а також зміна підходу до розслідування інцидентів відмови в обслуговуванні.

1. Linkov, I., Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. <https://doi.org/10.1007/978-3-319-77492-3>.
2. Cuel, R., Ponte, D., & Virili, F. (2022). Exploring digital resilience: Challenges for people and organizations. Springer Nature.
3. UK Council on Internet Safety. Digital Resilience Framework : станом на 18.09.2020. URL : <https://www.gov.uk/government/publications/digital-resilience-framework>.
4. МОН пропонує до громадського обговорення проєкт стандарту вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» на третьому (освітньо-науковому) рівні вищої освіти. URL: <https://t.ly/F3TSb> (дата доступу : 29.09.2023).
5. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999 із змінами згідно наказу Адміністрації Держспецв'язку від 28.12.2012 № 806. – 60 с.
6. Концепції забезпечення національної системи стійкості. Затверджено Указом Президента України від 27 вересня 2021 року № 479/2021. URL : <https://zakon.rada.gov.ua/laws/show/479/2021/> (дата доступу : 29.09.2023).
7. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
9. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454> (дата доступу: 20.09.2023).
10. Зубок В. Ефективність використання заходів з підвищення цифрової стійкості підчас тривалих відключень електропостачання. *Електронне моделювання*. 2023. Т. 45, № 1. С. 98-112. – <https://doi.org/10.15407/emodel.45.10.098>.
11. What happens during a blackout / T. Petermann et al. Norderstedt : BoD – Books on Demand, 2011.



12. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX : станом на 5 груд. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 02.10.2023).
13. Драгунцов Р., Зубок В. Моделювання загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання та потенційні заходи протидії. Електронне моделювання. 2023. Т. 45, № 3. С. 116–128. <https://doi.org/10.15407/emodel.45.03.116>.

## **ЖИВУЧЕСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ КРИТИЧНИХ ІНФРАСТРУКТУР**

Критична інфраструктура (англ. critical infrastructure) об'єднує системи і об'єкти, які відіграють незамінну роль у підтримці життєдіяльності людей, функціонуванні суспільства та розвитку країн. Такі інфраструктури включають енергетичні мережі, транспортні системи, телекомунікаційні мережі, банківські системи, водопостачання і водовідведення, системи теплопостачання тощо.

Критичні інфраструктури мають зберігати свою функціональність, стійкість та відновлюваність після аварій та надзвичайних ситуацій, таких як природні катастрофи, терористичні акти, кібератаки або технічні збої. Така властивість інфраструктур визначається терміном резильєнтність (англ. resilience). Поява цього терміну пов'язана, на наш погляд, із зростанням ризиків безпеки критичних інфраструктур, динамічністю ландшафту загроз, зростаючою взаємозалежністю більшості секторів людської діяльності і критичних інфраструктур, усвідомленням катастрофічних наслідків у разі виникнення і розвитку каскадних аварій, які можуть призвести до далекосяжних і довгострокових негативних впливів на життєдіяльність людини, суспільства, країни [1].

Резильєнтність критичної інфраструктури необхідна для безпеки та сталого розвитку в умовах загроз і небезпек, що існують в сучасному світі. Це важлива і бажана характеристика інфраструктури, що дозволяє розуміти здатність інфраструктури адаптуватися до агресивних умов функціонування, швидко відновлюватися після збоїв та мінімізувати негативний вплив на життєво важливі суспільні функції, економічну діяльність, громадське здоров'я та безпеку або навколишнє середовище.

Глобалізація привела до виникнення транскордонної та взаємозалежної мережі надання життєво важливих послуг з використанням ключових об'єктів критичних інфраструктур різних країн, і це ще більш ускладнило і посилило вимоги та заходи щодо резильєнтності критичних інфраструктур. Виникла необхідність забезпечувати скоординований захист, контекстуальну обізнаність, єдність методологій та розробку і впровадження дієвих механізмів адаптивного реагування на інциденти. В [1] запропоновано створення відповідних організаційних структур, зокрема для забезпечення ефективної оперативної співпраці між країнами, створення єдиної структурованої платформи реагування на інциденти (Cybersecurity Crisis Response Framework), що переросли у кризи та мають транскордонний характер. Передбачається багатоетапний підхід до повідомлення про значні інциденти, визначається термін, протягом якого організації різних країн повинні надавати попередження (24 години) і повідомлення (72 години) про серйозний інцидент, що стався в інфраструктурі країни.

Інформаційні системи сьогодні є у складі будь-якої критичної інфраструктури. Ці системи являють собою сукупність програмних, апаратних та організаційних засобів, які реалізують збір, обробку, зберігання та передачу інформації для забезпечення функціонування та розвитку інфраструктур. Інформаційні системи відіграють важливу роль у забезпеченні безпеки та ефективності функціонування критичних інфраструктур. Засоби цих систем сприяють швидкому виявленню інцидентів в критичних інфраструктурах, інформуванню про них і адекватному управлінню при відновленні функціонування інфраструктури після інцидентів (надзвичайних ситуацій). Відповідно резильєнтність критичних інфраструктур залежить від властивостей інформаційних систем, що входять до їх складу.

Зазвичай, інформаційні системи критичних інфраструктур включають наступні компоненти:

- *системи моніторингу*, які забезпечують постійний контроль за станом інфраструктурних об'єктів завдяки датчикам виявлення збоїв, витоків, перевантажень та інших аномалій;
- *системи збору та обробки даних*, що здійснюють збір інформації з різних джерел, таких як об'єктні датчики, системи контролю доступу, датчики відеоспостереження, проводять аналіз отриманої інформації для виявлення незвичних подій і загроз;
- *комунікаційні системи*, які забезпечують передачу інформації між різними компонентами системи, а також зв'язок з управлінськими центрами та операторами критичних інфраструктур;
- *системи управління*, що забезпечують управління та координацію реагування на надзвичайні ситуації, включаючи прийняття рішень, розподіл ресурсів та організацію відновлення функціонування;
- *системи резервного копіювання та відновлення*, які забезпечують збереження резервних копій даних та можливість їх відновлення у разі аварій чи кібератак;
- *системи безпеки та захисту інформації* із відповідними механізмами і технологіями захисту інформації від несанкціонованого доступу, кібератак і витоків даних;
- *аналітичні системи*, застосовуються для проведення аналізу ризиків, прогнозування потенційних загроз і виявлення уразливостей в критичних інфраструктурах.

Гарантовано довіряти послугам інформаційних систем можна лише за наявності у неї функціональної стійкості – властивості, що характеризує здатність системи зберігати (автоматично відновлювати) виконання повного або прийняттого набору функцій в умовах деструктивних впливів.

Функціональна стійкість інформаційної системи передбачає наявність у системи певного рівня надійності, відмовостійкості, адаптивності, живучості, що дозволяє їй зберігати і/або відновлювати виконання функцій в умовах різного роду збурюючих впливів, мінімізуючи ризики переходу системи в

аварійний (небезпечний) стан [2]. Інформаційні системи, які розробляються на засадах теорії живучості, мають не лише системи захисту від відомих загроз, але й вбудовані механізми підтримки живучості, що передбачають наявність елементів аналізу і прогнозування ризиків, створення певних базових рішень-шаблонів за принципом «клас ситуацій – дія», можливість безпечного припинення функціонування тощо. Такі системи у складі критичних інфраструктур сприятимуть підвищенню резильєнтності інфраструктури.

Вимоги до резильєнтності критичних інфраструктур потребують перманентного проведення заходів з аналізу й оцінювання ризиків, включаючи й малоймовірні, а також напрацювання заходів з протидії загрозам, реалізація яких може призвести до інцидентів із катастрофічними наслідками. Вже сьогодні, враховуючи глобальний характер загроз і масштабність інформаційних інфраструктур, пропонується використовувати програмне забезпечення з відкритим вихідним кодом, застосовувати відкриті стандарти, відкриті дані для забезпечення безпеки і зниження ризиків завдяки прозорості, впроваджувати активний розширений кіберзахист, сприяти створенню міжнародної бази кібервразливостей та заходів щодо їх своєчасної ліквідації і зменшення впливу на роботу систем. Таким чином, введення терміну «резильєнтність» приводить до необхідності певного розширення спектру задач, які покладаються на інформаційні системи критичних інфраструктур, як методологічного, так і практичного характеру: вибудови певної таксономії характеристик в галузі інформаційних систем, що є складовими критичних інфраструктур, розвитку ризик-орієнтованого підходу в частині напрацювання моделей для аналізу малоймовірних подій, що можуть призвести до інцидентів із катастрофічними наслідками, напрацювання конкретних механізмів, спрямованих на підтримку парадигми резильєнтності.

1. Директива (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року щодо стійкості критичних об'єктів та скасування Директиви Ради 2008/114/ЄС. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32022L2557&qid=1686557595058>.
2. Dodonov O., Gorbachyk O., Kuznietsova M. Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability. *CEUR Workshop Proceedings 2021, 3241*, pp.1-12. <http://ceur-ws.org/Vol-3241/paper1.pdf>.

## **ВПРОВАДЖЕННЯ ПАРАДИГМИ РЕЗИЛЬЄНТНОСТІ У ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ**

Резильєнтність та резистентність критичної інфраструктури (КІ) є важливими поняттями, особливо в умовах зростаючих загроз кібербезпеки та виникнення надзвичайних ситуації техногенного, природного і воєнного характеру, котрі можуть спричинити порушення звичного функціонування об'єктів. Для забезпечення стійкості та безпеки суспільства важливо розуміти ці поняття і приймати необхідні заходи для забезпечення їх реалізації.

Резистентність КІ означає її здатність протидіяти зовнішнім факторам впливу та забезпечувати необхідні послуги навіть після виникнення непередбачуваних подій або кризових ситуацій. Для підвищення резистентності інфраструктури можуть бути використані наступні підходи:

1. Диверсифікація: розташування інфраструктурних об'єктів у різних місцях для зменшення ризику впливу подій на велику площу одночасно.

2. Запаси та резерви: забезпечення наявності резервних запасів матеріалів, обладнання та ресурсів для відновлення роботи після аварій.

3. Технологічні інновації: використання новітніх технологій, які дозволяють швидко відновити функціонування після виникнення непередбачуваних ситуацій.

4. Захист від кіберзагроз: забезпечення цифрової безпеки об'єктів критичної інфраструктури від кібератак та інших загроз інформаційним системам.

Резильєнтність критичної інфраструктури відображає її здатність адаптуватися до змін і відновлюватися після виникнення кризових ситуацій. Впровадження парадигми резильєнтності у забезпеченні функціонування критичної інфраструктури України є важливим завданням для національної економічної безпеки і стійкості в умовах зростаючих загроз і ризиків.

Для підвищення резильєнтності варто вживати наступні заходи:

1. Попередження: системи попередження та реагування на ризики і загрози, які дозволяють завчасно виявляти небезпеку та приймати заходи для зменшення її впливу.

2. Адаптація: здатність інфраструктури адаптуватися до нових умов та змінювати свою структуру, функції та процеси відповідно до потреб ситуації.

3. Планування в разі кризи: розробка планів дій для відновлення роботи інфраструктури після аварій та кризових ситуацій.

4. Співпраця зі структурами управління кризовими ситуаціями, органами влади та іншими зацікавленими сторонами для ефективного відновлення інфраструктури.

5. Оцінка ризиків і вразливостей: проведення комплексної оцінки ризиків і уразливостей критичної інфраструктури, що дозволить визначити потенційні загрози та точки вразливості, на які потрібно звернути особливу увагу.

6. Розробка резильєнтних планів та стратегій для підвищення резильєнтності КІ, котрі повинні включати антикризові заходи для попередження, реагування та відновлення.

7. Інфраструктурні вдосконалення: здійснення необхідних інвестицій для підвищення технічного стану та надійності критичних об'єктів інфраструктури, а також впровадження новітніх технологій для забезпечення швидкого відновлення після аварій.

8. Комунікація та співпраця: розвиток механізмів співпраці між різними секторами, урядовими органами, владними структурами, громадськістю та приватним сектором для координації дій у разі кризових ситуацій.

9. Постійне підвищення кваліфікації та навиків: проведення регулярних тренувань і симуляцій з персоналом для підвищення їх готовності до дій у надзвичайних ситуаціях.

10. Цифрова безпека: забезпечення захисту критичної інфраструктури від кіберзагроз шляхом впровадження сучасних кібербезпекових заходів та механізмів потребує передбачити здійснення додаткових витрат на їх реалізацію.

11. Локальна самодостатність: розвиток механізмів та резервних ресурсів для забезпечення функціонування критичної інфраструктури в територіальних громадах в разі виникнення кризових ситуацій.

12. Постійне вдосконалення: впровадження циклу постійного вдосконалення, включаючи аналіз після-інцидентних ситуацій та вдосконалення планів на основі набутих знань.

Загальний підхід має бути цілеспрямованим на створення більш стійкої, адаптивної та відповідальної системи управління КІ, котра здатна ефективно функціонувати навіть в умовах надзвичайних ситуацій.

Загалом, забезпечення резистентності та резильєнтності критичної інфраструктури вимагає комплексного підходу, включаючи технічні, технологічні та організаційні заходи, а також управління ризиками.

Пропозиції до проекту Національної стратегії  
підвищення резильєнтності критичної інфраструктури

- оцінка ризиків і ідентифікація вразливостей: провести комплексну оцінку ризиків для кожного сектору критичної інфраструктури, визначити основні загрози та вразливості. Це дозволить зосередитися на найбільш значущих аспектах і розробити прийнятні заходи для запобігання і мінімізації наслідків можливих подій;
- забезпечення кібербезпеки: розробити та впровадити комплексні заходи щодо захисту критичної інфраструктури від кіберзагроз. Це може включати встановлення механізмів виявлення, запобігання та реагування на кібератаки, забезпечення надійних систем захисту, підвищення кваліфікації персоналу та співпрацю з приватним сектором щодо обміну інформацією;
- резервування та альтернативні маршрути: розробити плани резервування для критичної інфраструктури, що передбачають наявність альтернативних маршрутів, джерел постачання енергії та інших необхідних ресурсів. Це дозволить забезпечити продовження надання послуг навіть у разі аварій, технічних проблем чи небезпеки для об'єкта;
- підвищення свідомості та навчання: Здійснювати систематичні кампанії зі свідомого ставлення до стійкості критичної інфраструктури серед населення та працівників. Проводити навчання та тренування персоналу для реагування на надзвичайні ситуації, включаючи планування евакуації, надання першої допомоги та відновлення роботи після інциденту.
- співпраця та обмін інформацією: забезпечити ефективний механізм співпраці та обміну інформацією між всіма зацікавленими сторонами, включаючи державні органи, операторів критичної інфраструктури та інші відповідні суб'єкти. Це допоможе вчасно виявляти загрози, координувати дії під час кризових ситуацій та швидко реагувати на випадки порушень безпеки.
- використання новітніх технологій: застосування інноваційних технологій, таких як штучний інтелект, блокчейн, для покращення стійкості критичної інфраструктури, зокрема використання сенсорів та моніторингових систем для раннього виявлення проблем, прогнозування потенційних ризиків;
- фінансування та інвестиції: забезпечити необхідне фінансування та інвестиції для впровадження заходів з підвищення стійкості КІ. Це може включати державні фонди, публічно-приватні партнерства та стимулювання інвестицій приватного сектору у сферу безпеки та резильєнтності;
- міжнародне співробітництво: розглянути можливості підвищення співробітництва з міжнародними організаціями та іншими країнами з метою обміну досвідом та впровадження найкращих практик у галузі резильєнтності критичної інфраструктури. Спільні проекти, обмін експертами та координація дій сприятимуть зміцненню стійкості не лише на національному, а й на міжнародному рівні.

Рисунок 1 – Пропозиції до проекту Національної стратегії підвищення резильєнтності критичної інфраструктури

Підвищення рівня резильєнтності та резистентності української та європейської критичної інфраструктури є одним із магістральних пріоритетів безпекової політики країн Європейського Союзу, що відповідно закріплено в рішеннях Ради ЄС, котрі спрямовані на посилення заходів щодо підвищення стійкості та резильєнтності КІ [1]. У грудні 2022 року Рада ЄС прийняла Рекомендації, які стосуються скоординованого підходу щодо забезпечення стійкості КІ. Особливо рекомендовано запровадити необхідні інструменти та забезпечити координацію на рівні ЄС з метою підвищення готовності та реагування на безпекові інциденти, що можуть призвести до порушення надання життєво важливих послуг на внутрішньому ринку Євросоюзу. Також Рада ЄС ухвалила нову Директиву щодо стійкості критичних об'єктів у цей самий час. На початку 2023 р. було оголошено про синергію зусиль ЄС і НАТО щодо забезпечення стійкості критичної інфраструктури.

Україна на законодавчому рівні приділила увагу розвитку політики в сфері КІ. Деякі положення нової Директиви ЄС відповідають нормам Закону України «Про критичну інфраструктуру». Імплементация положень Закону, що відповідають Директиві ЄС, свідчить про те, що суб'єкти національної системи КІ намагаються зосередитися на встановленні вимог щодо фізичної безпеки цих об'єктів та контролі за діяльністю операторів КІ. Незважаючи на наявність законодавчих положень, розвиток механізмів для забезпечення стійкості надання послуг, стимулювання та підтримки операторів КІ, аналізу ризиків, обміну інформацією та координації діяльності у форматі державно-приватного партнерства є необхідними для повного комплаєнсу пріоритетам політики ЄС в цій сфері. З урахуванням цього, рекомендується, щоб Кабінет міністрів України та уповноважений орган у сфері КІ розглянули питання щодо розроблення проекту Національної стратегії підвищення стійкості критичної інфраструктури [2]. Пропозиції до проекту Національної стратегії підвищення резильєнтності критичної інфраструктури можуть включати аспекти, які відображені на рис. 1. Враховуючи ці пропозиції в Національній стратегії підвищення резильєнтності критичної інфраструктури, буде створено цілісний план заходів, спрямованих на забезпечення безпеки, ефективності та стабільності критичних об'єктів. Такий план сприятиме зменшенню ризиків, забезпеченню швидкого відновлення та надійності роботи інфраструктури, що є життєво важливим для суспільства та економіки.

1. Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR. en) 15623/22. <https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf>.
2. Нова директива ЄС щодо стійкості критичної інфраструктури (CER DIRECTIVE). <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/nova-dyrektyva-yes-shchodo-stiykosti-krytychnoyi-infrastruktury>.



## ПРОЦЕС УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ЯК СКЛАДОВА КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення кібербезпеки є важливим завданням, визначеним Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [1], Законом України «Про основні засади забезпечення кібербезпеки України» [2], Законом України «Про критичну інфраструктуру» [3]. Значну роль кібербезпеці відводиться і в Законі України «Про національну безпеку України» [4], що підтверджує залежність захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних кіберзагроз критичній інфраструктурі. Вирішення завдань з забезпечення кібербезпеки нерозривно пов'язано з забезпеченням стійкості.

Отже, проблема забезпечення кібербезпеки та кіберстійкості критичної інфраструктури є актуальною задачею, що потребує ефективних невідкладних рішень для забезпечення національної безпеки України.

Однією зі складових забезпечення кібербезпеки є процес управління вразливістю, що визначається NIST 800-40v3 Creating a Patch and Vulnerability Management Program [5].

Звісно, процес управління вразливістю включає в себе накопичення та оброблення великих наборів даних. Для уникнення невизначеностей в подальшому викладенні результатів даного дослідження з використанням теорії множин представимо математично ці набори даних.

Набір вразливостей ( $V$ ) представляє сукупність усіх відомих вразливостей. Кожна вразливість представлена як елемент у наборі  $V$ .

Набір систем ( $S$ ) представляє набір систем або активів, які підлягають оцінці вразливості та оцінці відповідності. Кожна система представлена як елемент множини  $S$ .

Набір політик ( $P$ ) представляє набір політик або правил безпеки, яким мають відповідати системи. Кожна політика представлена як елемент у наборі  $P$ .

Набір оцінки вразливості ( $A$ ) представляє результат оцінки вразливості, виконаної в системі. Кожна оцінка представлена як елемент у наборі  $A$ .

Набір оцінки відповідності ( $C$ ) представляє результат оцінки відповідності, виконаної в системі щодо певної політики. Кожна оцінка представлена як елемент у наборі  $C$ .

Визначимо зв'язки між цими наборами:

Набір вразливостей  $V$  – це набір вразливостей (1):

$$V = \{v1, v2, v3, \dots\} \quad (1)$$

Системний набір  $S$  – це набір систем (2):

$$S = \{s_1, s_2, s_3, \dots\} \quad (2)$$

Набір політик  $P$  – це набір політик (3):

$$P = \{p_1, p_2, p_3, \dots\} \quad (3)$$

Набір оцінки вразливості  $A$  – це набір оцінок вразливості (4):

$$A = \{a_1, a_2, a_3, \dots\} \quad (4)$$

де  $a_i$  – оцінка системи  $s_j$  проти вразливості  $v_k$ .

Набір  $C$  оцінки відповідності – це набір оцінок відповідності (5):

$$C = \{c_1, c_2, c_3, \dots\} \quad (5)$$

де  $c_i$  – оцінка системи  $s_j$  щодо політики  $p_k$ .

Такий підхід передбачає і використання операцій над множинами, таких як перетин, об'єднання, різниця, підмножина. Використовуючи ці набори та операції з наборами, стає можливим будувати математичні моделі для представлення зв'язків і взаємодій у управлінні вразливістю, наприклад, аналізування вразливості, оцінювання вразливості, оцінювання відповідності системи політиці, оцінювання відповідності набору систем набору політик.

З метою математично представлення зв'язків та взаємодії в управлінні вразливістю, ми можемо визначити наступні математичні моделі:

Модель аналізу вразливості

Розглянемо систему  $S$  і вразливість  $V$ . Можливо визначити функцію  $VA(S, V)$ , яка представляє аналіз уразливості системи  $S$  проти вразливості  $V$ . Результатом цієї функції може бути двійкове значення, яке вказує, чи присутня вразливість у системі. Наприклад,  $VA(S, V) = 1$ , якщо вразливість  $V$  присутня в системі  $S$ , і  $VA(S, V) = 0$  в іншому випадку.

Модель оцінки вразливості

Розглянемо набір систем  $S$  і набір вразливостей  $V$ . Ми можемо визначити функцію  $VAM(S, V)$ , яка представляє оцінку вразливості систем  $S$  проти вразливостей  $V$ . Цю функцію можна визначити як перетин уразливості функції аналізу для кожної системи та пари вразливостей. Математично ми можемо представити це як (6):

$$VAM(S, V) = \{(S, V) \mid VA(S, V) = 1\} \quad (6)$$

Результатом моделі оцінки вразливості  $VAM(S, V)$  є набір пар  $(S, V)$ , що вказує, які вразливості присутні в кожній системі.

### Модель відповідності системи політиці

Розглянемо систему  $S$  і політику  $P$ . Ми можемо визначити функцію  $PC(S, P)$ , яка представляє оцінку відповідності політики системи  $S$  щодо політики  $P$ . Результатом цієї функції може бути двійкове значення, яке вказує, чи система відповідає політиці чи ні. Наприклад,  $PC(S, P) = 1$ , якщо система  $S$  відповідає політиці  $P$ , і  $PC(S, P) = 0$  в іншому випадку.

### Модель оцінки відповідності набору систем набору політик

Розглянемо набір систем  $S$  і набір політик  $P$ . Ми можемо визначити функцію  $CEM(S, P)$ , яка представляє оцінку відповідності систем  $S$  політикам  $P$ . Цю функцію можна визначити як перетин функцій відповідності політик для кожної системи та пари політики. Математично ми можемо представити це як (7):

$$CEM(S, P) = \{(S, P) \mid PC(S, P) = 1\} \quad (7)$$

Результатом моделі оцінки відповідності  $CEM(S, P)$  є набір пар  $(S, P)$ , що вказує, які системи відповідають кожній політиці.

Ці математичні моделі дозволяють аналізувати вразливості, оцінювати відповідність політикам у структурований спосіб. Визначивши функції  $VA$ ,  $VAM$ ,  $PC$  і  $CEM$  можливо виконувати обчислення та отримувати корисні результати щодо стану безпеки систем і їх відповідності політикам.

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України № 447/2021 (2021) (Україна). <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
2. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2022) (Україна). <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
3. Про критичну інфраструктуру, Закон України № 1882-IX (2022) (Україна). <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
4. Про національну безпеку України, Закон України № 2469-VIII (2023) (Україна). <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
5. Souppaya M., & Scarfone K. (2013). *Guide to enterprise patch management technologies*. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-40r3>.

## **ЗАБЕЗПЕЧЕННЯ РАЦІОНАЛЬНОГО ПРИРОДОКОРИСТУВАННЯ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

У сучасній Україні сформована та реалізується нова державна екологічна політика, яка визначається Законом України "Про основні засади (Стратегію) державної екологічної політики на період до 2020 року", ухваленим 21 грудня 2010 р. [1]. Її метою визначено стабілізацію і поліпшення стану довкілля шляхом інтеграції екологічної політики до соціально-економічного розвитку України для гарантування екологічно безпечного природного середовища, запровадження екологічно збалансованої системи природокористування та збереження природних систем. Виконанню цієї мети мають сприяти державні органи та органи місцевого самоврядування. Стратегія містить 7 цілей національної екологічної політики, однією з яких є інтеграція екологічної політики та вдосконалення системи інтегрованого екологічного управління (ціль 4).

Вона передбачає, серед іншого, виконання таких завдань: розроблення та впровадження нормативно-правового забезпечення обов'язковості інтеграції екологічної політики до інших документів, що містять політичні та/або програмні засади державного, галузевого (секторального), регіонального та місцевого розвитку; інституційна розбудова і посилення ефективності державного управління в природоохоронній галузі; упровадження систем екологічного управління та підготовка державних цільових програм з екологізації окремих галузей національної економіки, що передбачають технічне переоснащення, запровадження енергоефективних і ресурсоощадних технологій, маловідходних, безвідходних та екологічно безпечних технологічних процесів.

Також, стратегія екологічно безпечного природокористування має передбачати формування та реалізацію механізму сприяння розвитку "зеленої" економіки в Україні в таких напрямках: економічне зростання має забезпечуватися при менш інтенсивному споживанні сировини та енергії в усіх секторах економіки за принципом "створювати більше вартості за меншого впливу на НПС"; державна політика стимулювання розвитку "зелених" видів діяльності, обмеження субсидій на підтримку забруднюючих довкілля виробництв, упровадження більш жорстких екологічних стандартів і відповідальності виробників і споживачів, продуманої системи державного регулювання та інвестицій; упровадження більш чистих технологій, які відкривають нові можливості зростання в "зелених" напрямках, компенсуючи втрату робочих місць у природоємних секторах.

На нашу думку, Стратегія державної екологічної політики має передбачати формування та реалізацію механізму сприяння розвитку "зеленої" економіки в Україні в таких напрямках: економічне зростання має забезпечуватися при менш

інтенсивному споживанні сировини та енергії в усіх секторах економіки за принципом "створювати більше вартості за меншого впливу"; державна політика стимулювання розвитку "зелених" видів діяльності, обмеження субсидій на підтримку забруднюючих доквілля виробництв, упровадження більш жорстких екологічних стандартів і відповідальності виробників і споживачів, продуманої системи державного регулювання та інвестицій; упровадження більш чистих технологій, які відкривають нові можливості зростання в "зелених" напрямках, компенсуючи втрату робочих місць у природоємних секторах; інвестування в підвищення енергоефективності, відновлювальну енергетику та управління відходами, що створює базу для розвитку підприємництва, інновацій та росту зайнятості населення на 20% до 2050 р. порівняно із звичайним сценарієм.

У контексті визначення концептуальних засад стратегії формування та реалізації державної екологічної політики в Україні доцільно визначити пріоритетними такі цілі: зміна моделей споживання в напрямку забезпечення збалансованого споживання та виробництва; забезпечення продовольчої безпеки та збалансованого сільського господарства; безпечна і доступна вода; підтримка динамічної стабільності клімату; упровадження чистої "зеленої" енергетики; збереження біорізноманіття; забезпечення функціонування здорових лісів; підтримка здоров'я населення та доступ до базового рівня медичних послуг; створення умов для економічної, екологічної і соціальної збалансованості міст [2].

Необхідно наголосити, що застосування досвіду країн ЄС та інших країн світу, що розкрито в Доповіді про глобальний зелений новий курс [2] дозволило визначити основні стратегічні напрямки екологічно безпечного природокористування: підвищення енергоефективності будівель, стійку енергетику, стійкий транспорт, стале сільське господарство, поліпшення запасів і якості води, розвиток екологічної інфраструктури, ефективне використання матеріалів та інвестування в утилізацію відходів.

Якщо оцінювати існуючий екологічний механізм природокористування за критерієм екологічної доцільності й поліпшення якості довкілля, то доведеться констатувати його неефективність щодо розв'язання проблеми не екологічно безпечного природокористування та неспроможність забезпечити екологічно сприятливі умови господарювання чи бути засобом до переходу до екологічно безпечного розвитку економіки країни. Аналіз організаційно-економічних інструментів екологічно безпечного регулювання показує, що і адміністративно-організаційні, і економічні методи мають як сильні, так і слабкі сторони. Тому при формуванні організаційно-економічного механізму управління охороною НПС необхідно знайти оптимальну структуру поєднання адміністративних і економічних важелів і методів, в також інструментів поточного і перспективного екологічно безпечного природокористування [3].

На основі системного підходу щодо формування стратегічних напрямів удосконалення управління екологічно безпечним природокористуванням

виявлено, що основні кроки повинні направлені на формування відповідного інституційного середовища та науково-технічного забезпечення і врахування особливостей розвитку окремих регіонів. Серед першочергових завдань, які для цього потрібно вирішити, можна назвати такі: створення наукових засад екологічної безпеки на базі визначення прийняттого ризику, в тому числі розробка методів інтегрованої оцінки екологічно безпечного природо-користування (промислових об'єктів тощо.) та методів вибору стратегії прийняттого ризику для функціонування промисловості; створення реєстру даних про найкращі доступні технічні рішення або методи, а також системи моніторингу екологічної безпеки; розробка прогностичних оцінок і сценаріїв розвитку природних екосистемних змін в Україні й адекватних заходів реагування; розробка соціально-економічних, нормативно-правових і організаційних заходів для забезпечення екологічно безпечного розвитку України в умовах сучасних ринкових відносин з урахуванням загроз, які мають техногенне або природне походження.

Застосування досвіду країн ЄС та деяких країн світу дозволило визначити головні стратегічні напрями забезпечення екологічно безпечного природокористування в Україні: підвищення енергоефективності будівель, стійку енергетику, стійкий транспорт, сталє сільське господарство, поліпшення запасів і якості води, розвиток екологічної інфраструктури, ефективне використання матеріалів та інвестування в утилізацію відходів.

1. Про Основні засади (стратегію) державної екологічної політики України на період до 2020 р.: Закон України № 2818-VI від 21 грудня 2010 р. Відомості ВР *України*. URL: [http://search.ligazakon.ua/l\\_doc2.nsf/link1/T102818.html](http://search.ligazakon.ua/l_doc2.nsf/link1/T102818.html).
2. Національна екологічна політика України: оцінка і стратегія розвитку. М-во охорони навколишнього природного середовища України, Програма розвитку ООН, Глобальний екологічний фонд. К., 2012. 189 с.
3. Наукові основи національної стратегії сталого розвитку України; [за наук. ред. акад. НААН України, д.е.н., проф. М. А. Хвесика]. К.: ДУ ІЕПСР НАН України, 2013. С. 43-49.

## ОГЛЯД МЕТРИК РЕЗИЛЬЄНТНОСТІ ЕНЕРГОСИСТЕМИ НА РІЗНИХ СТАДІЯХ ЖИТТЄВОГО ЦИКЛУ

Електроенергетичний комплекс є частиною критичної інфраструктури, епіцентром та рушійною силою економіки, національної безпеки та екологічної ситуації в країні. Він взаємопов'язаний з іншими компонентами критичної інфраструктури, такими як газо- та водопостачання, транспортні та комунікаційні системи. Збій в системі енергопостачання безпосередньо і значною мірою впливає на функціонування цих компонент критичної інфраструктури.

Електроенергія має глибокий вплив на всі сфери повсякденного життя, а її відсутність призводить до серйозних наслідків для громад. Брак електропостачання ускладнює надання медичної допомоги, здійснення багатьох видів робіт, забезпечення навчання дітей, а також призводить до порушення комунікаційних процесів.

Спільно з операторами системи розподілу, взимку 2022/2023 рр. компанія "Укренерго" успішно впровадила нові підходи до реагування на обстріли російськими ракетами та дронами енергетичної системи [1]. Ці підходи ґрунтуються на засвоєнні попереднього досвіду, удосконаленні організації ремонтно-відновлювальних робіт та дедалі швидшому та ефективнішому реагуванню на руйнівні події, що відповідає загальносвітовим принципам покращення резильєнтності енергосистеми.

Забезпечення резильєнтності систем є однією з головних тенденцій у світі для забезпечення безпеки як критичної інфраструктури, так і національної безпеки в цілому. Основною властивістю резильєнтної системи є її здатність до ефективної дії протягом усіх етапів кризового реагування з метою виконання цільових функцій. Через своє економічне, гуманітарне і геополітичне значення об'єкти енергетичної інфраструктури є особливо частими цілями російської військової агресії. Тому у контексті резильєнтності енергосистеми, ця концепція може бути визначена як його здатність витримувати порушення роботи та продовжувати надавати доступні енергетичні послуги споживачам. Це означає, що система здатна надійно функціонувати у нормальних умовах, протистояти загрозам, адаптуватися до умов, що постійно змінюються, і швидко відновлюватися після реалізації будь-яких загроз (атак, руйнування, тощо).

На рис. 1 представлено життєвий цикл резильєнтності, розроблений у [2]. Він містить різні етапи планування та управління резильєнтністю, включаючи цикл зворотного зв'язку для врахування досвіду від уроків, отриманих із попередніх подій. Ця ілюстрація підкреслює, що резильєнтність є більше ніж надійність чи здатність до відновлення. Резильєнтність передбачає планування і пом'якшення цих подій до, під час і після їх виникнення.

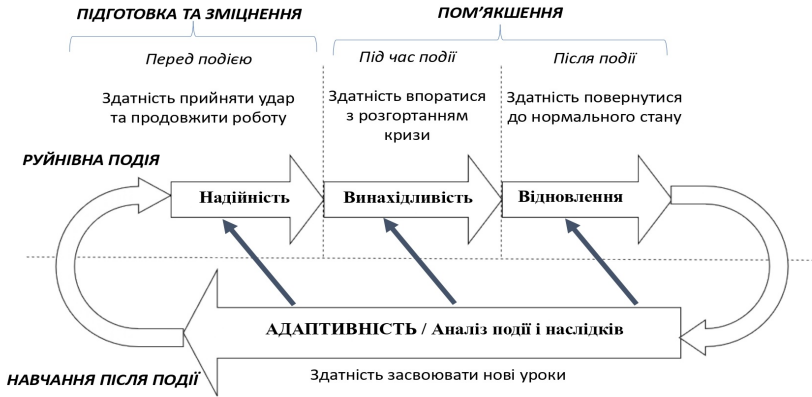


Рисунок 1 – Життєвий цикл резильентності [2]

Характеристики резильентності енергосистеми включають такі аспекти, як стійкість, надійність, резервування, а також швидкість реагування та відновлення. Стійкість фокусується на посиленні компонентів, надійність зосереджується на проектуванні компонентів для роботи в різних умовах, резервування включає встановлення резервних компонентів, а швидкість реагування та відновлення стосуються того, наскільки швидко та ефективно система реагує під час збою [3].

У загальному випадку оцінка резильентності енергосистеми відбувається по різному на різних стадіях її життєвого циклу, як показано на рис. 2, і містить як якісну оцінку перед руйнівною подією, так і кількісну оцінку після події.

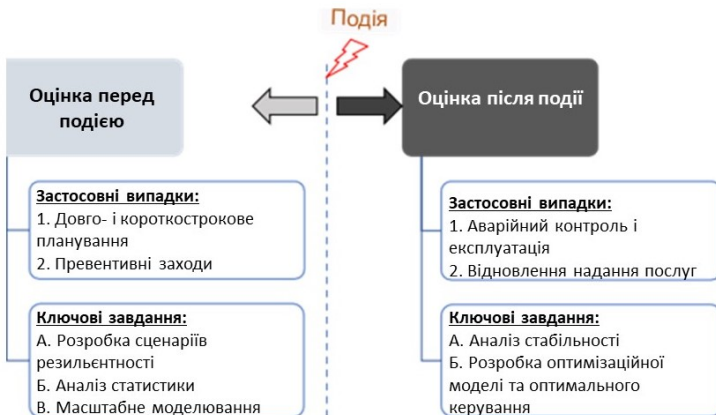


Рисунок 2 – Оцінка резильентності до та після руйнівних подій



Наразі не існує універсальної метрики резильєнтності, яка підходила б для всіх випадків. Було виконано аналіз існуючих підходів до кількісної оцінки резильєнтності, спрямованих передусім на моніторинг пошкодження енергосистеми та її відновлення [4-13].

До події оцінка резильєнтності відбувається за показниками стабільності, надійності та топології. Основні метрики оцінки за цими показниками наведено в табл. 1.

Таблиця 1 – Метрики резильєнтності до надзвичайної події

№	Показник	Метрики	Опис
1	Стабільність	Запас стійкості в перехідних процесах	Область стійкості, що відповідає стабільній точці рівноваги енергосистеми після змодельованої події
2	Стабільність	Застосовна область захисту	Мінімальне рішення дистанційного реле, встановлене після імітованого усунення несправності.
3	Топологія	Ефект підрахунку гілок	Відношення загальної кількості з'єднаних гілок для кожної комбінації шляхів (без зациклення) в можливій мережі до числа всіх критичних навантажень
4	Топологія	Накладання гілок	Загальна кількість спільних гілок у кожній комбінації шляхів (без зациклення) в можливій мережі
5	Топологія	Дублювання джерел	Відношення кількості доступних джерел, що використовуються для живлення всіх критичних навантажень, до числа всіх критичних навантажень в кожній можливій мережі
6	Топологія	Резервування ліній	Відношення загальної кількості ліній, доступних для всіх критичних навантажень, що підключаються до всіх джерел, до загальної кількості критичних навантажень в кожній можливій мережі
7	Топологія	Наявність центрального вузла	Відношення загальної довжини всіх найкоротших ліній, що проходять через певний вузол, до загальної довжини всіх найкоротших ліній між усіма парами вузлів мережі.
8	Надійність	Резерв живлення критичного навантаження	Метрика резильєнтності, що оцінює безперервне постачання критичного навантаження в разі надзвичайної події.
9	Надійність	Очікувана надійність	Покращення/погіршення показників надійності, коли ресурс вважається 100% надійним або 100 % відмова генерації під час моделювання.

Після руйнівної події оцінка резильєнтності відбувається за показниками стабільності, надійності та відновлення. Основні метрики оцінки за цими показниками наведено в табл. 2.

Таблиця 2 – Метрики резильєнтності після надзвичайної події

№	Показник	Метрики	Опис
1	Міцність Стабільність Надійність	Швидкість падіння продуктивності	Загальна кількість зниженої продуктивності системи, поділена на час, протягом якого продуктивність системи знизилася.
2	Міцність Стабільність Надійність	Максимальне падіння продуктивності	Продуктивність системи під час нормального стану за вирахуванням найнижчої продуктивності системи через подію. Він визначається під час руйнівної події і враховує, наскільки низько падає резильєнтність/продуктивність.
3	Стабільність, Надійність	Інтенсивність деградації	Загальний час, протягом якого продуктивність системи тримається на найнижчому/найгіршому значенні через подію.
4	Відновлення	Коефіцієнт відновлення продуктивності	Загальна кількість відновленої продуктивності системи, поділена на час відновлення продуктивності системи.
5	Надійність	Безперебійне обслуговування	Область нижче кривої стійкості/ продуктивності на різних етапах, враховуючи що облік системних послуг не переривається через подію.
6	Відновлення Надійність	Ефективність відновлення	Час, коли продуктивність системи впала з нормального стану до найгіршого, по відношенню до загального часу, протягом якого робота системи була порушена через подію та часу відновлення. Вказує на ефективність відновлення при різних рівнях порушень.
7	Відновлення Надійність	Резильєнтність мережі	Співвідношення порушеної роботи системи до нормальної продуктивності, помноженої на співвідношення відновленої системи до нормальної продуктивності та ефективності відновлення з часом. Вказує на індекс функціональності мережі.

У табл. 3 наведено три найпоширеніші показники, які не належать ні до категорії превентивної чи відновлювальної фази.

Таблиця 3 – Метрики резильєнтності загального значення

№	Показник	Метрики	Опис
1	Відновлення Міцність	Економічна оцінка пошкоджень /збитків	Вартість скидання навантаження/штрафи через подію.
2	Відновлення Міцність	Індекс відновлення потужності в реальному часі	Відношення поточної відновленої продуктивності системи до найгіршої продуктивності, поділене на загальну втрату продуктивності системи через подію.
3	Відновлення Міцність	Миттєве безперервне обслуговування	Відношення миттєвої продуктивності системи до цільової продуктивності під час події.

Так, економічний показник у табл. 3 широко використовується в існуючій літературі для оптимізації реакції резильєнтності енергосистеми. Незважаючи на те, що ця метрика в основному використовується в контексті після події, її також можна використовувати в оцінці резильєнтності до події, щоб керувати плануванням резильєнтності. Інші дві метрики в табл. 3 спрямовані на кількісну оцінку продуктивності системи під час події, тому вони більш придатні для підтримки прийняття рішень у надзвичайних ситуаціях у реальному часі.

1. Ржеутська Л. Що допомогло українській енергетиці пережити важку зиму. Deutsche Welle. <https://www.dw.com/uk/so-dopomoglo-ukrainskij-energetici-pereziti-vazku-zimu-raketnih-udariv-rt/a-64995509>.
2. Moteff J.D. (2012). *Critical infrastructure resilience: the evolution of policy and programs and issues for congress*. Congressional Research Service, R42683.
3. Cabinet Office. (2011). *Keeping the Country Running: Natural Hazards and Infrastructure (A Guide to improving the resilience of critical infrastructure and essential services)* [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61342/natural-hazards-infrastructure.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf).
4. Yao Y., Weijia L., and Rishabh J. 2022. *Power System Resilience Evaluation Framework and Metric Review: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5D00-80817.
5. Zhang H., Bie Z., Li G., and Lin Y., “Assessment method and metrics of power system resilience after disasters,” *J. Eng.*, vol. 2019, no. 16, pp. 880–883, 2019.
6. Talukder S., Ibrahim M., and Kumar R., “Resilience Indices for Power/Cyber- physical Systems,” *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 4, pp. 2159–2172, 2021.
7. Bajpai P., Chanda S., and Srivastava A.K., “A novel metric to quantify and enable resilient distribution system using graph theory and Choquet integral,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2918–2929, 2018.

8. Ouyang M., Pan Z., Hong L., and Zhao L., "Correlation analysis of different vulnerability metrics on power grids," *Phys. A Stat. Mech. its Appl.*, vol. 396, pp. 204–211, 2014.
9. Abbasi S., Barati M., and Lim G.J., "A parallel sectionalized restoration scheme for resilient smart grid systems," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1660–1670, 2019.
10. Chanda S., Srivastava A.K., Mohanpurkar M.U., and Hovsopian R., "Quantifying power distribution system resiliency using code-based metric," *IEEE Trans. Ind. Appl.*, vol. 54, no. 4, pp. 3676–3686, 2018.
11. Panteli M. et. al. "Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3747–3757, 2017.
12. Espiritu J.F., Coit D.W., and Prakash U., "Component criticality importance measures for the power industry," *Electr. Power Syst. Res.*, vol. 77, no. 5–6, pp. 407–420, 2007.
13. Murphy S., Sowell F. and Apt J., "A time-dependent model of generator failures and recoveries captures correlated events and quantifies temperature dependence," *Appl. Energy*, vol. 253, pp. 1-10, July. 2019.

## **ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ АРХІТЕКТУРИ ТИПУ LLaMA ДЛЯ ШВИДКОГО ПРИЙНЯТТЯ РІШЕНЬ У ВІДНОВЛЕННІ ГЛОБАЛЬНОЇ ЕНЕРГОСИСТЕМИ**

Використання чат-ботів на основі LLM (large language model) показує свою практичну корисність у різноманітних сферах. Спеціаліст, що приймає складне технічне рішення, на етапі збору інформації, може задати декілька влучних питань такому боту і швидко отримати необхідну відповідь з посиланням на відповідний нормативний документ чи його частину (наприклад, на розділ потрібного ISO стандарту або пункт інструкції складного обладнання). Таким чином, актуальним завданням є розвиток технологій залучення такого роду чат-ботів в якості асистента, що зможе допомогти спеціалісту швидше зібрати інформацію для підвищення оперативності та обґрунтованості прийняття відповідного рішення.

У лютому 2023-го року компанія MetaAI надала загальний доступ до своїх у розробок в області нейронних мереж типу LLM, так звані LLaMA (Large Language Model Meta AI) [1].

Результати досліджень можливостей моделей нової архітектури, проведених командою вчених із MetaAI, стверджують, що здатності моделі до формування читабельного тексту та формуванні текстових відповідей на відкриті запитання при певних конфігураціях перевершують результати загальновідомої GPT-3 [2].

Оскільки із міркувань інформаційної безпеки GPT-3 не можна використовувати для роботи із оперативною інформацією про стан вузлів глобальної енергосистеми, актуальною є проблема пошуку альтернатив для автономної (без виходу системи в Інтернет) роботи систем аналогічних чат-боту GPT-3.5, саме тому фокус даної роботи припав на моделі LLaMA, які можна використати і налаштувати для роботи в Інtranеті.

Як було згадано вище, через міркування інформаційної безпеки неможливо використати GPT-3.5[3] або його загально доступних аналогів для вирішення ряду задач через такі проблеми:

- відкриті системи, подібні GPT-3.5, являються прикладом black box [4] системи, її автори не розкривають повний механізм їх роботи і не гарантують відтворюваність результатів із плином часу;
- такі системи оброблюють інформацію на боці сервера-хоста моделі, тобто на серверах компанії OpenAI, яка попереджає про збір даних та не гарантує їх анонімне зберігання;
- нефіксована цінова політика для комерційного сегменту не дає можливість передбачити ціну використання такого роду системи у перспективі років.

Для дослідження можливості використання моделей LLaMA було створено прототип автономного англomовного веб чат-боту для навігації у ISO 50001 [5].

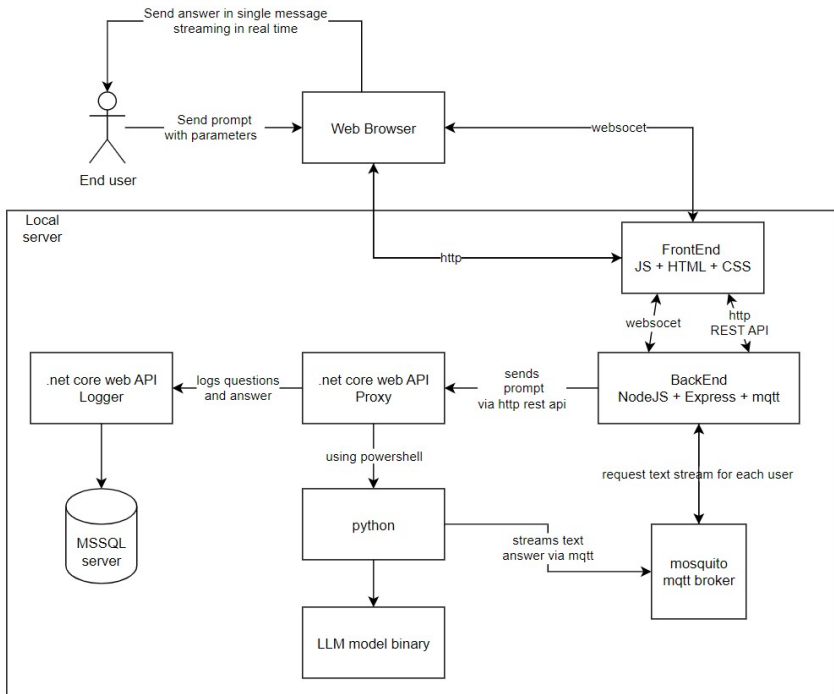


Рисунок 1 – Загальна архітектура розробленого прототипу автономного чат-боту

Послідовність головних подій у системі:

1. За допомогою веб інтерфейсу у браузері користувач надсилає чат-боту запитання з параметрами у контексті ISO 50001.
2. За допомогою JavaScript формується REST API запит із питанням та параметрами.
3. NodeJS проксі отримує запит та перенаправляє до .NET Core API сервісу, тимчасово блокує для усіх користувачів доступ до чат-боту.
4. Сервіс оброблює запит і формує powershell команду для запуску python скрипта.
5. Python скрипт запускає модель та отримує відповідь у формі текстового потоку.
6. Python скрипт по мірі отримання відповіді передає текстові данні на зберігання в окрему комірку локального MQTT брокера Mosquito [6].

7. NodeJS веб додаток через MQTT поступово отримує відповідь на питання та надсилає у якості відповіді на регулярний webSocket запит із боку браузера кінцевого користувача.
8. .NET Core API сервіс логує повне запитання та відповідь у базу даних MSSQL Server, надсилає на сторону NodeJS повідомлення про відновлення доступу до боту для усіх користувачів

## Chat with Guanaco-7B

**You:** What is the role of top management in ISO 50001 implementation?

**Bot:** The role of the top management at a workplace or organization that wants to get certified for ISO 50001 should be one of the most important factors when it comes to the success of the implementation. The ISO 50001 standard requires that an organization's Senior Management should lead and direct the activities of the organization in order to achieve its objectives, and ensure that the system is compliant with all ISO standards. This can be done by delegating tasks and authority to the department managers of the organization, and being directly responsible for ensuring the system is

Wait, bot is busy... Send

500	40	0.95	0.8
1.1	-1		

Created by [Oleksandr Tsyvliak](#) using locally hosted [guanaco-7B-GGM](#)

Рисунок 2 – Веб інтерфейс прототипу

Варто зазначити що для підвищення ефективності чат-боту до кожного запиту можна задати 6 основних параметрів [7]:

1. `max_new_tokens` визначає максимальну кількість нових токенів, які модель може згенерувати в одному виклику.
2. `top_k` використовується для обмеження кількості варіантів токенів, які модель враховує при генерації тексту.
3. `top_p` встановлює поріг ймовірності для включення токенів у генерацію, забираючи менш ймовірні варіанти.
4. `temperature` регулює рівень "креативності" моделі, контролюючи розподіл ймовірностей токенів під час генерації.
5. `repetition_penalty` обмежує повторення токенів у вихідному тексті, покращуючи різноманітність генерації.
6. `seed` визначає початковий стан генерації, що дозволяє отримувати однакові результати при однаковому значенні `seed`.

За для контролю якості «найменшій» із доступних моделей за допомогою прототипу чат-боту згаданого вище було задано 16 екзаменаційних питань із 4-ма варіантами відповіді. Без спеціального підбору оптимальних параметрів і без прямого доступу до повного тексту ISO 50001, бот правильно відповів на 10 запитань. Також бот успішно відповідає на загальні відкриті питання та навіть у вигляді прототипу вирішує поставлену задачу.

Отже, розроблення технологій для застосування LLaMA з метою підвищення оперативності прийняття рішень, зокрема у відновленні енергосистеми, є актуальним та перспективним завданням.

1. Introducing LLaMA: A foundational, 65-billion-parameter large language model. <https://ai.meta.com/blog/large-language-model-llama-meta-ai/>
2. LLaMA: Open and Efficient Foundation Language Models. <https://arxiv.org/abs/2302.13971>
3. GPT-3.5 Turbo fine-tuning and API updates. <https://openai.com/blog/gpt-3-5-turbo-fine-tuning-and-api-updates>
4. Black Box, [https://en.wikipedia.org/wiki/Black\\_box](https://en.wikipedia.org/wiki/Black_box)
5. ISO 50001 – Energy management systems. <https://www.iso.org/publication/PUB100400.html>
6. Eclipse Mosquitto™ An open source MQTT broker, <https://mosquitto.org/>
7. LLM Token selection strategies: Top-K, Top-p, and Temperature <https://peterchng.com/blog/2023/05/02/token-selection-strategies-top-k-top-p-and-temperature/>



## ВИКОРИСТАННЯ БАЗ ДАНИХ У ІОТ ПЛАТФОРМИ THINGSBOARD: ПЕРЕВАГИ ТА НЕДОЛІКИ РІЗНИХ ПІДХОДІВ

В епоху розвитку Інтернету Речей (IoT) вибір платформи для керування пристроями є критично важливим. ThingsBoard – одна з провідних IoT платформ [1]. Авторами платформи є випускники Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», зокрема кафедри прикладної математики [2].

IoT платформа ThingsBoard пропонує гнучкі рішення для інтеграції різних типів пристроїв та джерел даних. Втім, така гнучкість породжує ключове питання: який підхід до бази даних обрати для підвищення продуктивності та надійності системи?

Розглянемо основні підходи до використання баз даних на IoT платформі ThingsBoard.

### 1. PostgreSQL

PostgreSQL – це потужна об'єктно-реляційна база даних, яка забезпечує широкі можливості та високий рівень надійності.

*Переваги:*

*Універсальність.* PostgreSQL підтримує різноманітні типи даних та функції, включаючи JSON, геопросторові запити та ін.

*Спільнота.* Завдяки великій активній спільноті користувачів і розробників PostgreSQL, існує величезна кількість ресурсів, додатків, інструментів та розширень.

*Високий рівень безпеки.* PostgreSQL надає широкі можливості налаштування безпеки, включаючи рольову модель доступу та шифрування.

*Засоби оптимізації.* Інструменти для моніторингу дозволяють оптимізувати роботу з базою даних.

*Недоліки:*

*Обмежена горизонтальна масштабованість.* Хоча PostgreSQL має відмінні показники вертикального масштабування, його горизонтальна масштабованість може бути обмеженою у порівнянні з розподіленими базами даних;

*Складність оптимізації великих обсягів даних (Big Data).* При зберіганні великих обсягів даних можуть виникати проблеми з процесом VACUUM, який очищає застарілі записи;

*Неоптимальна для забезпечення високого ступеня доступності.* Щоб досягти високого ступеня доступності, може знадобитися використовувати додаткові інструменти та конфігурації [3].

### 2. PostgreSQL + Timescale

TimescaleDB – це розширення для PostgreSQL, яке оптимізує базу для

часових рядів. В даному підході ThingsBoard зберігатиме дані часових рядів в гіпертаблиці TimescaleDB, продовжуючи використовувати PostgreSQL для збереження основних об'єктів (пристроїв/активів/інформаційних панелей/клієнтів).

**Переваги:**

*Висока продуктивність для часових рядів.* TimescaleDB оптимізовано для обробки часових рядів, що покращує швидкість запису та зчитування;

*Сумісність з PostgreSQL.* Користувачі можуть використовувати всі можливості PostgreSQL та одночасно користуватися перевагами TimescaleDB;

*Автоматичне масштабування.* TimescaleDB може автоматично розділяти дані на чанки, що спрощує процес масштабування;

*Ефективне агрегування.* Забезпечує високоефективні запити для агрегування даних.

**Недоліки:**

*Залежність від розширень.* TimescaleDB базується на розширенні PostgreSQL, що може призвести до проблем із сумісністю у майбутньому;

*Потреба в спеціалізованих знаннях.* Для оптимальної роботи з TimescaleDB потрібно мати глибокі знання як про PostgreSQL, так і про Timescale;

*Вартість масштабування.* Хоча Timescale дозволяє ефективно масштабувати, вартість апаратного забезпечення для великих обсягів даних може бути великою [4].

### **3. PostgreSQL + Cassandra**

Cassandra – це розподілена база даних для Big Data з високою доступністю. ThingsBoard зберігатиме дані часових рядів у Cassandra, продовжуючи використовувати PostgreSQL для збереження основних об'єктів (пристроїв/активів/інформаційних панелей/клієнтів).

**Переваги:**

*Горизонтальне масштабування.* Cassandra розроблена для того, щоб легко та ефективно масштабуватися, додаючи нові вузли;

*Висока доступність.* Розподілена архітектура Cassandra забезпечує високий ступінь доступності даних, навіть якщо деякі вузли зазнають збою;

*Гнучкість даних.* Cassandra дозволяє гнучко моделювати дані за допомогою її стовбчикової структури, що сприяє швидким записам та запитам;

*Розподілені операції.* Операції читання та запису можуть розподілятися серед усіх вузлів у кластері, оптимізуючи швидкість та ефективність.

**Недоліки:**

*Складність.* Cassandra вимагає глибоких знань для правильного налаштування та обслуговування, що бути викликом для команд, які звикли працювати тільки з реляційними базами даних.

*Затримка у запитах.* В залежності від конфігурації Cassandra може мати велику затримку відгуку на деякі види запитів, особливо коли даних дуже багато.

*Потреба в регулярному моніторингу.* Для забезпечення оптимальної роботи та відсутності проблем потрібен постійний моніторинг та налаштування [5].

Таким чином, вибір бази даних для IoT платформи – це ключове рішення, яке впливає на продуктивність, надійність та масштабованість системи. Кожен з розглянутих підходів – **PostgreSQL**, **PostgreSQL + Timescale**, та **PostgreSQL + Cassandra** – має свої унікальні переваги та недоліки.

**PostgreSQL** підходить для проєктів, де потрібна універсальність, висока безпека та відмінні засоби оптимізації.

**PostgreSQL + Timescale** ефективний для сценаріїв, для великих обсягів даних часових рядів та забезпечення високоефективних запитів агрегування даних цих рядів, при цьому зберігаючи всі переваги PostgreSQL.

**PostgreSQL + Cassandra** є найкращим варіантом для дуже великих обсягів даних часових рядів та великих швидкостей запису, де потрібне горизонтальне масштабування та високий ступінь доступності.

Підсумовуючи, слід зауважити, що це лише початковий крок у вирішенні завдань щодо підвищення живучості та резильєнтності IoT систем. Подальші дослідження можуть бути спрямовані на розробку нових методів інтеграції та оптимізації баз даних для IoT платформ, зокрема платформи ThingsBoard.

1. Crozdesk.com – Business Software Search. (2023). ThingsBoard. Retrieved from <https://crozdesk.com/software/thingsboard>.
2. ThingsBoard IoT Platform. (2017). Retrieved from <https://thingsboard.io/company/>.
3. The PostgreSQL Global Development Group. (2023). PostgreSQL: The World's Most Advanced Open Source Relational Database. Retrieved from <https://www.postgresql.org/>.
4. Timescale Inc. (2023). PostgreSQL++ for time series and events Retrieved from <https://www.timescale.com/>.
5. The Apache Software Foundation. (2023). Open Source NoSQL Database. Retrieved from <https://cassandra.apache.org/>.

## **РЕЗИЛЬЄНТНІСТЬ ІОТ СИСТЕМ В УМОВАХ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ПЕРЕДАЧІ ДАНИХ**

Системи Інтернету речей (ІоТ) стрімко розвиваються і поширюються в останні роки, вбудовуючись у різні аспекти повсякденного людського життя, від розумних будинків до промислових процесів [1]. Однак це широке впровадження породило низку проблем і складнощів, які необхідно вирішити, щоб ці системи продемонстрували стійкість у передачі даних [2].

Одним із ключових аспектів поточної екосистеми ІоТ є широке розмаїття використовуваних пристроїв і протоколів зв'язку. Пристрої ІоТ бувають різних видів і вони працюють на різних протоколах зв'язку, таких як Wi-Fi, Bluetooth, Zigbee, LoRa та стільникові мережі [3]. Ця неоднорідність створює проблеми з точки зору сумісності та безпеки. Крім того, актуальною проблемою є масштабованість систем ІоТ. Оскільки кількість підключених пристроїв продовжує зростати, керування даними, створеними цими пристроями, та забезпечення ефективної передачі виходить на перший план.

У сфері дослідження резильєнтності систем ІоТ щодо цілісності передачі даних використання онтологій і семантичних технологій для опису системних пристроїв ІоТ пропонує безліч переваг [4]. Ці технології відіграють ключову роль у покращенні розуміння, управління та контролю над багатомодульною системою Інтернету речей, забезпечуючи цілісність даних, що передаються [5].

Онтології забезпечують структурований і стандартизований спосіб представлення знань про пристрої ІоТ. Вони визначають зв'язки, властивості та класи, які характеризують ці пристрої та їхні функції. Використовуючи онтології, дослідники та практики можуть створити загальний словник і семантичну структуру для опису пристроїв ІоТ. Це стандартизоване представлення полегшує взаємодію між пристроями та системами, забезпечуючи безперебійний зв'язок і обмін даними.

Семантичні технології дають змогу системам ІоТ досягати більш інтелектуальних і контекстно-залежних операцій. Вони дозволяють пристроям анувати інформацію значущими метаданими, описуючи не лише самі дані, але й контекст, у якому вони були згенеровані. Ця контекстна інформація має вирішальне значення для підтримки цілісності даних, оскільки дозволяє пристроям приймати обґрунтовані рішення щодо подальшої передачі, поєднання та обробки даних [6].

Крім того, онтології та семантичні технології полегшують автоматизоване обґрунтування та прийняття рішень у системах ІоТ. Пристрої можуть визначати зв'язки, залежності та обмеження між даними, що може бути безцінним для виявлення аномалій або потенційних загроз цілісності даних. Наприклад, якщо датчик виявляє раптовий, незрозумілий стрибок температури, який не

узгоджується з моделями історичних даних, він може подати сповіщення або самостійно вжити коригувальних дій.

Розглянувши всі типи онтологій, ми обрали саме три, онтологія пристрою описує функціональні та нефункціональні характеристики даних реального датчика. Онтологія предметної області – це свого роду базовий набір знань і зв'язків для кожної предметної області, в яку інтегрований IoT. Онтологія верхнього рівня зберігає інформацію про всі функції та дії системи. Усі онтології описані на мові OWL з використанням середовища Protégé. У табл. 1 наведено кількісні характеристики понять, правил і аксіом.

Таблиця 1 – Характеристика онтології передачі даних в IoT системах

Артефакти онтології	Кількість
Поняття	120
Властивості	200
Аксіомі	54
Взаємозв'язки	150

Мова SPARQL використовувалася для запитів на отримання даних з онтологій. Було проаналізовано 24 запити до онтології, і всі відповіді відповідають поставленому завданню. Триває подальший розвиток у масштабуванні чат-бота для керування розумним будинком за допомогою більшої кількості пристроїв і покращенні показників продуктивності.

Такі проактивні заходи підвищують резильєнтність систем Інтернету речей шляхом пом'якшення потенційних проблем із цілісністю даних до їх ескалації. Загалом використання онтологій і семантичних технологій в описі системних пристроїв IoT дозволяє цим системам працювати ефективніше, інтелектуальніше та безпечніше, зрештою забезпечуючи цілісність передачі даних при виявленні різноманітних проблем і невизначеностей.

1. IoT Editorial Office, I. (2023). Acknowledgment to the reviewers of IoT in 2022. *IoT*, 4(1), 56. <https://doi.org/10.3390/iot4010003>.
2. Delic, K. A. (2016). On resilience of IoT systems. *Ubiquity*, 2016(February), 1–7. <https://doi.org/10.1145/2822885>.
3. Misić, J., Ali, M.Z., & Misić, V.B. (2018). Protocol architectures for IoT domains. *IEEE Network*, 32(4), 81–87. <https://doi.org/10.1109/mnet.2018.1700395>.
4. Novo, O., & Francesco, M.D. (2020). Semantic interoperability in the IoT. *ACM Transactions on Internet of Things*, 1(1), 1–25. <https://doi.org/10.1145/3375838>.
5. Kulykivska, N., & Timenko, A. (2019). A structure of semantic service in a distributed knowledge based system. *Computer Modeling and Intelligent Systems*, 2353, 533–543. <https://doi.org/10.32782/cmisi/2353-42>.
6. Palo, H.K. (2021). Semantic IoT: The Key to Realizing IoT Value. У *Semantic IoT: Theory and applications* (с. 81–102). Springer International Publishing. [https://doi.org/10.1007/978-3-030-64619-6\\_4](https://doi.org/10.1007/978-3-030-64619-6_4).

## **ELECTRON USECASE1: DEFENDING AGAINST POWER GRID CYBER ATTACKS – INSIGHTS FROM UKRAINE**

The Ukraine power grid hack incident in 2015 was a significant event that highlighted the vulnerability of critical infrastructure systems to cyber-attacks. In response to this incident, many organizations and cybersecurity experts have developed use cases and scenarios that explore the potential consequences of a similar attack and how to prevent it.

Cyber Attack on Ukrainian Power Grid – Situation Overview: The massive, nation-state attack first struck the Prykarpattyaoblenergo control center, which, in turn, took out 30 substations. Two other distribution centers, Chernivtsioblenergo and Kyivoblenergo, were also hit at the same time but on a smaller scale. The attack left 230,000 residents without power, along with two of the three distribution centers that were hacked because the attack took out the back-up generators at the center, as well. The electricity outage lasted up to six hours for residents, but the computers on-site that were infected couldn't be salvaged. Cyber-attack on Ukrainian power grid is the first publicly documented case of power outage that was caused by a cyber-attack. Attackers used spear phishing to plant malware called 17 BlackEnergy3 which disabled computers that controlled the system. Moreover, not only did the attackers disable computers, they overwhelmed call centers as well, so that the customers could not get in touch with companies' customer care centers and thus made response activities more difficult to complete. (FireEye 2016) Michael Assante, SANS lead on ICS and SCADA security commented on this attack, saying that the attackers demonstrated planning, coordination, and the ability to use malware and possible direct remote access to blind system dispatchers, cause undesirable state changes to the distribution electricity infrastructure, and attempt to delay the restoration by wiping SCADA servers after they caused the outage." In his own words, the attack was complex and the malware was just one of three main components that enabled the cyber-attack. (Assante 2016).

One of ELECTRON Use Case1 inspired by the Ukraine power grid hack incident might involve a scenario where a group of hackers gain access to a utility company's network and deploy malware that allows them to take control of critical systems, including power generation and distribution. The attackers then proceed to disrupt the energy supply, causing a widespread power outage that affects thousands of homes and businesses.

To prevent this scenario from occurring, the Use Case might explore a range of cybersecurity measures and response actions, such as:

- Implementing multi-factor authentication and access controls to prevent unauthorized access to critical systems.
- Deploying network monitoring tools to detect and respond to unusual activity on the network.

- Regularly backing up critical data to prevent loss and ensure quick recovery in case of an attack.
- Conducting regular cybersecurity training and awareness programs for employees to recognize and respond to cyber threats.
- Developing and implementing a comprehensive incident response plan that includes strategies for identifying and mitigating cyber-attacks, as well as procedures for communicating with customers and the public in the event of a disruption.
- Regularly conducting penetration testing and vulnerability assessments to identify and address potential weaknesses in the system.

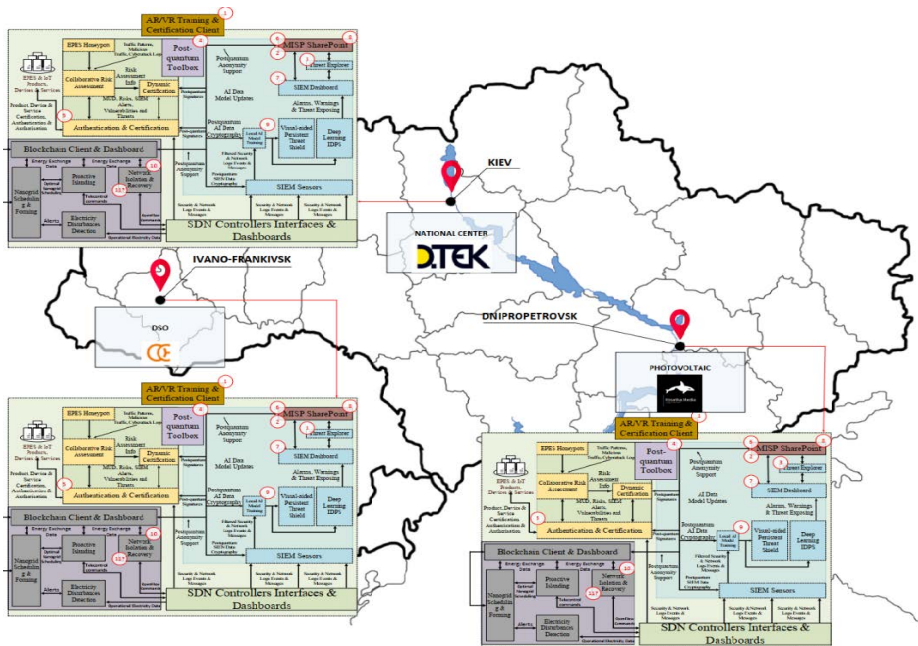


Figure 2 – Use Case 1 Architecture

Use Case 1 aims to exhibit the ability of the ELECTRON system to safeguard and protect a real electrical network from possible cyberattacks and to effectively mitigate their impact, therefore keeping the investments safe and avoiding possible cascading effects [1]. In particular, it is expected that ELECTRON will detect and mitigate threats that can cause a distribution system to stop functioning, such as Denial of Service (DoS) attacks, as well as threats that can cause some grid parts to overcharge, such as False Data Injection (FDI) attacks. As mentioned previously, unauthorized access attacks can surrender control of the Substation to an adversary

who can then switch substations on and off, thus stressing the electric grid and causing a blackout. It shall, therefore be attempted to utilize ELECTRON to shield the electrical network from such attacks. Finally, ELECTRON shall attempt to guarantee the privacy and encryption of the data transmitted through its communication channels, to protect DSO data, from potential Man in the Middle (MitM) attacks.

On Digital Security in Ukraine, the aim focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets & market incentives in Europe, following an end-user driven approach, including for instance law enforcement agencies, first responders, operators of critical infrastructures, ICT service providers, ICT manufacturers, market operators and citizens.

The abilities of the ELECTRON project allow to provide the implementation of next-generation power systems capable of resisting energy systems against cyberattacks, increasing data confidentiality through four main initiatives: risk assessment and evaluation, detection and prevention of anomalies, mitigation of failures and acceleration of systems recovery, elimination of internal threats and through staff training and certification.

ELECTRON Use Case1 inspired by the Ukraine power grid hack incident can provide valuable insights into the potential consequences of a cyber-attack on critical infrastructure systems and help organizations to develop effective strategies for prevention and response [2].

1. ELECTRON architecture, blog 2022 <https://electron-project.eu/blog/electron-architecture/>.
2. Use Case 1 Addressing and Mitigating Cyberattacks and Data Leaking in Ukraine & Azerbaijan <https://electron-project.eu/use-cases/use-case-1/>.



## **ПРОГРАМОВАНІ ЛОГІЧНІ ІНТЕГРАЛЬНІ СХЕМИ ЯК ОСНОВА ПІДВИЩЕННЯ ЖИВУЧОСТІ СУЧАСНИХ ТЕХНОЛОГІЧНИХ СИСТЕМ**

Сучасні технологічні системи являють собою автоматизовані або автоматичні системи, які є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначені для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних [1].

Зазначимо, що технологічні системи являють собою складні технічні системи, відносяться до об'єктів критичної інформаційної інфраструктури, в якості основних елементів містять засоби обчислювальної техніки – процесори, блоки пам'яті, перетворювачі, датчики, вимірювальні та виконавчі пристрої, елементною базою яких є інтегральні схеми.

Важливість задач, які вирішуються сучасними технологічними системами, з одного боку, і складність таких систем, з іншого боку, вимагають від таких систем не лише високої надійності, а й живучості, враховуючи той факт, що дані системи постійно знаходяться під несприятливим впливом, а останнім часом також під впливом кібератак.

На відміну від надійності, яка оцінює стійкість складних технічних систем, з точки зору елементної надмірності та резервування, живучість дозволяє забезпечити як структурну, так і функціональну стійкість системи в процесі її функціонування. При цьому підвищення живучості здійснюється не лише класичними механізмами розпізнавання, протидії та відновлення, а й спеціальними засобами адаптації, реконструкції, реконфігурації і реорганізації. Це дозволяє створювати структури, які забезпечують виконання критичної підмножини функцій для досягнення мети функціонування [2].

Так, останнім часом для підвищення надійності і живучості складних технічних систем широко використовується підхід, заснований на застосуванні в якості елементної бази програмованих логічних інтегральних схем (ПЛІС) [3]. Програмовані логічні інтегральні схеми є матрицею програмованих логічних елементів із SPLD (Simple Programmable Logic Devices), CPLD (Complex Programmable Logic Device), FPGA (Field-Programmable Gate Array), FLEX (Flexible Logic Element Matrix) структурами. Завдяки цим структурам створюється новий клас систем – універсальні системи на кристалі (System-on-Chip – SoC).

Система на кристалі, або SoC, являє собою обчислювальну систему, реалізовану в інтегральному виконанні, до складу якої входять високопродуктивний процесор або декілька процесорів, математичний процесор

обробки даних та цифрової обробки сигналів, додаткові модулі пам'яті, набори периферійних пристроїв (контролерів) тощо. Така організація обчислювальної системи набула широкого поширення завдяки своїй універсальності, малому енергоспоживанню і навіть можливості реконфігурації її алгоритмічної структури шляхом перепрограмування ПЛІС.

Зазначимо, що на сьогодні системи на кристалі витісняють громіздкі обчислювальні структури, реалізовані за допомогою набору інтегральних схем, замінюючи їх сучасними мікроконтролерами (PIC, AVR, MSP430, STM-32, Cortex-M, TSP-32 тощо), програмованими логічними інтегральними схемами (ПЛІС – CPLD, FPGA, FLEX) та одноплатними комп'ютерами Raspberry Pi, Beagle Bone Black, тощо.

Аналіз сучасної технічної літератури свідчить про те, що застосування ПЛІС в якості елементної бази побудови цифрових пристроїв та обчислювальних систем відкриває нові можливості щодо підвищення живучості цифрових пристроїв та обчислювальних систем не лише від несприятливого впливу, а також від впливу кібератак.

Так, в [4] для підвищення живучості обчислювальних систем запропоновано підхід, в основі якого лежить реалізація на ПЛІС принципу активної відмовостійкості, а саме: виявлення відмови шляхом застосування існуючих методів контролю складних технічних засобів; локалізація відмови шляхом застосування методів тестового та функціонального діагностування; відновлення правильного функціонування системи шляхом реконфігурації її внутрішньої структури на рівні логічних елементів. При цьому зазначимо, що в основу реконфігурації внутрішньої структури цифрових пристроїв та обчислювальних систем покладено положення прескриптивної теорії, яка розглядає питання цілеспрямованого управління об'єктами різної природи, що перебувають у стані «конфлікту» з іншими об'єктами [5].

Отже, реалізація принципу активної відмовостійкості на сучасній програмованій елементній базі дає можливість протидіяти несприятливим впливам і, тим самим, підвищити живучість технологічних систем у цілому.

1. Про основні засади забезпечення кібербезпеки України, Закон № 2163-VIII (2017). <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
2. Додонов, А., & Ландэ, Д. (2011). *Живучесть информационных систем*. Наукова думка. 256 с.
3. Штаненко, С., & Самохвалов, Ю. (2021). Технологія System-on-Chip як основа підвищення живучості складних технічних систем. *Сучасна спеціальна техніка: ДНДІ МВС України*, (3 (66)), с. 31–43.
4. Штаненко, С., Самохвалов, Ю., & Толюпа, С. (2023). Методичний підхід до відновлення правильного функціонування вбудованих систем на рівні програмованої елементної бази. *Збірник наукових праць «Системи і технології зв'язку, інформатизації та кібербезпеки»*, (3), с. 171–181.
5. Обухов, В., & Павлов, В. (1979). *Синтез избыточных дискретных устройств с реконфигурацией структуры*. Наукова думка. 156 с.

## КОРОЗИЙНА СТІЙКІСТЬ І ЖИВУЧІСТЬ ТЕПЛОВИДІЛЯЮЧИХ ЕЛЕМЕНТІВ АКТИВНОЇ ЗОНИ ЯДЕРНОГО РЕАКТОРА

Цирконій та його сплави Zr-1%Nb (Україна), Zr-2, Zr-3, Zr-4 (США), Zr-Nb-Cu (Канада), Zr-Cu-Fe, Zr-Nb-Sn (ФРГ), Zr-(0,5-5)%Cu (Великобританія), M5 (Франція) та ін. – матеріали, що використовуються у сучасному реакторобудуванні. Рівень механічних властивостей і їх стабільності в умовах впливу зовнішніх чинників (високих температур, радіаційного опромінення, агресивних середовищ), а в умовах війни в Україні ще й під можливими загрозами пошкодження устаткування енергоблоків АЕС в результаті військових дій, має відповідати жорстким вимогам. Легування сплавів цирконію залізом підвищує його корозійну та радіаційну стійкість в умовах роботи ядерного реактора. Водночас, додаткове легування сплавів цирконію киснем знижує його технологічність, що потребує розробки нової деформаційної та термічної схеми виготовлення оболонкових труб. Визначити оптимальний вміст заліза за таких умов – актуальна задача дослідницького, технологічного процесу, а також задача модельної підтримки вирішення даної проблеми.

В роботах [1-2] проведено вимірювання швидкості корозії зразків сплаву цирконію Zr-1%Nb з різним вмістом заліза (табл. 1) і побудовано апроксимаційний поліном (1) залежності відкості  $V(F, T)$  від вмісту заліза  $F$  і терміну  $T$  перебування зразків в умовах, наближених до реальних експлуатаційних в ядерному реакторі.

Таблиця 1 – Значення швидкості корозії

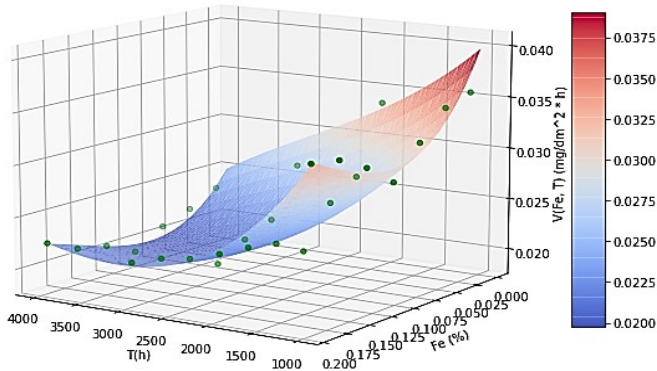
Fe, % T, год	0,012	0,042	0,072	0,102	0,132	0,162	0,192
1000	0,0358	0,03495	0,0323	0,0293	0,0314	0,03285	0,03326
2000	0,03383	0,02722	0,02542	0,02153	0,02311	0,02359	0,02385
3000	0,02653	0,02178	0,02062	0,01905	0,02041	0,02132	0,02179
4000	0,023145	0,02174	0,02075	0,01904	0,02045	0,02104	0,02242

$$\begin{aligned}
 V(F, T) = & a_0 + a_1T + a_2F + a_3T^2 + a_4T \cdot F + a_5F^2 + \\
 & + a_6T^3 + a_7T^2 \cdot F + a_8T \cdot F^2 + a_9F^3,
 \end{aligned}
 \tag{1}$$

де коефіцієнти поліному (1) подано в табл. 2.

Таблиця 2 – Коефіцієнти апроксимаційного поліному (1)

$a_0$	$a_1$	$a_2$	$a_3$	$a_4$
-0.68953395	-0.59437232	-0.22295343	0.36915152	0.0747594
$a_5$	$a_6$	$a_7$	$a_8$	$a_9$
0.33696609	-0.09272832	0,14789556	-0.05873025	-0.09225197

Рисунок 1 – Модель залежності  $V(F, T)$ .

Отримані результати привели до висновку, що оптимальне значення вагового вмісту заліза, при фіксованому значенні терміну часу  $T$ , при якому спостерігається мінімум швидкості утворення корозії, зосереджене в інтервалі, що містить значення  $F=0.1\%$  (рисунок 1).

Експериментальні дані, представлені в табл. 1, безумовно не є точними, бо завжди має місце інструментальна похибка вимірювань, хаотичні викривлення невідомої величини, спостерігається вплив умов проведення експерименту на значення вимірюваної величини і т.д. Результати спостережень є обмеженими – це безумовний факт, але вони мають характер невизначеності і неповноти інформації. Сформулюємо задачу визначення швидкості корозії зразків цирконію за таких умов. В такій ситуації поняття множини (інтервалу) невизначеності виміру, що безумовно містить істинне значення спостереження, відкриває можливість змоделювати процес зміни степені корозії в зразках сплаву цирконію. В термінах інтервального аналізу дана задача є задачею визначення інтервальної функції  $V(F, T^*)$  [3],  $T^*$  – фіксоване значення терміну часу перебування зразків в умовах експерименту, і знаходження оптимального значення  $\arg \min V(F, T^*)$ , що можна визначити, як задачу глобальної оптимізації [4] або як задачу інтервального квадратичного програмування [5, 6].

За даними експерименту (рисунок 2) з великою ймовірністю функція залежності швидкості корозійного процесу від вмісту заліза, зокрема при проведенні дослідження протягом  $T^1 = 1000$  годин, має характер квадратичної залежності. Тобто інтервальна функція  $V(F, T^*)$  матиме вигляд

$$V(F, T^1) = \mathbf{A}_0^1 + \mathbf{A}_1^1 \cdot F + \mathbf{A}_2^1 \cdot F^2 = \left[ \underline{V(F, T^1)}, \overline{V(F, T^1)} \right], \quad (2)$$

де  $\mathbf{A}_0^1 = \left[ \underline{A}_0^1, \overline{A}_0^1 \right], \mathbf{A}_1^1 = \left[ \underline{A}_1^1, \overline{A}_1^1 \right], \mathbf{A}_2^1 = \left[ \underline{A}_2^1, \overline{A}_2^1 \right]$  – інтервальні коефіцієнти.

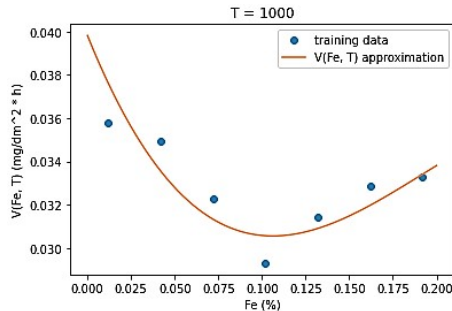


Рисунок 2 – Залежність  $V(F, 1000)$  швидкості корозійного процесу від вмісту заліза при фіксованому значенні часу  $T = 1000$  годин.

Квадратичними будуть залежності і в випадках  $T^2 = 2000, T^3 = 3000, T^4 = 4000$  годин.

Задача пошуку оптимального значення інтервальної функції  $V(F, T^*)$  і оптимального значення (інтервального значення) параметру  $F$  є сукупністю двох оптимізаційних задач: визначення мінімуму функції  $\underline{V(F, T^*)}$  і мінімуму  $\overline{V(F, T^*)}$ . Якщо розв'язками даних задач є інтервали  $\mathbf{F}_1$  і  $\mathbf{F}_2$ , то шуканою множиною (інтервал або точка) значення параметру  $F$  слід вважати  $\mathbf{F}^* = \mathbf{F}_1 \cap \mathbf{F}_2$ , якщо такий перетин існує.

Використання інструментарію інтервального аналізу дозволяє визначити не лише точку оптимуму, але й інтервал змін значень параметра, який відповідає ситуації невизначеності вимірюваних значень цільової функції, врахуванню похибок різного походження і їх степені впливу, а також містить всі такі значення, в яких інтервальна функція досягає мінімуму.

1. Yefimov, O.V., Pylypenko, M.M., Lyubchuk, L.M., Potanina, T.V., Kravchenko, V.P., Yesypenko, T.O., Harkusha, T.A. (2023). The method for optimizing the iron content in the nuclear reactors. Problems of Atomic Science and Technology, 2(144), 46-51. <https://doi.org/10.46813/2023-144-046>.

2. Pylypenko, M.M., Drobyshevska, A.O., Zuyok, V.A. (2022). Influence of iron additives on the corrosion resistance of the Zr-1%Nb alloy under operating conditions of a nuclear reactor. *Problems of atomic science and technology*. 1(137), 51-54. <https://doi.org/10.46813/2022-137-51>.
3. Moore, R.E., Kearfott, R.B., Cloud, M.J. (2009). *Introduction to interval analysis*. Philadelphia. Society for Industrial and Applied Mathematics.
4. Eldon, H. (1980). Global Optimization Using Interval Analysis – The Multi-Dimensional Case. *Numerische Mathematik*. 34, 247-270.
5. Elsisy, M.A., Hammad, D.A., El-Shorbagy, M.A. (2020). Solving Interval Quadratic Programming Problems by Using the Numerical Method and Swarm Algorithms. *Hindawi*. <https://doi.org/10.1155/2020/6105952>.
6. Wei, L., Xiaoli, T. (2008). Numerical Solution method for general interval quadratic programming. *Applied Mathematics and Computation*, 2 (202), 589-595. <https://doi.org/10.1016/j.amc.2008.02.39>.

## **FLEXIBILITY OF THE ENERGY SYSTEM MODEL**

The Energy Union is one of the main priorities of the new European Commission. The energy transition must be supported by models, and thus by the collaboration of modeling teams on methodology and data.

Many energy modeling teams need to analyze the transition from the current energy system to future systems with significantly higher shares of renewable energy sources (RES). The models used to solve these problems have questions about aspects of flexibility.

Flexibility is “system’s ability to cope with short-term uncertainty in the system’s energy variables.” While in the past a high share of thermal power plants guaranteed sufficient flexibility of the energy system, the increase in the share of variable RES is changing this paradigm. These RES create a new source of short-term uncertainties arising at the hourly level. In this regard, the development of uncertainties, which require flexibility, occur along the complete supply chain in energy systems. They often appear due to deviations from the forecast (e.g. wind flow, power exchange, end use, demand) regardless of the energy system sector. To eliminate these deviations, it is necessary to have available a number of technological options, such as demand response, network and storage, expansion, excess capacity, reduction of peak supply of RES.

In the last few years, the share of power plants using RES in the structure of generating capacities of UES of Ukraine has significantly increased. The presence of a significant share of such generating capacities leads to the fact that daily fluctuations in the consumption/generation of electrical energy are superimposed on significant fluctuations in the capacity of RES installations, associated with changes in atmospheric conditions. In the winter season, the presence of such fluctuations is compensated for by the general participation in the regulation of the frequency of hydroelectric power plants, gas power plants, and thermal power plants.

Future energy systems are likely to be a complex combination of centralized and decentralized energy production with a wide range of energy resources and new energy technology. As electricity consumption becomes more important, the use of demand flexibility is a complex and multidisciplinary definition. In order to adequately analyze and mitigate the impact of the increase in the share of variable generation in the energy system, the existing methodological analysis and modeling of energy systems need improvement at all levels, including frequency and voltage stability studies, economic dispatching, regional planning models, and global integrated assessment models.

A central question to be modeled and analyzed is the value of flexibility, i.e. what is the value of flexible generation, flexible demand and other flexibility options such as energy storage and/or a combination of these options. Consideration should be given to the value of flexibility in different time scales, in different geographic regions

and in different regional markets. The distribution of the value of flexibility among different participants in energy systems is also an important issue.

In today's open energy markets, the most important market indicator is the spot price, but energy market models are difficult to combine into different economic approaches. Social welfare is a tool for evaluating society. End users make decisions based on business economics and include other important aspects such as distribution, costs and taxes. If we want to evaluate the value or usability of demand management, we need to use several types of modeling approaches to evaluate it from all sides, for example, society, system, utility, network, end user.

It is important to pay attention to physical and economic aspects, as both are relevant and related to obtain useful and valid information [1, 2]. It is necessary to consider what type of uncertainty arises from the penetration of intermittent energy sources and what flexibility is required to solve the problems imposed on the electricity system, how flexible technologies will be used and to what extent competition between these technologies may arise, or what characteristics determine the effective integration of electricity from large shares of RES .

There are several methodological approaches to modeling the flexibility of energy systems:

- Using heuristics;
- Sectoral highly detailed models;
- Combined models.

With the advent of more computing power, efficient codes, new numerical approaches, parallel computing, and intelligent algorithmic designs, there is an opportunity to revise the structure and architecture of energy system models and long-term planning models. Therefore, a special emphasis is placed on the integration of energy systems: the creation of technical and economic tools for industries. It is necessary to build a well-functioning integrated energy system at the national and international levels. The research program includes areas that cover the necessary range of topics, including control and forecasting, modeling and analysis, economics, finance and consumers that together make up the energy system.

Energy conservation has advantages in terms of fast response time, uncertainty management, ability to reduce constraints, but it may be difficult to justify economically in many systems until high levels of variable RES are seen. Energy storage will compete with other flexible resources such as interconnection and more, efficient operation of the existing thermal generator park and demand management. Detailed system modeling is required to understand the challenges surrounding the benefits of energy storage in terms of flexibility, ancillary services and uncertainty.

Currently available models are not able to adequately reflect flexibility issues, so new approaches are needed in power system modeling.

For example, TIMES models establish a correct and useful hierarchy of costs, but this does not provide information on issues such as technical viability. Moreover, in TIMES-like models, increasing the number of time slices only addresses the variability itself, but usually does not take into account operational constraints, and



thus these models are often insufficient to provide flexibility. Also, this option significantly increases the complexity and time of the model.

Proposed models of energy systems to meet future energy needs generate paths of a complete energy system, choosing energy technologies for end use, transformation and energy supply technologies with the possibility of setting restrictions, such as maximum carbon dioxide emissions, minimum renewable energy, maximum energy security, etc. Computationally, this makes the problems more manageable, but there are trade-offs in terms of accuracy and solution quality.

To simplify the model, it is necessary to achieve the right trade-off between utility and computational complexity. This requires identifying the critical assumptions that affect the model's results. In this way, it is determined what can be simplified and what can be simulated without compromising the accuracy and reliability of the model results.

Determining the appropriate level of temporal and geographic resolution, using options for parallelization, flexibility, technology, and a clustering block of methods (which significantly reduce run time), and choosing which constraints to include or not include in the model are the most important options available for simulation.

In addition to methodological challenges, data collection for models is a separate challenge that includes a large number of different technological options along with detailed technical constraints in energy system models, requiring vast amounts of information. Two major areas of data improvement relate to the assessment of renewable energy potential, as well as the forecasting of future demand response and demand profiles.

The flexibility of the system can also be set through regulation (for example, forced speed increase). The representation of market and regulatory aspects needs to be improved so that the models are useful with well-founded results. Preserving the multiplicity of models is important because it allows policy-specific models to be adapted, as well as benchmarking results to increase robustness.

The need for flexibility of energy systems is due to the rapid development of RES. Demands for flexibility encourage the convergence of planning and operational decision-making in energy systems. System models to properly capture energy flexibility require increasing levels of detail that, given the limitations of modeling techniques and computing power, involve finding the right balance between detail and scope.

1. J. Ma, V. Silva, R. Belhomme, D. Kirschen, L. Ochoa Evaluating and planning flexibility in sustainable power systems// IEEE Transactions on Sustainable Energy, 2013, Vol. 4, no. 1, pp. 200-209.
2. J. Ma Evaluating and Planning Flexibility in a Sustainable Power System with Large Wind Penetration /University of Manchester, 2012.

## ПРОБЛЕМАТИКА ПІДБОРУ МЕТРИК ДЛЯ ОЦІНКИ КІБЕРВІДМОВСТІЙКОСТІ

### Вступ

Забезпечення кібервідмовостійкості відіграє надзвичайно важливу роль для секторів промисловості, ІТ-систем та для життєдіяльності цілих держав. Щоб забезпечити надійність систем, інженери шукають способи застосування концепцій кібервідмовостійкості та інтеграції технологій підвищення стійкості в архітектури, конструкції та операційні системи.

### Основна частина

Насамперед потрібно розібратися з понятійним апаратом. У всій англійській літературі існує консенсус щодо терміну "*Cyber resilience*" (прямий переклад – кіберстійкість), там де ми вживаємо термін *кібервідмовостійкість* [1]. Кібервідмовостійкість – це здатність організації забезпечити розвиток діяльності (стійкість підприємства) за рахунок готовності до кіберзагроз, можливості реагування на них, засобів відновлення після кібератак [2]. Цю здатність можна розглядати на різних рівнях (див. табл. 1). Кожен рівень пропонує свої унікальні виклики, методи та можливі засоби контролю щодо забезпечення кібервідмовостійкості. Отже, здатність постійно досягати запланованого результату може стосуватися не тільки лише окремих країн, а також організацій чи навіть конкретних ІТ-систем. Однак, щоб кібервідмовостійкість була ефективною, її потрібно розглядати цілісно, на кількох рівнях, паралельно.

Таблиця 1 – Кібервідмовостійкість на різних рівнях

Рівень	Масштаб	Приклад
Міжнаціональний	Для конфедерацій	Європейський союз
Національний	Для країни	Україна
Регіональний	Для регіону, або міста	Київ
Організаційний	Для організації	Компанія
Функціональний	Для бізнес-функцій	Процес захисту
Технічний	Для технічних систем	ІТ-система, мережа

Кібервідмовостійкість може бути актуальною властивістю в різних масштабах або областях. Ці області приблизно відповідають чотирьом областям у матриці кібервідмовостійкості:

- компоненти та системи, які можуть бути виявлені за допомогою фізичних засобів;
- системи, які можуть бути оцінені в інформаційній або технічній сфері;
- програми та операції з кібербезпеки всередині організації;
- структури та механізми для прийняття рішень, пов'язаних із кібервідмовостійкістю, в організаційному, галузевому, регіональному, національному чи транснаціональному масштабах [3].



Рисунок 1 – Масштаб, у якому можна оцінити кіберстійкість [4]

Згідно даних Національного інституту стандартів і технологій (NIST) можна виділити такі характеристичні параметри кібервідмовостійкості:

Основні функції:

1. *Ідентифікація* – завчасний пошук індикаторів впливу, векторів атак, які можна використати, щоб проникнути у ІТ-екосистему.
2. *Захист* – зменшення вразливих місць відповідно до вашої терпимості до ризику.
3. *Виявлення* – виявлення індикаторів компрометації за допомогою аудиту в реальному часі, виявлення аномалій та попередження.
4. *Відповідь* – швидкий збір та аналіз інформації про інцидент, задля прийняття обґрунтованих рішень щодо найкращого способу дій.
5. *Відновлення* – швидке, точне та ефективне відновлення системи і даних.
6. *Керування* – це наскрізна функція, яка інформує та підтримує інших; наприклад, результати управління визначають пріоритетність засобів контролю безпеки.

Чотири мети кібервідмовостійкості. Мета – це твердження високого рівня про очікувані результати. Чотири мети, описані в керівництві NIST:

- *передбачення* – підтримка стану інформованої готовності до негараздів;

- *витримка* – продовжувати свою важливу місію чи бізнес-функції, незважаючи на труднощі;
- *відновлення* – здатність відновити свою місію під час та після негараздів, можливо, використовуючи поетапний процес;
- *адаптація* – кінцева мета – змінити місію організації та їхню підтримку у відповідь на зміни в IT-середовищі та ландшафті загроз.

Цілі кібервідмовостійкості. Цілі – це більш конкретні заяви про очікувані результати. Згідно NIST окреслює вісім цілей кібервідмовостійкості:

1. *Запобігання або уникнення* – запобігання успішному виконанню атаки або реалізації несприятливих умов.

2. *Підготовка* – розуміння того, що негаразди відбудуться, і відповідно, дотримання набору реалістичних реакцій для подолання очікуваних негараздів.

3. *Продовження* – максимізація тривалості та життєздатності основних місій або бізнес-функцій під час труднощів.

4. *Обмеження* – обмеження шкоди від негараздів, завданих цінним активам, таким як ті, що зберігають або обробляють конфіденційну інформацію або підтримують важливі для місії можливості.

5. *Відновлення* – відновлення якомога більше функцій місії чи бізнесу після негараздів, гарантуючи, що відновлені ресурси є надійними.

6. *Розуміння* – підтримка корисного представлення місії та бізнес-залежностей і статусу ресурсів щодо можливих негараздів.

7. *Трансформація* – зміна місії або бізнес-функції та їх допоміжних процесів, щоб краще справлятися з труднощами.

8. *Перебудова* – зміна системи, місії та допоміжної архітектури, щоб ефективніше справлятися з труднощами.

#### Основні системи для оцінки кібервідмовостійкості:

- метрика групи I. Лінкова (Resilience metrics for cyber systems) [5];
- фреймворк для оцінки кіберстійкості, розроблений всесвітнім економічним форумом [6];
- стандарти Агентства Європейського для мережевої та інформаційної безпеки (European Union Agency for Network and Information Security (ENISA) Standards);
- платформа для підвищення рівня кібербезпеки критично-важливої інфраструктури (Національний інститут стандартів і технологій (NIST));
- методологія дослідників американської неприбуткової організації Корпорація Mitre.

#### **Висновки**

Наступним етапом після формування понятійного апарату має стати розробка методик метрик кіберстійкості. Позаяк процес порівняння систем різних організацій вимагає узгодженості припущень щодо контексту, у якому показник використовується, необхідно отримувати оцінку кібервідмовостійкості об'єктів.

Потрібна більш тонка система підбору, ранжирування та підрахунку

показників для метрик, щоб детально порівнювати альтернативні потенційні вимоги систем/об'єктів, можливості чи рішення.

Це дасть можливість адаптувати, застосувати існуючі концепції та створити власну модель кібервідмовостійкості для українських реалій.

1. Гальчинський Л.Ю., Личик В.В. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство. Київ: Міжрегіональна Академія управління персоналом, 2023. Випуск 2 (8). 98 с. – Режим доступу: <http://journals.maup.com.ua/index.php/it/issue/view/260>.
2. Björck F., Henkel M., Stirna J. Zdravkovic J. (2015). Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*. Vol. 353. Stockholm University. pp. 311–316.
3. Bodeau D., Graubart R., McQuaid R., Woodill J. (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report.
4. Bodeau D. and Graubart R., "Cyber Resiliency Metrics: Key Observations (PR Case No. 16-0779)," May 2016. [Online]. Available: <https://www.mitre.org/publications>.
5. Linkov I., Eisenberg D.A., Plourde K, Seager T.P., Resilience metrics for cyber systems December 2013 *Environment Systems and Decisions* 33(4) DOI: 10.1007/s10669-013-9485-y.
6. World Economic Forum (2016a) A framework for assessing cyber resilience. URL – [http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016\\_WEF.pdf](http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf).

## МОДЕЛІ ТА АРХІТЕКТУРА МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМИ УКРАЇНИ

**Актуальність** розгляду даної теми спричинив прогресивний науковий вплив та запровадження нових методів цифрових технології в діагностиці, які почали впроваджуватися у сучасному медичному обладнанні, що призвело до необхідності проведення суттєвих змін в сфері охорони здоров'я, а також механізмах та каналах взаємодії між обладнанням, пацієнтами та постачальниками медичних послуг. В основу цих змін лягли механізми за якими відбувається збір, обробка, обмін, зберігання та аналіз медико-санітарної інформації про пацієнта. Також це спричинило необхідність створення єдиної загальної системи медичних інформаційних стандартів.

Провідне місце в цих процесах зайняли медичні інформаційні системи (МІС) різного рівня, створені на підставі діючих стандартів та призначені для автоматизації різноманітних процесів з обробки даних, які відбуваються в закладах системи охорони здоров'я.

**Метою даної роботи** є дослідження МІС запроваджених в Україні та методи підвищення їх функціональності.

Починаючи з 2017 року Національною службою здоров'я України поступово впроваджується електронна система охорони здоров'я (ЕСОЗ) e-Health (рис. 1).



Рисунок 1 – Ключові ролі держави та бізнесу у електронній системі охорони здоров'я України

В Україні система e-Health складається з центрального компонента (ЦБД) – він відповідає за централізоване зберігання і обробку інформації та різноманітних МІС які пройшли тестування ДП «Електронне здоров'я» (рис. 2).



Рисунок 2 – Архітектура системи e-Health в Україні

При цьому слід зазначити що кожний медичний заклад України обирає свою модель МІС відповідно до власних потреб.

МІС які отримали допуск на ринок України використовують різні моделі для організації обміну та передачі медичної інформації, за їх функціональним призначенням можна виділити наступні моделі:

1. **Централізована модель:** У централізованій моделі існує один центральний сервер або центральна база даних, до якої підключені різні медичні заклади або системи. Усі дані зберігаються та обробляються центральним сервером, а доступ до них надається з різних точок підключення. Це дозволяє зручно керувати медичною інформацією та забезпечує її централізований доступ.

2. **Децентралізована модель:** У децентралізованій моделі кожен медичний заклад або система має власну базу даних, яка зберігає медичну інформацію. Ці бази даних можуть бути підключені між собою, щоб обмінюватися важливими даними. Кожен заклад має свою автономію та контроль над своєю медичною інформацією.

3. **Розподілена модель:** У розподіленій моделі медична інформація розподілена по різних вузлах або серверах, які мають повну копію даних або їх фрагменти. Кожен вузол може працювати самостійно та незалежно, але при потребі дані можуть бути синхронізовані між вузлами. Це забезпечує резервне копіювання та доступ до медичної інформації в разі відмови одного з вузлів.

4. **Хмарна модель:** У хмарній моделі медична інформація зберігається та обробляється на хмарних серверах, які надають доступ до даних через Інтернет (рис. 3). Медичні заклади або системи можуть використовувати послуги хмарних провайдерів для зберігання та обробки своїх даних. Це дозволяє швидкий та зручний доступ до медичної інформації з будь-якого місця, де є Інтернет-підключення.

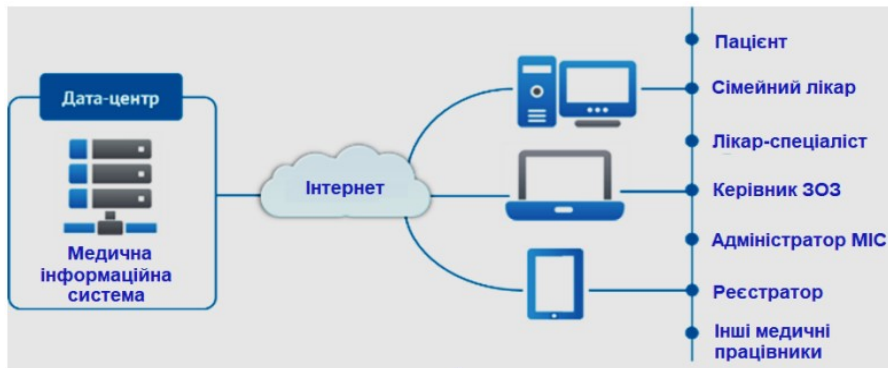


Рисунок 3 – Схема функціональної взаємодії користувачів з МІС на базі хмарних технологій

**5. Гібридна модель:** Гібридна модель поєднує різні аспекти централізованої, децентралізованої, розподіленої та хмарної моделей. Вона дозволяє комбінувати різні підходи в залежності від потреб та вимог медичних закладів або систем. Наприклад, може бути централізована база даних, але з можливістю підключення локальних систем у розподіленому режимі.

Однак, незалежно від обраної моделі МІС, доволі важливим питанням для закладів охорони здоров'я залишається збереження МІС своєї функціональності. У контексті МІС, живучість і резильєнтність є важливими для забезпечення безперервності надання медичної допомоги. Порушення роботи МІС може призвести до переривання надання медичних послуг, що може мати серйозні наслідки для пацієнтів.

Існує ряд заходів, які можна вжити для підвищення живучості та резильєнтності медичних інформаційних систем. Ці заходи можна класифікувати на наступні категорії:

- **архітектурні рішення:** використання високодоступних і відмовостійких архітектурних рішень, таких як розподілені системи, кластери і розподілені бази даних;
- **технологічні рішення:** використання технологій, які підвищують живучість і резильєнтність, таких як резервне копіювання, відновлення після аварії, імітація відмов і моніторинг;
- **процедурні рішення:** розробка процедур і процесів для управління порушеннями, такими як плани відновлення після аварії і процедури реагування на інциденти.

Рис. 4 ілюструє використання розподіленої архітектури для підвищення живучості МІС. У цьому випадку система розділена на кілька компонентів, які розташовані в різних місцях. Це означає, що якщо один компонент вийде з ладу, інші компоненти зможуть продовжувати працювати.



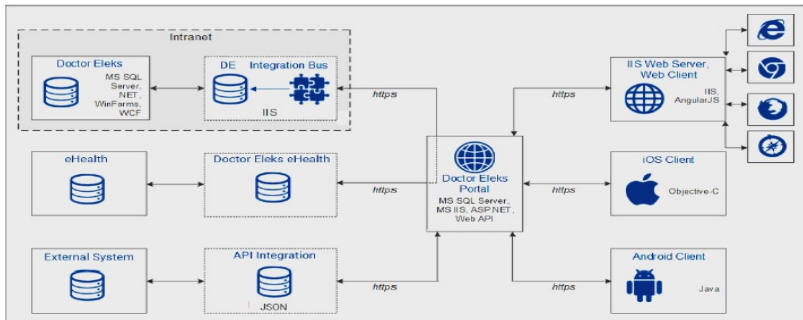


Рисунок 4 – Архітектура МІС «Доктор Елекс»

Сьогодні у світі також активно розглядається можливість використання штучного інтелекту (ШІ) та інших інноваційних технологій які можуть відігравати критичну роль у підвищенні живучості та резильєнтності медичних інформаційних систем (МІС). Наведемо деякі з методів та практичних аспектів які обговорюються в світі:

- використання ШІ для постійного моніторингу стану МІС та аналізу даних може допомогти вчасно виявляти збої та проблеми. Нейронні мережі можуть використовуватися для прогнозування збоїв на основі аналізу динаміки даних;
- ШІ може керувати автоматичним відновленням МІС після збоїв. Наприклад, система може виявити збій у сервері та переключити роботу на резервний сервер без втрати доступності;
- використання ШІ для діагностики та попередження збоїв. Алгоритми машинного навчання можуть вивчати звичайну роботу системи та виявляти аномальні патерни, які можуть вказувати на можливі збої;
- моделі машинного навчання можуть допомогти прогнозувати пікові навантаження на МІС. На основі цих прогнозів можна налаштувати ресурси для оптимальної продуктивності;
- використання комп'ютерного моделювання для емуляції різних сценаріїв збоїв та роботи МІС у віртуальному середовищі. Це дозволяє визначити слабкі місця та вдосконалити систему;
- впровадження голосових і текстових інтерфейсів для взаємодії з МІС може полегшити користувачам доступ до інформації під час збоїв і надзвичайних ситуацій;
- використання технології Blockchain для забезпечення надійності та безпеки зберігання медичних даних та логів подій.

**У висновку** можна зазначити що питання розвитку МІС їх впровадження в медичних закладах України та використання новітніх технологій для підвищення функціональності є актуальним і вимагає подальших всебічних наукових досліджень, фахівцями різних галузей.

1. «Цифрові трансформації системи охорони здоров'я в умовах реформування». Т. В. Запорожець, doi:10.32702/2307-2156-2021.10.3.
2. «Впровадження засобів цифрового управління в сфері охорони здоров'я» / Л.Ф. Соколенко, С.О. Линник. doi:10.32702/2307-2156-2020.8.53.
3. Електронна система охорони здоров'я в Україні. Електронний ресурс. Доступ за посиланням <https://ehealth.gov.ua>.
4. Медична інформаційна система «Доктор Елекс»: основи роботи. Під редакцією І. Березовської, Ю. Триуса. Львів, Ліга-Прес, 2018 р.
5. Кудрявець В.В., Кобилянська О.В., Кобзар В.А. Архітектура та технології медичних інформаційних систем: Навчальний посібник. – Львів: Видавництво Львівської політехніки, 2018. – 160 с.
6. Лещенко В.В., Мельник О.А., Сірик В.І. Методи та технології забезпечення безпеки медичних інформаційних систем: Навчальний посібник. – Вінниця: Національний технічний університет України "Вінницький політехнічний інститут", 2020. – 146 с.
7. "Artificial Intelligence in Healthcare: Anticipating Challenges" – J.J. Wallach. Published on 7.7.2020 in Vol 22, No 7 (2020): July. Електронний ресурс, посилання на сайт <https://www.jmir.org/2020/7/e17707>.
8. "Resilience and Security of Healthcare IT Systems" – G.von Lubitz. Електронний ресурс. посилання на сайт <https://www.sciencedirect.com/science/article/pii/S0166497222001304>.

## **ДЕЯКІ ПИТАННЯ ВПЛИВУ ТЕХНІЧНОГО СТАНУ ДВИГУНІВ ВЛАСНИХ ПОТРЕБ НА ОЦІНКУ РЕЗИЛЬЄНТНОСТІ ТЕПЛОВОЇ ЕЛЕКТРОСТАНЦІЇ**

Електроенергетичні системи – це кіберфізичні системи, операції та процеси в яких організуються, контролюються та проводиться їх моніторинг за допомогою комп'ютерних мереж. Незважаючи на свої величезні переваги, комп'ютерні мережі є критично важливими компонентами електроенергетичних систем, що піддаються ризику кіберзагроз. Тому зменшення кібернетичних ризиків в електроенергетичних мережах привертає багато уваги дослідників. Деякі автори [1] пропонують поглиблений аналіз безпеки електроенергетичних систем. Їх підхід ґрунтується на розширеному визначенні ризику, що включає такі фактори, як загрози, вразливість, непередбачені обставини та вплив. Він визначає динамічний вибір непередбачених обставин на основі поточних ідентифікованих загроз. Існує декілька визначень резильєнтності. Одне з перших визначень стійкості було розроблено в 1973 році в рамках дослідження екологічних систем, а саме: "Міра стійкості системи до змін і збурень, яка дозволяє їй зберігати постійні відносини між своїми станами": "Міра стійкості систем і здатності поглинати зміни та збурення, зберігаючи при цьому ті ж самі взаємозв'язки між змінними стану" [2]. Резильєнтність широко вивчається також в таких дисциплінах як екологія, психологія теорія катастроф та ін [3].

Належне визначення пріоритетів є ефективним способом вирішення питань безпеки та управління ризиками. Він спрямований на максимізацію переваг наявних ресурсів шляхом зосередження на найбільш важливих питаннях і, таким чином, мінімізації властивих безпеці ризиків [4]. Такий процес, безумовно, передбачає і) використання деяких порівняльних суджень для визначення системи ранжування та ii) техніку підтримки прийняття рішень для оцінки та порівняння різних варіантів рішення щодо визначення пріоритетів. У цьому контексті, переважна більшість існуючих практик визначення пріоритетів залежить лише від якісних показників та/або процесів прийняття рішень, що ґрунтуються на ступенях важливості. Якісні судження та показники, як правило, дуже суб'єктивні. Таким чином, вони можуть призвести до прийняття рішень, сильно заангажованих індивідуальними поглядами. На такі рішення може вплинути неточна інтерпретація стану системи, спричинена вимушеним консенсусом суджень на несприятливу подію.

На практиці процес управління та оцінки ризиків включає в себе кілька інших технічних та організаційних факторів, а не лише показники ступеня важкості несприятливої події.

Парадигма аналізу ризиків в енергетиці безумовно пов'язана з парадигмою ризиків, яка існує при створенні систем кібербезпеки.

Згідно цієї парадигми ризику, У відповідності з ISO/IEC 27000:2009 [5], інформаційна безпека включає до себе три основних виміри конфіденційність, доступність та цілісність.

Модель адитивного ризику інформаційної безпеки можна представити наступним чином:

$$H_c p_c + H_i p_i + H_a p_a = R$$

де  $H_c p_c$  – ризик конфіденційності;  $H_i p_i$  – ризик цілісності;  $H_a p_a$  – ризик доступності;  $R$  – загальний ризик;  $H$  – величина втрат;  $p$  – вірогідність втрат.

Шкала оцінки ризику має 100 значень. Оскільки  $0 \leq p \leq 1$  то  $1 \leq H \leq 100$ .

Для оцінки ризиків виходу із ладу енергетичного блоку можливі наступні парадигми:

$H_c p_c$  – ризик конфіденційності буде відповідати ризику несанкціонованого доступу до безпроводного приймача та технічного стану такого приймача;

$H_i p_i$  – ризик цілісності – розрахунковий ресурс та вірогідність виходу з ладу двигуна власних потреб;

$H_a p_a$  – ризик доступності – фактичний ресурс та вірогідність виходу з ладу двигуна власних потреб, який залежить від режиму роботи та технічних показників (наприклад вібраційних, згідно ДСТУ ИСО10816-3-2014 «Контролювання стану машин за результатами вимірювання вібрації на необертюваних частинах» та МЕК 60034-1-2007 «Машини електричні обертові».

В доповіді розглянуто використання даного підходу для оцінки резильєнтності двигунів власних потреб Трипільської ТЕЦ [6].

1. Alshavish A., de Meer H., Risk Mitigation in Electric Power Systems: Where to start? *Energy Informatics*, 2019, Open Access.
2. Holling C.G. Resilience and Stability of Ecological Systems. *Annual Review of Ecological Systematics*, 1973, vol., 4, pp. 1-23.
3. Espinoza-Zelaya C., Bai Moon J. Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC PapersOnLine* 55-10, 2022, pp. 2252-2257.
4. Gonzalez-Granadillo G., Garsia-Galfaro J., Alvares E., El-Barbori M., Debar H. Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the rori index. *Comput. Elect. Eng.* Vol. 47, pp.13-34.
5. ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary.
6. Титко О.І. Підвищення надійності та ефективності електричних машин у динамічних режимах генеруючих енергоблоків. *Праці Інституту електродинаміки НАН України*: 2009. – Вип 23. – С. 83-90.

## ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ПІДПРИЄМСТВА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Впровадження та поширення інформаційних технологій у всіх сферах сучасного бізнесу призвело до збільшення обсягів електронної комерції та створило сприятливі умови для розвитку онлайн-торгівлі. Фактор цифровізації безпосередній суттєвий вплив на розвиток підприємств сфери електронної комерції, у тому числі на формування конкурентоспроможності, з огляду на зростання у 2022 році кількості користувачів Інтернету до п'яти мільярдів осіб. За статистикою, частка інтернет-торгівлі у світовому товарообігу роздрібних продажів зросла від 14% у 2019 році до 19,5% у 2022 році [1]. Актуальність питання впровадження стратегії резильєнтності в управління підприємством електронної комерції стає особливо очевидною при розгляді прогнозів щодо розширення цієї галузі: до кінця 2023 року світовий ринок електронної комерції досягне обсягу в 6,3 трильйона доларів США, що становитиме 21,2% від загального обсягу роздрібних продажів [2].

З точки зору управління бізнес-процесами підприємства електронної, стратегію резильєнтності можна розглядати як [3]: здатність системи своєчасно реагувати на появу внутрішніх вразливостей; формування безперервності бізнесу; наявність концепцій швидкого відновлення після шоків та зовнішніх збурень; гнучкість інформаційного забезпечення для прийняття своєчасних управлінських рішень.

З точки зору сучасної міжнародної практики резильєнтність розглядається як здатність підприємства протидіяти гібридним загрозам, у тому числі інформаційним вразливостям в системі управління, відновлювати і набувати стійкості у кризових ситуаціях. Одним із шляхів подолання цих викликів є діджиталізація та якість інформаційного забезпечення системи управління. Наприклад, Україна хоч і має один з найнижчих рівнів доступу до Інтернету в Європі – 65% (на початок 2022 року цей показник становив 71,8%), однак з цієї групи лише 44% користувачів Інтернету здійснюють покупки онлайн.

Незважаючи на те, що електронна комерція стала невід'ємною частиною нашого щоденного життя, електронна комерція також призводить до нових ризиків, таких як кібератаки, технічні збої, порушення приватності і багато інших. Ці загрози можуть призвести до великих фінансових втрат, порушення довіри клієнтів і навіть припинення діяльності підприємств..

Навіть після незначного спаду, що пов'язано з економічною нестабільністю країни, спричиненою війною, сегмент електронної комерції поступово зростає. Однак, такий стрімкий розвиток нині супроводжується великою кількістю управлінських викликів і загроз для ритейлерів e-commerce, таких як: недосконалість логістичних моделей доставки товарів, складність процесу обробки повернутих та залишених замовлень, адаптація до змін в чинному

законодавстві, масштабованість, сумісність та стабільна робота інформаційних систем, відбір та адаптація персоналу тощо. Такий широкий спектр наявних проблем для підприємств електронної комерції демонструє необхідність імплементації політик резильєнтності в управлінні бізнес-процесами.

Управління резильєнтністю підприємства електронної комерції є важливим завданням, особливо в умовах змінного бізнес-середовища та надзвичайних ситуацій, таких як пандемія, технічні збої, військовий стан, повосенне відновлення в контексті купівельної спроможності.

Для забезпечення управління резильєнтністю на підприємстві електронної комерції як необхідно зосередити увагу на такі системні заходи:

- проведення регулярних аналізів ризиків та оновлення планів відповідно до змін у середовищі;
- розгортання резервних серверів і дата-центрів для забезпечення надійності і неперервності операцій;
- використання різних постачальників послуг хостингу та інфраструктури для запобігання відмова в обслуговуванні;
- використання сучасних засобів шифрування та захисту даних;
- проведення регулярних аудитів безпеки та тестів на проникнення;
- забезпечення дотримання нормативних вимог щодо захисту персональних даних (GDPR);
- удосконалення механізмів спілкування з клієнтами, постачальниками та іншими зацікавленими сторонами під час кризових ситуацій онлайн;
- залучення персоналу до процесу прийняття рішень у кризових ситуаціях та створення команди реагування.

Зазначені практики можуть допомогти підприємствам електронної комерції в Україні зберегти резильєнтність та впоратися з різними викликами в сучасному бізнесі.

1. Щербак О. Електронна торгівля. Українська та світова практика правового регулювання. Дельта інтернешнл сервіс | Delta International Services. URL: <https://disua.com.ua/uk/elektronna-torgivlya-ukrayinska-ta-svitovapraktyka-pravovogo-regulyuvannya/> (дата звернення: 30.09.2023).
2. Kinan M. Global ecommerce statistics and trends to guide your store (2023). Shopify Plus. URL: <https://www.shopify.com/enterprise/global-ecommerce-statistics> (date of access: 30.09.2023).
3. Rudrajeet P. Organizational resilience through crisis strategic planning: doctoral thesis. 2013. URL: <http://urn.kb.se/resolve?urn=urn:nbn:se:hb:diva-3669> (date of access: 30.09.2023).

## РОЗРОБКА МЕТОДИКИ ОЦІНКИ ПРОФІЛІВ ФУНКЦІОНАЛЬНИХ ПОСЛУГ ЗАХИСТУ НА БАЗІ ОПТИМІЗАЦІЙНИХ ПІДХОДІВ

Для вирішення завдання розробки методики проектування профілів, які можуть адаптуватися до різних підкласів автоматизованих систем, пропонується використовувати метод динамічного програмування. Актуальність цієї проблеми зумовлена відсутністю на даний момент нормативного документа Держспецзв'язку України, який регулював би методику проектування профілів, здатних адаптуватися до загроз, пов'язаних з різними підкласами автоматизованих систем, такими як АС-1, АС-2 та АС-3. Розроблювана методика вперше включатиме можливість боротьби з загрозами, які можуть торкатися конфіденційності, цілісності та доступності інформації (підкласи К, Ц, Д), а також одночасно загрози, що поєднують різні аспекти (підкласи КЦ, КД, СД, КЦД) даних аспектів безпеки.

При використанні класичного підходу [1], ми можемо створити прикладний алгоритм або методику для оцінки профілів, які можуть адаптуватися до загроз, специфічних для різних підкласів автоматизованих систем, таких як АС-1, АС-2 та АС-3, при розробці систем захисту. Для цього необхідно провести дослідження вимог, встановлених у НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99, та визначити практичний зміст, що дозволить нам розробити методику для обчислення параметрів цільової функції при процесі оптимізації:

$$\begin{aligned}\Psi_i(x_i) &= [1 - (1 - \gamma)^{x_i - a_i}] \\ x_i &\geq a_i, i = 1, 2, \dots, n \\ a_i &= -\ln[w_i(i - \beta_i)^{m_i}]\end{aligned}$$

Програмна реалізація даної методики дозволить реалізувати систему підтримки прийняття рішень для побудови профілів, адаптивних за підкласами АС із використанням математичного методу динамічного програмування, що дозволить оптимізувати сам процес побудови профілю безпеки.

Подальшим розвитком цього є вирішення зворотної задачі по розрахунку рівня захищеності заданого профілю профілів безпеки. Пряма та зворотна задачі в комплексі при вирішенні будують основу для розробки нових профілів або коригування вже існуючих, визначаючи наукові причини для цього, що підтверджує актуальність отриманих результатів.

1. Bellman R.E. Dynamic Programming. – Princeton University Press, 2010. – 392 p.

## **INTRODUCTION OF THE NIST CYBERSECURITY FRAMEWORK INTO THE REGULATORY FRAMEWORK OF UKRAINE, AS A BASIS FOR THE INTRODUCTION OF CYBER RESILIENCE AND IMPLEMENTATION OF CYBER RESILIENCE REVIEW**

The relevance of cybersecurity of energy sector facilities has been especially evident since the beginning of the open aggression of the Russian Federation against Ukraine starting from February 24, 2022.

From the beginning of the military aggression, the occupiers showed a special interest in the capture and destruction of energy facilities. On February 24, 2022 the Kakhovskaya hydroelectric power station was captured. On 25 February, Russian troops blew up a gas pipeline near Kharkiv, Ukraine's second-largest city. On 2 March, 2022, Russia claimed to have taken control of the area surrounding the 5.7GW nuclear power plant in Zaporizhzhia, Europe's largest. In addition, during the period of autumn 2022 – spring 2023, the occupiers repeatedly launched rocket-bomb strikes specifically at energy facilities. At the same time, according to the analysis of the specialists of the ESET corporation, which works in close contact with the State Service for Special Communications and Information Protection of Ukraine, energy facilities were one of the priority targets of cyberattacks by the aggressor state [1].

Such activity of the enemy caused the accelerated modernization of requirements for the protection of critical infrastructure, including in cyberspace. At the beginning of last year, the state of regulatory regulation of cyber security issues was not fully determined. It is worth noting that the requirements for cyber security for critical infrastructure objects are described in the following legal documents:

- Law of Ukraine on the Basic Principles of Cybersecurity in Ukraine [2];
- Law of Ukraine on information protection in information and communication systems [3];
- Resolution of the Cabinet of Ministers of Ukraine on Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects [4];
- Law of Ukraine on Critical Infrastructure [5].

Law of Ukraine "About Critical Infrastructure" was entered into force on June 15, 2022 and finally defined a special body that will have to develop requirements for the protection of critical infrastructure and create a register of critical infrastructure objects – this body is State Service of Special Communications and Information Protection of Ukraine. Also, according to the text of the Law, a list of types of organizations is included, which, according to their type of activity, belong to critical infrastructure. Energy is included in this list. In addition, an important innovation of this law is the introduction of a risk-based approach and the requirement for insurance of security risks.

In 2021, the Administration of the State Service for Special Communications and Information Protection of Ukraine published Order No. 601 dated October 6, 2021, containing "Methodical recommendations on increasing the level of cyber protection



of critical information infrastructure"[6]. Changes to this order, which were approved by the orders of the State Special Communications Administration dated 12.10.2021 No. 616 and dated 10.07, were published later. 2022 No. 343. These recommendations are developed taking into account the Framework for Improving Critical Infrastructure Cybersecurity issued in 2014 and updated in 2018 by the National Institute of Standards and Technology of the United States of America (NIST Cybersecurity Framework – NIST CSF) [7].

As a next step, on March 24, 2023, the Cabinet of Ministers of Ukraine adopted the Resolution on "Some issues of conducting an independent audit of information security at critical infrastructure facilities", which introduced a mandatory cyber security audit of critical infrastructure facilities every 2 or 3 years (depending on the category criticality) [8].

Since the State Service for Special Communications and Information Protection of Ukraine is responsible for the cyber protection of critical infrastructure objects, it can be stated that at the moment there are 3 different ways to confirm compliance with cyber security requirements, according to the 601st Order:

- Construction of a comprehensive information protection system with confirmed compliance (KSZI);
- Building an information security management system (ISMS);
- Audit for compliance with NIST CSF requirements and re-audit following implementation of recommendations.

In addition, it should be noted that some Ukrainian energy companies fall under the scope of regulation of the European Union in matters of cyber security. For example, the Ukrenergo company, as an operator of the dispatching and trunk transmission system, is part of the European network of electricity transmission system operators, which unites 43 operators in 39 countries of the European continent – ENTSO-E (European Network of Transmission System Operators for Electricity), which has and develops its cybersecurity requirements – Network code on energy cybersecurity.

The recast of the Electricity Regulation (Regulation (EU) 2019/943) [9] gives the Commission a mandate to develop a network code for cybersecurity. The Smart Grids Task Force has been doing preparatory work since 2017, and released its second interim report in July 2018. The report recommends setting up an early warning system for the energy sector in Europe, cross-border and cross-organisation risk management, minimum security requirements for critical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

In January 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code. The Network Code on Cybersecurity(NCCS) is the first network code that will be developed according to the new rules established by the European Union on the internal market for electricity and is expected to enter into force by January 2024. The network code aims to set a European standard for the cybersecurity of cross-border

electricity flows. It focuses on improving cybersecurity resilience through the enhancement of threat decision and incident reporting and proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services. On January 14, 2022, the preparation of the draft document was completed. [10]

At the same time, the State Service for Special Communications and Information Protection of Ukraine and the Cabinet of Ministers of Ukraine, with the active help of international partners, are working on updating Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019 "On the approval of General requirements for cyber protection of critical infrastructure objects", which will lead to the acquisition of NIST CSF status is necessarily the standard for critical infrastructure facilities, instead of a recommendation status. This is a very important and timely step, as it will allow to synchronize the issue of cyber protection of critical infrastructure with the United States and implement a standard that was created specifically for critical infrastructure, as well as remove the variability of the choice of the approach by which to build cyber security at the objects of critical infrastructure.

Thus, it can be stated that at the moment in the Ukrainian regulatory and legal field there is an approach based on building cybersecurity, but not cyberresilience.

Cybersecurity and cyberresilience are related concepts but have distinct meanings in the context of digital security. While legislation varies between Europe and the USA, the following explanations provide general definitions and highlight the importance of prioritizing cybersecurity before focusing on cyber resilience in the energy sector:

– Cybersecurity: Cybersecurity refers to the measures and practices employed to protect digital systems, networks, and data from unauthorized access, damage, disruption, or theft. It involves the implementation of safeguards, technologies, and processes to prevent, detect, respond to, and recover from cyber threats. Cybersecurity focuses on safeguarding the confidentiality, integrity, and availability of information and systems.

- Legislation in Europe: In Europe, the General Data Protection Regulation (GDPR) includes provisions related to cybersecurity, as it aims to protect personal data from unauthorized access or breach. Additionally, the EU Directive on Security of Network and Information Systems (NIS Directive) emphasizes the need for robust cybersecurity practices in critical infrastructure sectors, including energy.
- Legislation in the USA: The United States has several cybersecurity-related laws, including the Federal Information Security Modernization Act (FISMA), the Cybersecurity Information Sharing Act (CISA), and the NIST Cybersecurity Framework. These laws promote the implementation of cybersecurity measures across government agencies and critical infrastructure sectors, including the energy sector.

– Cyber resilience: Cyber resilience encompasses the ability of digital systems, networks, and infrastructure to withstand, adapt to, and recover from cyber threats,

incidents, or disruptions. It involves a proactive and holistic approach that combines cybersecurity measures, incident response capabilities, and business continuity plans to ensure the continuity of critical operations and services.

- Legislation in Europe: In Europe, the term "cyber resilience" is often used instead of "cyber stability." The NIS Directive addresses the need for enhancing the resilience of critical infrastructure, including the energy sector. It sets security and incident reporting requirements to improve the sector's preparedness for cyber incidents.
- Legislation in the USA: In the USA, the concept of cyber resilience is typically incorporated within the broader framework of cybersecurity. The NIST Cybersecurity Framework, for instance, emphasizes the importance of resilience and the ability to recover from cyber incidents, ensuring the stability and continuity of systems and services.

At the same time, the US Department of Homeland Security developed Cyber Resilience Review [11]. The Cyber Resilience Review comprises 42 goals and 141 specific practices extracted from the CERT-RMM and organized in 10 domains [12]:

- 1) Asset Management;
- 2) Controls Management;
- 3) Configuration and Change Management;
- 4) Vulnerability Management;
- 5) Incident Management;
- 6) Service Continuity Management;
- 7) Risk Management;
- 8) External Dependency Management;
- 9) Training and Awareness;
- 10) Situational Awareness.

The introduction of the NIST Cybersecurity Framework into the regulatory framework of Ukraine can potentially help in furthering the implementation of cyber resilience and the use of the Cyber Resilience Review (CRR) methodology. Here's how:

1. Common Framework for Cybersecurity: The NIST Cybersecurity Framework is a widely recognized and respected set of guidelines and best practices for managing and improving cybersecurity risk. It provides a structured approach to cybersecurity that organizations around the world use to enhance their cybersecurity posture. By adopting this framework, Ukraine can establish a common foundation for cybersecurity practices across various sectors and organizations.

2. International Acceptance: The NIST Cybersecurity Framework has gained international acceptance, making it easier for organizations in Ukraine to align their cybersecurity efforts with global standards. This alignment can enhance the country's cybersecurity posture and facilitate international cooperation in addressing cyber threats.

3. Comprehensive Guidance: The NIST Cybersecurity Framework covers various aspects of cybersecurity, including risk management, cybersecurity controls,

incident response, and recovery. It provides a holistic approach to cybersecurity that goes beyond just prevention and includes resilience strategies. This aligns well with the concept of cyber resilience, which emphasizes not only preventing cyber incidents but also preparing for, responding to, and recovering from them.

4. Reference for Cyber Resilience Implementation: The NIST Cybersecurity Framework can serve as a valuable reference for implementing cyber resilience measures. Organizations in Ukraine can use the framework's guidelines to assess their current cybersecurity posture, identify gaps, and develop strategies for enhancing their cyber resilience.

5. Integration with the CRR: The Cyber Resilience Review methodology, developed by the U.S. Department of Homeland Security, is designed to assess an organization's cybersecurity capabilities and readiness. The NIST Cybersecurity Framework can be integrated with the CRR to provide a structured and comprehensive approach to assessing and improving cyber resilience. The framework's guidelines can help organizations address the areas identified during a CRR assessment.

6. Regulatory Alignment: When Ukraine incorporates the NIST Cybersecurity Framework into its regulatory framework, it can require organizations, particularly critical infrastructure providers and government agencies, to adhere to its principles and guidelines. This can help ensure a consistent and high level of cyber resilience across key sectors of the country's infrastructure.

However, it's important to note that the successful implementation of any cybersecurity framework, including NIST, requires a commitment from both public and private sectors, as well as adequate resources and ongoing monitoring and adaptation to evolving cyber threats. Additionally, the regulatory and legal aspects of incorporating such frameworks into a country's laws and regulations need careful consideration.

Overall, adopting the NIST Cybersecurity Framework can be a significant step in enhancing cybersecurity and cyber resilience in Ukraine, but it should be part of a broader cybersecurity strategy that includes education, awareness, collaboration, and ongoing improvement efforts.

1. A year of devastating cyber attacks in Ukraine: how threats attacked users and organizations, URL: <https://www.eset.com/ua/about/newsroom/press-releases/malware/god-razrushitelnykh-kiberatak-v-ukraine-kak-ugrozy-atakovali-polzovateley-i-organizatsii/>.
2. Law of Ukraine on the Basic Principles of Cybersecurity in Ukraine, URL: <https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text> Application date: 15.05.2022.
3. Law of Ukraine on information protection in information and communication systems, URL: <https://zakon.rada.gov.ua/laws/show/80/94-bp?lang=en#Text> (link is external) Application date: 15.05.2022.
4. Resolution of the Cabinet of Ministers of Ukraine on Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects, URL: <https://zakon.rada.gov.ua/laws/show/518-2019-п?lang=en#Text> Application date: 15.05.2022.

5. Law of Ukraine on Critical Infrastructure, URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
6. Order No. 601 dated October 6, 2021 of Administration of the State Service for Special Communications and Information Protection of Ukraine "Methodical recommendations on increasing the level of cyber protection of critical information infrastructure", URL: <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>.
7. NIST Cybersecurity Framework, URL: <https://www.nist.gov/cyberframework>.
8. Resolution of the Cabinet of Ministers of Ukraine "Some issues of conducting an independent audit of information security at critical infrastructure facilities", URL: <https://www.kmu.gov.ua/npas/deiaki-pytannia-provedennia-nezaleznoho-audytu-informatsi-inoi-bezpeky-na-s257-240323>.
9. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast), URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943&from=EN>.
10. Network Code on Cybersecurity Drafting Status, URL: [https://www.entsoe.eu/network\\_codes/nccs/](https://www.entsoe.eu/network_codes/nccs/).
11. Cyber Resilience Review Fact Sheet <https://www.cisa.gov/sites/default/files/c3vp/crr-fact-sheet.pdf>.
12. Cyber Resilience Review: Method Description and Self-Assessment User Guide, URL [https://www.cisa.gov/sites/default/files/publications/2\\_CRR%25204.0\\_Self-Assessment\\_User\\_Guide\\_April\\_2020.pdf](https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf).

## **МОДЕЛЬ КІЛЬКІСНОГО ОЦІНЮВАННЯ СТІЙКОСТІ СИСТЕМИ (РОЗПОДІЛУ ЕНЕРГЕТИЧНИХ РЕСУРСІВ)**

### **Вступ**

Система – предмет дослідження – поєднує елементи із різними властивостями, між ними – певні взаємовідносини, тут завжди є вузькі місця, конфлікти, компроміси тощо, але система діє, забезпечуючи певну функцію, «живе». Зовнішнє оточення атакує систему, неявно чи явно, природно чи керовано за поставленою ціллю, погіршуючи її поточний функціональний стан. Система опирається, намагаючись якнайкраще зберегти функціонал певними внутрішніми змінами, скажімо, зміною організаційної та ресурсної структури, загалом, це процес на виснаження. При цьому одні параметри системи зменшуються, інші, наприклад, вартісні, зростають.

За модельним сценарієм атакуючі дії можна представити поступовими покровоко підсиленими провокаційними діями («сударами»), формуванням відповідних збурень і виявленням реакції вразливих елементів («вузьких місць»), з-за них, зрозуміло, реакції усієї системи як показника її стійкості, звідси – потреба мати кількісну модель оцінювання стійкості системи чи процесу для розуміння, передбачення й формування певних рішень на основі відповідних розрахунків.

### **Підхід**

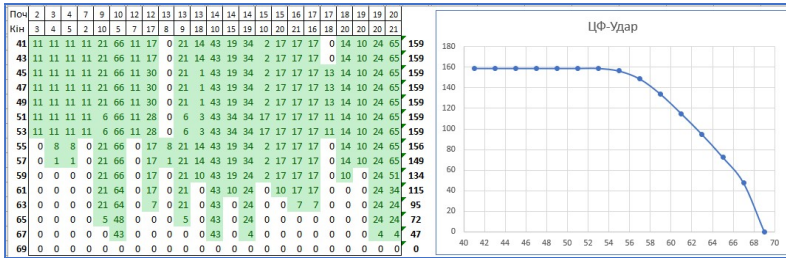
Якщо розробити і застосувати оптимізаційну модель відповідної задачі, де існує апарат аналізу чутливості (значень шуканих змінних оптимального рішення від значень початкових даних), в модель додається вхід зі значеннями ударів, від одного до кількох, що враховується в обмеженні на шукані змінні рішення. Тоді кожна поточна ситуація, що склалася на момент атаки певної інтенсивності, виявивши чергову «слабкість» (у вигляді змінених певних входів), покровоком пошуком оновленого оптимуму (в результаті оптимальної реконфігурації структури) буде відображати стійкий стан системи, модельний процес можна представити відповідною діаграмою. Цей підхід також застосовується при визначенні раціональної програми відновлення відповідної системи, де за покровоко зростаючим певним ресурсом стійкий стан забезпечується найкращим застосуванням ресурсу.

### **Приклад**

Система представлена ненаправленою мережевою структурою (між парами вузлів направлені назустріч чи паралельні дуги), яка дозволяє заданим чином певним вузлам надати статус джерела, стоку чи транзитного пункту, що може застосовано в моделі розподіленої генерації. Використана модифікована модель задачі про максимальний потік, доповнена модулем врахування послідовної атаки і, відповідно, зміною вагових коефіцієнтів для оптимального перерозподілу потоків.

## Тестування мережевої структури

Протокол (атакуючий показник:  $0 \div 69$ ), структура: рядки – кроки, згідно зростання значення показника атаки; стовпці – 69 елементів/дуг, неактивні приховані, останній містить значення ЦФ; елементи – поточні значення дугових потоків, фрагмент:



На кожному кроці циклічного алгоритму: генерується чергове значення сили удару, це значення враховується в правій частині обмеження на шукані значення змінних рішення (decision variables), розв'язується поставлена задача потокової оптимізації, ціль: знайти найкращий розподіл потоків мережею за змінними значеннями входів.

### Аналіз результату

В моделі дві шукані змінні: значення дугових потоків і показника атаки, що входить в праву частину обмеження для шуканих потоків.

Оскільки критерієм оптимізації є максимум цільової функції, значення цих двох змінних визначаються узгоджено задля утримання максимального потоку якнайдовше, значучи, що ціль атаки – нанести шкоду, за цим критерієм черговою «жертвою» атаки вибирається дуга, зменшення ваги якої і наступний перерозподіл потоків нанесуть якнайменшу шкоду. Таким чином, вважаємо, що розв'язок цієї задачі оптимізації за цим критерієм на кожному кроці атаки кількісно оцінює стан стійкості системи, де враховані задані входи і обмеження на шукані змінні, кожен рядок таблиці протоколу – це повна характеристика цього стану у вигляді усіх активних потоків від джерел до стоків.

Якщо для поставленої задачі існує лінійна оптимізаційна модель, кількісна оцінка стійкості досягається завдяки апарату аналізу чутливості, у відповідних предметних показниках.

1. Кузьмичов А.І. Модельне оцінювання та аналіз вразливості взаємозалежних інфраструктур. *Реєстрація, зберігання і оброб. даних*. Щорічна підсумкова наукова конф. 16-17 травня 2019 року: Зб./за ред. В.В. Петрова. К.: ІПІРІ НАН України, 2019. С. 69-71.
2. Додонов О.Г., Кузьмичов А.І. Мережеві організаційні структури управління. Моделювання та візуалізація засобами Excel. К.: Вид-во Ліра-К, 2021. 297 с.
3. Кузьмичов А.І., Чернецька Ю.В., Шестаков В.А. Пошук і аналіз чутливості часових оптимальних планів постачання енергетичних ресурсів із застосуванням надбудови SolverTable // *Реєстрація, зберігання і обробка даних*. 2022. Т. 24. № 2. С. 62-71.

## ОГЛЯД РІВНІВ ЗАБЕЗПЕЧЕННЯ РЕЗИЛІЄНТНОСТІ У ГАЛУЗІ ЕНЕРГЕТИКИ

На сьогодні актуальність поняття «резилієнтності» набуває все більшої ваги, особливо у контексті триваючих атак країни-агресора, у тому числі на енергетичний сектор економіки України – як на рівні фізичному [1], так і на рівні вирішення задач кібербезпеки [2].

Варто, однак, зауважити, що зазначене поняття має дещо відмінні інтерпретації, серед яких вбачається доречним відзначити, зокрема, визначення «резилієнтності», що надається Національною академією наук Сполучених Штатів Америки: властивість досліджуваної системи, що полягає у здатності «підготуватися» до несприятливих подій, планувати такі події, сприймати їх, відновлюватися від наслідків зазначених подій і більш успішно адаптуватися до них [3]. Разом із цим, у наукових публікаціях зазначається, зокрема, потреба у переосмисленні концептуальної складової в основі названого поняття [4, 5], у тому числі з урахуванням мінливості ризиків, а також із наголосом на доцільності опрацювання засад резилієнтності вже на етапі проектування процесу розроблення відповідних систем [6]. Більше того, виокремлюється першорядна важливість забезпечення резилієнтності саме енергетичних систем: при цьому відзначається стрімке зростання відносної частки кіберзагроз, у тому числі як наслідок реалізації концепції «Smart grid» [7].

З урахуванням вищезазначеного, у межах науково-дослідної діяльності Інституту проблем моделювання в енергетиці ім. Г.С. Пухова НАН України проблему забезпечення резилієнтності енергетичного сектору України адресовано, зокрема, у рамках вирішуваних задач проєкту W911NF-22-2-0153 [8]. Окрім цього, у якості суміжного напрямку досліджень, механізми сприяння резилієнтності опрацьовуються також і при вирішенні задач НДДКР № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики», у тому числі шляхом розроблення методів і засобів контролю несуперечності програмно-алгоритмічної складової критичних систем, призначених до застосування при вирішенні задач енергетики [9, 10].

1. Nikolaieva, I., & Zwijnenburg, W. (2022). *Risks and impacts from attacks on energy infrastructure in Ukraine*. PAX report. Dec. 2022. [https://paxforpeace.nl/media/download/PAX\\_Ukraine\\_energy\\_infrastructure\\_FIN.pdf](https://paxforpeace.nl/media/download/PAX_Ukraine_energy_infrastructure_FIN.pdf).
2. Davydiuk, A., & Zubok, V. (2023). Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War. *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia, 121–139. <https://doi.org/10.23919/CyCon58705.2023.10181813>.
3. National Research Council. (2012). *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/13457>.



4. Ganin, A.A., Kitsak, M., Marchese, D., Keisler, J.M., Seager, T., & Linkov, I. (2017). Resilience and efficiency in transportation networks. *Science Advances*, 3(12). <https://doi.org/10.1126%2Fsciadv.1701079>.
5. Linkov, I., & Trump, B.D. (2019). *The Science and Practice of Resilience*. Springer. ISBN 978-3-030-04563-0. <https://doi.org/10.1007/978-3-030-04563-4>
6. Linkov, I. et al. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, 407–409. <https://doi.org/10.1038/nclimate2227>.
7. Jasiunas, J., Lund, P.D., & Mikkola, J. (2021). Energy system resilience – A review. *Renewable and Sustainable Energy Reviews*, 150. <https://doi.org/10.1016/j.rser.2021.111476>.
8. Науковці прийняли участь у виставці в рамках форуму «Безпека критичної інфраструктури та гуманітарна протимінна діяльність». (2023). Retrieved from <https://ipme.kiev.ua/2023/05/18/naukovci-prijnyali-uchast-u-vistavci-v-ramkax-forumu-bezpeka-kritichno%D1%97-infrastrukturi-ta-gumanitarna-protiminna-diyalnist>.
9. Shkarupylo, V., Blinov, I., Dusheba, V., & Alsayaydeh J.A.J. (2023). Case Driven TLC Model Checker Analysis in Energy Scenario. *CEUR Workshop Proceedings*, 3392, 65–75. ISSN 1613-0073. <https://doi.org/10.32782/cm15/3392-6>.
10. Шкарупило В.В., & Душеба В.В. (2023). Щодо аспектів контролю несуперечності програмно-алгоритмічної складової систем критичного призначення. Продовольча та екологічна безпека в умовах війни та повоєнної відбудови: виклики для України та світу: мат. Міжн. наук.-практ. конф., секція 5: Інженерія, енергетика та інформаційні технології в умовах війни та післявоєнній відбудові країни (м. Київ, 25 трав. 2023 р.): тези доп. Київ: НУБіП України, 170–172. [https://nubip.edu.ua/sites/default/files/u381/sekciya\\_5.pdf](https://nubip.edu.ua/sites/default/files/u381/sekciya_5.pdf).

## **РЕЗИЛЬЄНТНИЙ ПІДХІД ДО ПОБУДОВИ РОЗПОДІЛЕНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

На сьогодні інформаційна безпека широкого класу спільнот забезпечується, здебільшого, за допомогою комерційних продуктів, які впроваджуються відповідно до стандартів або нормативних документів, що визначають критерії захищеності інформації для цих спільнот.

Центри зберігання та обробки критичної інформації, канали передачі даних, засоби активної протидії кібератакам централізовані та локалізовані. Впровадження систем забезпечення інформаційної безпеки проводиться директивно, малочисельними групами висококваліфікованих уповноважених осіб. Роль пересічних членів спільноти пасивна і полягає у виконанні приписаних норм і настанов, а рівень залученості та обізнаності в питаннях забезпечення захисту як особистої інформації, так і інформаційного кластера спільноти – досить низький.

Такий підхід виправданий і ефективний для протидії конвенціональним загрозам, ризики яких заздалегідь виявлено та опрацьовано, але недовірливий щодо стохастичних сценаріїв загроз з високим руйнівним впливом.

У відповідь на глобальні виклики, пов'язані зі змінами клімату, епідеміологічною обстановкою та отриманням національними і транснаціональними злочинними угрупованнями доступу до передових наступальних технологій у кіберсфері, пропонується внесення змін до наявної моделі системи забезпечення інформаційної безпеки, які б підвищили її резильєнтність.

Децентралізація сховищ даних і систем інформаційної безпеки, шляхом добровільного розподілу уніфікованих апаратних обчислювальних компонентів між учасниками спільноти – одна з можливих змін.

В якості основних елементів такої розподіленої системи пропонується використовувати компактні захищені комп'ютерні модулі, здатні ініціювати шифровані підключення до подібних об'єктів і серверів керування у широкому діапазоні дротових і бездротових мереж, обмінюватися даними і виконувати синхронізацію для виконання чотирьох основних сервісних функцій:

1. Розподілене зберігання критично важливих даних дає змогу керувати, обробляти великі обсяги інформації, забезпечуючи масштабованість і гарантуючи відмовостійкість [1].

2. Розподілені обчислення [2], які можуть бути використані: у криптографії; для навчання нейромереж, орієнтованих на безпеку; у великих наукових проєктах тощо.

3. Багатовекторні сценарії активної протидії кібератакам і наступальні кібероперації [3], як то: дезорганізація атак противника на основі застосування неправдивих інформаційних об'єктів; вплив на комунікаційну структуру і

структуру даних джерел атак; функціональне ураження засобів атакувальників шляхом отримання контролю над їхніми обчислювальними ресурсами.

4. Екстрене оповіщення та зв'язок із членами спільноти в разі виникнення кризових ситуацій.

Модулі можуть бути розміщені в організаціях, підприємствах і приватних оселях членів спільноти, які відповідають за їхнє збереження, наявність електроживлення та підключення до комп'ютерних мереж, без можливості безпосереднього доступу до програмного забезпечення та даних системи, яка керується компетентними органами.

Додатковим елементом, який може підвищити загальний рівень резильєнтності системи інформаційної безпеки спільнот є розробка та підтримка програмного забезпечення з відкритим вихідним кодом.

Для децентралізованої моделі забезпечення інформаційної безпеки особливо важливими є такі його типи:

1. Антивірусні програми.

2. Сканери вразливостей – програмні засоби, які слугують для здійснення діагностики та моніторингу мережевих комп'ютерів, що дають змогу сканувати мережі, комп'ютери та додатки щодо виявлення можливих проблем у системі безпеки, оцінювати та усувати вразливості.

3. Ханіпоти та Desertion-системи – фейкові ресурси, що мімікують під реальні об'єкти інфраструктури і є приманкою для зловмисників; задача ханіпотів – наразитися на атаку або несанкціоноване дослідження, що дає змогу детектувати вторгнення і вивчити стратегію атакуючого [4].

Ці програмні продукти (рис. 1), встановлені на персональних комп'ютерах членів спільноти, зможуть: по-перше, задовольнити їх базові потреби в кіберзахисті робочих станцій; по-друге, стати джерелом Великих даних (Big Data), які можуть бути використані спеціалізованими неймережами для моніторингу стану інформаційної безпеки спільноти й надання сценаріїв оперативного реагування на загрози, що виникають.

Слід зазначити, що при створенні розподіленої системи, яка забезпечує інформаційну безпеку будь-якої спільноти, надзвичайно важливим є фактор трастоспроможності системи, яка визначається емерджентним поєднанням безпеки, безпечності для користувачів, резильєнтності та приватності для всіх її компонентів [5].

Обов'язковим також є фактор добровільної участі та наявності паритету між інтересами окремих членів спільноти та інтересів спільноти загалом – усі експлуатаційні, часові та моральні витрати мають бути належним чином компенсовані.

Резюмуючи вищевикладене, можна зазначити, що запропонований підхід до побудови розподіленої системи забезпечення інформаційної безпеки фундаментально збільшує її резильєнтність. У разі атаки або знищення окремого модуля або навіть групи модулів, частини системи, що залишилися, продовжують функціонувати незалежно, забезпечуючи збереження важливої

інформації і гаранторздатності критичних функцій, створюючи базу для швидкої адаптації та відновлення.

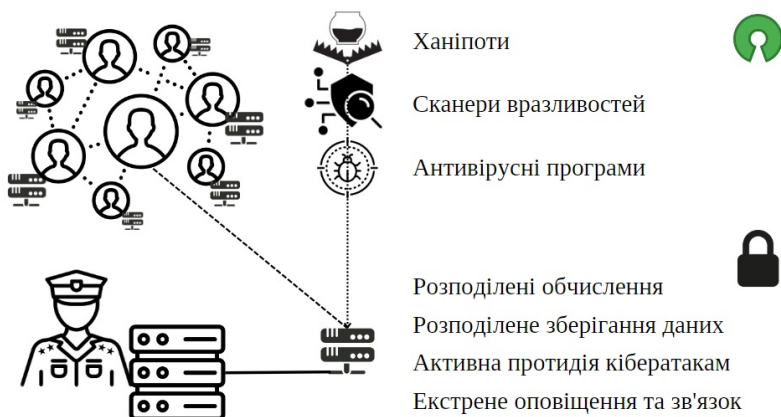


Рисунок 1 – Елементи розподіленої системи

Крім того, інтеграція опенсорсного програмного забезпечення посилює прозорість і довіру до системи, надаючи змогу спільноті брати активну участь у її вдосконаленні.

1. Patel Y.S., Kumar P., Yadav R., Misra R. (2022). Distributed Storage Infrastructure: Foundations, Analytics, Tools, and Applications. In: Chaturvedi, M., Patel, P., Yadav, R. (eds) Recent Advancements in ICT Infrastructure and Applications. Studies in Infrastructure and Control. Springer, Singapore. [https://doi.org/10.1007/978-981-19-2374-6\\_6](https://doi.org/10.1007/978-981-19-2374-6_6).
2. Tanenbaum, Andrew S.; Steen, Maarten van (2002). Distributed systems: principles and paradigms. Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 0-13-088893-1.
3. Eva-Nour Repussard, Offensive cyber operations: understanding intangible warfare, International Affairs, Volume 99, Issue 3, May 2023, Pages 1332–1333, <https://doi.org/10.1093/ia/iiaad071>.
4. Mokube, Iyatiti; Adams, Michele (March 2007). "Honeypots: Concepts, approaches, and challenges". Proceedings of the 45th annual southeast regional conference. pp. 321–326. <https://doi.org/10.1145/1233341.1233399>.
5. NIST Special Publication 800-160, Volume 1. Engineering trustworthy secure systems. (2022). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-160v1r1>.

М.М. Худинцев, І.Л. Палажченко

## ПОКАЗНИКИ ВІДНОВЛЕННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Аналіз рекомендацій з захисту (кіберзахисту) критичної інформаційної інфраструктури [1] свідчить про суттєвий вплив показників відновлення інфраструктури, які можна виділити (відокремити) від інших показників захисту (див. табл. 1).

Таблиця 1 – Показники відновлення критичної інформаційної інфраструктури

Функція захисту	Категорія заходу	Показники відновлення (підкатегорія заходу)	Умовна вага
Ідентифікація (ID)	Управління активами (ID.AM)	ID.AM-0: Перелік та категоризації об'єктів критичної інфраструктури затверджені	1
		ID.AM-1: Інвентаризуються фізичні пристрої та системи в організації	2
		ID.AM-2: Інвентаризуються програмні платформи та додатки в організації	2
		ID.AM-3: Інвентаризуються відокремлені/віддалені підрозділи, організації в сфері управління, персонал	2
	Ділове середовище (ID.BE)	ID.BE-2: Місце організації в критичній інфраструктурі та її галузевому секторі визначається та повідомляється	1
		ID.BE-4: Встановлено залежності та критичні функції для надання критичних послуг	3
		ID.BE-5: Вимоги до відмовостійкості для підтримки надання критично важливих послуг встановлені для всіх робочих станів	3
	Стратегія управління ризиками	ID.RM-3: Визначення організацією стійкості до ризику базується на її ролі в критичній	3

	(ID.RM)	інфраструктурі та аналізі ризиків у певному секторі	
	Управління ризиками ланцюга поставок (ID.SC)	ID.SC-5: Планування реагування та відновлення, а також тестування проводяться разом із постачальниками та сторонніми постачальниками	3
Захист (PR)	Обізнаність і навчання (PR.AT)	PR.AT-1: Усі користувачі проінформовані та навчені	2
		PR.AT-4: Старші керівники розуміють ролі та відповідальність	1
		PR.AT-5: Персонал із фізичної та інформаційної безпеки розуміє ролі та обов'язки	1
	Безпека даних (PR.DS)	PR.DS-7: Середовища розробки та тестування відокремлені від середовища виробництва	1
	Процеси та процедури захисту інформації (PR.IP)]	PR.IP-4: Резервне копіювання інформації виконується, підтримується та тестується	2
		PR.IP-9: Плани реагування (на інциденти та забезпечення безперервності роботи) і плани відновлення (аварійного відновлення) існують і ними керуються	8
		PR.IP-10: Плани реагування та відновлення перевіряються	4
Технології захисту (PR.PT)	PR.PT-5: Механізми відмовостійкості реалізовані для досягнення вимог стійкості в нормальних і несприятливих ситуаціях	1	
Реагування (RS)	Планування реагування (RS.RP)	RS.RP-1: План реагування виконується під час або після події	8
	Зв'язки (RS.CO)	RS.CO-1: Персонал знає свої ролі та порядок дій, коли потрібна реакція	4
		RS.CO-3: Інформація передається відповідно до планів реагування	4

		RS.CO-4: Координація із зацікавленими сторонами відбувається відповідно до планів реагування	4
Відновлення (RC)	Планування відновлення (RC.RP)	RC.RP-1: План відновлення виконується під час або після інциденту	8
	Покращення (RC.IM)	RC.IM-1: Плани відновлення включають отримані висновки	8
		RC.IM-2: Оновлено стратегії відновлення	8
	Комунікації (RC.CO)	RC.CO-2: Репутація після події відновлюється	8
		RC.CO-3: Діяльність з відновлення повідомляється внутрішнім і зовнішнім зацікавленим сторонам, виконавчим і управлінським командам	8

Зв'язок показників відновлювання критичної інформаційної інфраструктури з стійкістю (резильєнтністю) такої інфраструктури описується в рамках моделі локального індексу кібербезпеки [2], показниками якого виступатимуть показники відновлювання критичної інформаційної інфраструктури.

Вимірювання показників індексу здійснюється шляхом експертного оцінювання. У найпростіших моделях індексу використовується дво- або багатобальна система дискретної експертної оцінки з ваговими коефіцієнтами, які дорівнюють 1. Більш складні моделі використовують системи безперервної оцінки та/або змінні (самоузгоджені) вагові коефіцієнти (можливий варіант значень вагових коефіцієнтів наведено у табл. 1).

1. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 06 жовтня 2021 року № 601 <https://cip.gov.ua/services/cm/api/attachment/download?id=42914>.
2. Худинцев М.М., Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог). Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. К.: 2021. 240 с.

## **ЗАПРОВАДЖЕННЯ ЕЛЕМЕНТІВ «DEMAND RESPONSE» ДЛЯ ЗАБЕЗПЕЧЕННЯ НАДІЙНОЇ РОБОТИ ЕНЕРГОСИСТЕМИ УКРАЇНИ ПІД ЧАС ПРОХОДЖЕННЯ ОСІННЬО-ЗИМОВОГО ПЕРІОДУ**

Після пошкодження енергосистеми України внаслідок ракетних атак протягом 2022-2023 рр. виникли проблеми із постачанням електроенергії споживачам як через мережеві обмеження, так і по балансу потужностей в ОЕС України. Під час проходження осінньо-зимового періоду (ОЗП) 2022/2023 більшість споживачів електроенергії України були знеструмленими принаймні 8-10 годин на добу через застосування диспетчерами НЕК «Укренерго» графіків обмежень потужності чи графіків аварійних відключень (далі – ГАВ) для збереження надійної роботи енергосистеми країни. При цьому, обсяги споживання, які заводяться під черги ГАВ, складаються відповідно до [1], та залежать від споживання електричної потужності в годину суміщеного максимуму навантаження ОЕС України в режимний день замірів грудня попереднього року кожного ОСР.

Одним із шляхів забезпечення надійної роботи ОЕС України в такі особливі періоди є управління попитом (англ. Demand Response), під яким розуміється зміна споживання електроенергії її кінцевими споживачами на запит диспетчерської служби, у відповідь на зміну економічних стимулів або коли надійність функціонування електроенергетичної системи є під загрозою.

Управління попитом електричної енергії сьогодні є складовою цифрової трансформації електроенергетики України [2, 3], а необхідність забезпечення такого управління передбачена Концепцією впровадження “розумних мереж” в Україні до 2035 року [4], в якій визначені загальні напрямки впровадження і використання технологій «розумних мереж».

В умовах масштабних руйнувань енергетичної інфраструктури в Україні дефіцит генерації в енергосистемі відчуватиметься у воєнний та післявоєнний періоди. А у періоди зимових максимумів електроспоживання виникатиме потреба у запровадженні графіків почергової подачі електричної енергії.

Для зниження потреби у запровадженні графіків почергової подачі електроенергії необхідно активніше реалізовувати заходи із регулювання рівнів електроспоживання у побутовому секторі. Слід зазначити, що основні заходи регулювання рівнів електроспоживання побутового сектору дієві саме як спосіб уникнення аварійних відключень споживачів. В умовах запровадження графіків почергової подачі електричної енергії попит на електроенергію набуватиме ознак аномальної еластичності, і навантаження заживлених споживачів збільшуватиметься навіть за збільшення вартості електричної енергії. Найбільш поширеними засобами регулювання графіків навантаження побутових споживачів (які, зазвичай не мають складних систем автоматичної зміни потужності за



віддаленим запитом з диспетчерського центру), є зрізання піку електроспоживання та перенесення навантаження на непікові години доби.

До основних способів стимулювання побутових споживачів змінити власний графік електроспоживання відносять:

- інформування населення про дефіцит генерації в енергосистемі та потребу зменшити електроспоживання;
- запровадження тарифів на електричну енергію, які стимулюють побутових споживачів зменшувати електроспоживання у пікові години доби та переносити використання побутових електроприладів на години нічного мінімуму електроспоживання;
- регулювання побутовим споживачем власного графіка електроспоживання як оплачувана послуга для служби диспетчерського управління.

Для забезпечення надійної роботи ОЕС України під час проходження осінньо-зимового максимуму навантажень у 2023-2024 рр., найбільш доцільним, з точки зору витрат часу на реалізацію, є застосування такого способу регулювання споживання, як «Інформування населення про дефіцит генерації в енергосистемі». За умови активного долучення до його реалізації фахівців профільних міністерств (зокрема Міністерства енергетики України та Міністерства цифрової трансформації України), Оператора системи передачі та операторів системи розподілу, за необхідності – органів місцевого самоврядування, можливо у найкоротші терміни реалізувати механізм інформування населення про дефіцит генерації в енергосистемі через застосунок «Дія», та, як наслідок – зменшити кількість застосувань графіків аварійних відключень споживачів при проходженні ОЗП. Доцільним є і запровадження таких методів регулювання електроспоживання, як «Тарифні стимули до зміни графіків електроспоживання» та «Сплачувана послуга зміни електроспоживання», але враховуючи довготривалий період для їх реалізації, вони можуть бути запроваджені у більш тривалій перспективі.

1. ІНСТРУКЦІЯ про складання і застосування графіків обмеження та аварійного відключення споживачів, а також протиаварійних систем зниження електроспоживання (посилання на електронний ресурс: <https://zakon.rada.gov.ua/laws/show/z0151-07#Text>).
2. Кириленко О.В., Блінов І.В., Зайцев С.О., Палачов С.О., Васильченко В.І. Впровадження міжнародних та європейських стандартів для розвитку ОЕС України згідно концепції Smart Grid. Праці Інституту електродинаміки Національної академії наук України. 2022. № 63. С. 5-12. doi: <https://doi.org/10.15407/publishing2022.63.005>.
3. Кириленко О.В., Блінов І.В., Денисюк С.П. Цифрова трансформація енергетики: сучасні тенденції та завдання. Праці Інституту електродинаміки Національної академії наук України. 2023. № 65. С. 5-14 DOI: <https://doi.org/10.15407/publishing2023.65.005>.
4. Концепція впровадження “розумних мереж” в Україні до 2035 року. Розпорядження КМУ від 14.10.2022 р. № 908-р.

## ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

КІ включає об'єкти енергетики, водопостачання, системи транспорту, телекомунікаційні мережі, банківські і фінансові установи, системи охорони здоров'я, аеропорти, мости, газогони тощо [1]. Під час повномасштабної збройної агресії з боку РФ в Україні гостро постає питання забезпечення живучості та резильєнтності критичної інфраструктури (КІ) в Україні неодноразово мали місце порушення у функціонуванні критичних інфраструктур [2].

Взаємна залежність об'єктів КІ зазвичай визначається як множина однаправлених зв'язків між парами об'єктів, зумовлений тим, що зміна стану першого певним чином впливає на функціонування пов'язаного. Взаємозалежність є комбінацією пари таких залежностей. Таким чином, дослідження стану живучості та резильєнтності певного набору вимагає аналізу односторонніх залежностей, які її складають.

Взаємозалежність між об'єктами КІ може призвести до серйозних економічних і фізичних збитків у регіональному, загальнодержавному та навіть у планетарному масштабі. Виявлення та аналіз явних та прихованих зв'язків та залежностей, які існують між елементами КІ є необхідною складовою для розробки стратегій захисту та реагування на загрози живучості та резильєнтності КІ, а також мінімізації руйнівних наслідків деструктивних впливів [3, 4].

В даний момент управління різних галузей критичної інфраструктури окремо один від одного часто перешкоджає аналізувати їх взаємозалежності та ймовірні каскадні ефекти.

Для аналізу взаємозалежності КІ пропонується виділити наступні види залежностей між об'єктами КІ:

- фізичні – характеризують зв'язки, пов'язані з передачею певних ресурсів (електроенергії, сировини, пального, тощо);
- комунікаційні – характеризують зв'язки на рівнях управління, пов'язані з інформаційним обміном;
- геопросторові – відображають відстань між елементами КІ та ймовірність того, що порушення роботи одного об'єкта може вплинути на інші, розташовані поблизу;
- управлінські – характеризують зв'язки прийняття рішень на різних рівнях КІ.

В якості базового інструменту моделювання пропонується використання графової бази даних Neo4j (знання-орієнтованої технології), яка дозволяє досліджувати показники живучості та резильєнтності в моделях КІ шляхом аналізу залежностей та взаємозв'язків між елементами КІ, використовуючи

графові алгоритми [5, 6]. Neo4j використовує резервування графів, усуваючи обмеження на адміністрування та резервування даних за рахунок власне вбудованих механізмів.

На рисунку представлена частина моделі критичної інфраструктури, що включає об'єкти водопостачання, енергопостачання, охорони здоров'я, транспорту та телекомунікацій.

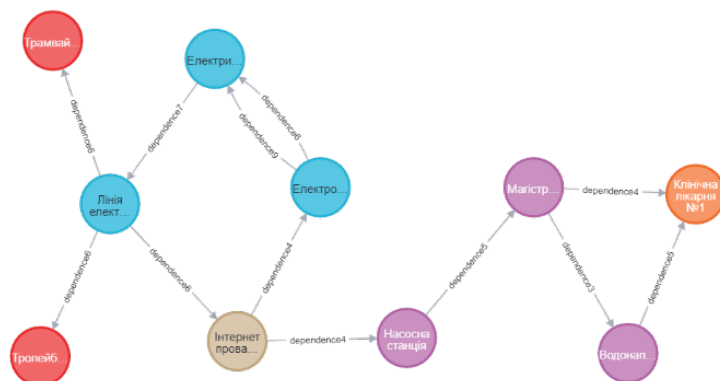


Рисунок 1 – Взаємозалежності об'єктів КІ в базі даних Neo4J

Використання даного підходу дозволяє здійснювати пошук, фільтрацію, агрегацію та аналіз даних, що базуються на явних та неявних зв'язках між об'єктами КІ. Подальші дослідження передбачають розробку моделюючого комплексу для аналізу сценаріїв, що включають впливи на функціонування КІ і визначити недооцінені загрози які можуть призвести каскадних ефектів.

1. Бірюков, Д. С., Кондратов, С. І., & Суходоля, О. (2016). Зелена книга з питань захисту критичної інфраструктури в Україні. ОМ Суходолі. Київ: НІСД.
2. Додонов, О. Г., Горбачик, О. С., & Кузнецова, М. Г. (2022). Підвищення безпеки критичних інфраструктур засобами автоматизованих систем організаційного управління. Реєстрація, зберігання і обробка даних, 24(1), 74-81.
3. Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems*, 6(2), 21.
4. Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. (2022). Systematic review of critical infrastructure resilience indicators. *Construction Innovation*.
5. Chang, V., Songala, Y. K., Xu, Q. A., & Liu, B. S. C. (2022). Scientific Data Analysis using Neo4j. In *FEMIB* (pp. 75-84).
6. Додонов О.Г., Сенченко В.Р., Пуятін В.Г., Бойченко А.В., Коваль О.В. (2023). Методологічні та технологічні аспекти комп'ютерного моделювання сценаріїв прийняття рішень. *Математичні машини і системи*. 2023 – 3, 65-88.

## ЗАПОБІГАННЯ ТА ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД АТАК БПЛА

Безпілотний літальний апарат або просто Дрон, – має більш ніж вікову історію. До початку 21 століття дрони застосовувалися в основному: у військових цілях, перевірки погоди та картографії. Дрони тільки недавно знайшли своє застосування у сфері бізнесу та у побуті. Перші безпілотні літальні апарати з'явилися ще до розвитку літака.

Одні з перших таких апаратів були аеростати, із прикріпленими до них вибуховими пристроями, і після заданого часу – скидали бомби. Вперше ідею застосування таких апаратів запропонував лейтенант австрійської армії Франції під час облоги Венеції.

Після появи технологій радіоуправління можливості безпілотних літальних апаратів збільшилися. Такі літальні апарати застосовувалися для відпрацювання повітряних ударів на площі під час Другої світової війни, яка стала катализатором розвитку ракетної техніки. З'явилися такі знамениті ракети як Фау-1 та Фау-2, які вже на своєму борту мали Автопілот, і були роботами, що літають.

На початку 21 століття завдяки здешевленню електроніки та появи компактних навігаційних приладів, а також розвитку супутникових навігаційних систем, – стало можливим створення недорогих та маленьких безпілотних літальних апаратів. Рік появи комерційних безпілотних літальних апаратів мульті роторного типу, прийнято вважати 2007 рік, коли німецька компанія micoscapsules представила свої власні напрацювання. Їхній апарат зміг здійснювати навігацію за допомогою супутникової навігаційної системи, а також міг автономно виконувати завдання та літати по точках.

Сучасні безпілотні літальні апарати (БПЛА) – включають БПЛА різноманітних розмірів – від великих військових апаратів до маленьких гелікоптерів, що спокійно поміщаються на долоні.

БПЛА включає 4 програмні модулі:

- система управління літальним апаратом, яка дозволяє контролювати літальний апарат та здійснювати дослідження із заданої траєкторії;
- навігаційна система, яка дозволяє зрозуміти та визначити його місце розташування щодо будь-якої системи координат;
- система побудови мапи, яка дозволяє літальному апарату орієнтуватися в невідомих умовах та виявляти об'єкти на шляху прямування;
- система планування маршруту, що дозволяє ефективно та грамотно побудувати маршрут літального апарату, щоб він не зіткнувся з будь-якими об'єктами, а також виконав свою місію максимально ефективно.

Сучасні методи боротьби із БПЛА включають в себе розробку технічної системи (комплексу) протидії. Кожна технічна система (комплекс) захисту ОКІ й

боротьби з БПЛА, як складна система, повинна мати у своєму складі ряд технічних складових (підсистем), поєднаних у єдине ціле.

Кожна складна система складається з підсистем, що мають своє цільове призначення. Умовно, у складі складних технічних систем виділяють за призначенням інформаційну, керуючу, виконавчу підсистеми та підсистему забезпечення. Їх спільна робота і повинна забезпечити ефективну роботу всієї системи захисту ОКІ і боротьби з БПЛА.

Зрозуміло, що кожна з наведених підсистем повинна працювати належним чином, з відповідною ефективністю. Їх розробка та виготовлення потребують певного фінансування та визначають кінцеву вартість всієї складної системи. Аналіз сучасних атак на об'єкти критичної інфраструктури, пов'язаних із застосуванням терористами та ворогом безпілотних літальних апаратів для розвідки, враховує також пошкодження від віддаленої кібератаки по об'єктам критичної інфраструктури [1].

Сучасна робота комплексів протидії БПЛА залежить від вартості знешкодження БПЛА тим чи іншим способом. За результатами оцінки ефективності способів протидії БПЛА доцільним є подальше

порівняння способів за критерієм «ефективність – вартість». Оцінка використання декількох способів протидії зводиться до формування єдиного критерію шляхом згортки цільових критеріїв кожної з підсистем.

Моделювання управління БПЛА, програмування поведінки та напрямку польоту [2] під час атаки на конкретні об'єкти критичної інфраструктури (ОКІ), дозволяє розробити алгоритми дій під різні ситуації ураження ОКІ. Підготовка ОКІ під конкретні сценарії протидії дозволить заздалегідь провести додатковий аналіз системи захисту [3], та вкажіть на слабкі місця що потребують покращення (дублювання), для підвищення резильєнтності систем захисту ОКІ. Резильєнтність системи – це можливість к самовідновленню та ефективному застосуванню наявних ресурсів для продовження виконання роботи, при певних пошкодженнях систем ОКІ [4]. Підвищення резильєнтності системи шляхом модернізації та застосування сучасних технології потребують оперативного та ефективного навчання персоналу.

Аналіз моделювання та врахування роботи засобів боротьби (комплексів) та протидії БПЛА, дозволять розрахувати приблизну собівартість втрат та підготувати рекомендації до існуючих алгоритмів дій (сценаріїв) захисту ОКІ. Підготовка ОКІ до можливих сценаріїв та подій підвищує рівень резильєнтності, але потребує значного навчання для персоналу.

1. Невольніченко А.І., Шарій В.І. Проблематика управління сферою воєнної безпеки. Наука і оборона, No1, 2000.
2. Igor Korobiichuk, Yuriy Danik, Oleksyj Samchyshyn The estimation algorithm of operative capabilities of complex countermeasures to resist UAVs // Simulation: Transactions of the Society for Modeling and Simulation International, 7 August 2018, vol. 95, pp. 569 – 573. DOI: 10.1177/0037549718791264.

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.
4. Невольніченко А.І. Екологічний менеджмент як по фактор підвищення ефективності «системи екологічної безпеки» : реферат, Київ, 2019. 64 с.

## ІЄРАРХІЇ СКОРОЧЕННЯ ДЛЯ ПРИСКОРЕННЯ ОБЧИСЛЕННЯ НАЙКОРОТШОГО ШЛЯХУ

Пошук оптимальних маршрутів між пунктами є фундаментальною проблемою в різних галузях – від логістики до робототехніки. Наприклад, ця задача є ключовою для автономних військових дронів, які повинні швидко знаходити оптимальний шлях до цілі, уникаючи радарів та інших перешкод. Алгоритми пошуку шляху також використовуються в промислових роботах для навігації на виробництві та оптимізації логістичних операцій. Метою даної роботи є аналіз методу ієрархії скорочення та оцінка його ефективності для вирішення задачі пошуку оптимального шляху в складних графах.

Класичні алгоритми найкоротшого шляху, такі як Дейкстри, дозволяють обчислювати найкоротші шляхи від початкової точки, але погано масштабуються на великих графах. Ієрархії скорочення надають потужну техніку попередньої обробки для оптимізації графів для на порядок швидших запитів найкоротшого шляху від точки до точки.

Ієрархії скорочення працюють шляхом систематичного скорочення вершин графа і додавання ребер для збереження відстаней між сусідами [1]. Згорання вершини видаляє її з графа. Між його сусідами додаються короткі шляхи, які "перескакують" через вершину з вагою, що дорівнює найкоротшому шляху через стиснуту вершину.

Стратегічне скорочення вершин згортає граф до розрідженої структури, що містить лише найважливіші зв'язки для глобально оптимальних найкоротших шляхів. Порядок скорочення вершин сильно впливає на продуктивність. Звичайні евристики в першу чергу скорочують вершини з меншим ступенем ребер. Альтернативні розглядають метрики, такі як порядок топологічного сортування.

Після стиснення запиту найкоротшого шляху розширюють лише невелику частину вершин. Пропускаючи скорочені вершини і слідуючи найкоротшим шляхам, простір пошуку можна скоротити з  $N$  вершин до  $O(\log N)$  [2]. Це дозволяє на порядки швидше обчислювати маршрути від точки до точки у порівнянні з неоптимізованими графами.

Побудова впорядкування скорочення та додавання ярликів вимагає значних витрат пам'яті та обчислювальних накладних витрат. Однак ці витрати на попередню обробку амортизуються за рахунок швидших онлайн-запитів. Для статичних графів, таких як дорожні мережі, попередню обробку потрібно виконати лише один раз. Динамічні графи вимагають коригування відповідних ярликів для відновлення оптимальності при оновленні ребер.

Такі варіанти, як ієрархії автомагістралей, підвищують продуктивність, розбиваючи граф на рівні ієрархії перед стисненням. Це фокусує попередню обробку на найважливіших зв'язках. Практична інженерія значно прискорює

попередню обробку і зменшує кількість ярликів за допомогою таких методів, як уникнення надлишкових ярликів.

Методи апроксимації забезпечують компроміси між оптимальністю та швидкістю, що налаштовуються. Обмеження ребер скорочення дає кращу продуктивність запиту ціною потенційно неоптимальних шляхів. Такі методи дозволяють гнучко керувати спектром оптимальності та затримок відповідно до вимог програми.

Ієрархії скорочення відмінно підходять для планування в масивних графах, де традиційні алгоритми дають збої. Застосування варіюються від маршрутизації через континентальні дорожні мережі до пошуку шляхів у відеоіграх на великій місцевості. Мілісекундні швидкості запитів дозволяють швидко реагувати на навігацію і перепланувати в реальному часі в міру зміни середовища.

Незважаючи на концептуальну простоту, ефективне використання ієрархій скорочення вимагає обережності, щоб максимізувати продуктивність і керувати накладними витратами на попередню обробку. Адаптивні та паралельні стратегії обробки допомагають масштабувати масивні графіки. Наближення можуть значно прискорити запити з мінімальною субоптимальністю. Загалом, ієрархії скорочення є незамінним алгоритмічним інструментом для блискавичних обчислень найкоротшого шляху.

Проведений огляд дозволить краще зрозуміти можливості та обмеження цього підходу і визначити оптимальні стратегії його застосування для конкретних практичних задач. Це має важливе значення як для розробки ефективних алгоритмів навігації автономних військових БПЛА, так і для створення швидких систем пошуку оптимального маршруту в громадському транспорті та логістиці. Ґрунтовний аналіз ієрархій скорочення дозволить реалізувати їх повний потенціал у різноманітних практичних застосуваннях.

1. Гайзбергер Р., Сандерс П., Шультес Д., та Деллінг Д. (2008). Ієрархії скорочення: Швидша і простіша ієрархічна маршрутизація в дорожніх мережах. Міжнародний семінар з експериментальних та ефективних алгоритмів (с. 319-333). Шпрінгер, Берлін, Гейдельберг.
2. Абрахам І., Деллінг Д., Гольдберг А.В., та Вернек Р.Ф. (2011). Алгоритм маркування на основі вузлів для найкоротших шляхів у дорожніх мережах. Міжнародний симпозіум з експериментальних алгоритмів (с. 230-241). Springer, Берлін, Гейдельберг.



## **ПІДВИЩЕННЯ СТІЙКОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ШЛЯХОМ ВИКОРИСТАННЯ ЗАХИЩЕНОГО ЗВ'ЯЗКУ**

В умовах дії воєнного стану надзвичайно важливим є забезпечення стійкого функціонування технічних систем, в тому числі тих, що використовуються на об'єктах критичної інфраструктури (КІ). Оскільки для здійснення та управління технологічними процесами на складних об'єктах КІ використовуються комп'ютерні засоби, в тому числі мережеві, питання підвищення показників їх живучості та резильєнтність безпосередньо залежить від здатності до відновлення мережевої інфраструктури [1].

Метою роботи є дослідження технології VPN як засобу побудови захищених комп'ютерних мереж для цифровізованих технічних підсистем об'єктів КІ.

Віртуальна приватна мережа (VPN – Virtual Private Network) є технологією, яка дозволяє створювати захищене з'єднання між абонентами мережі, використовуючи в якості засобу комунікації публічну мережу загального користування, таку як Інтернет. Конфіденційність даних, що передаються через віртуальну приватну мережу, забезпечується криптографічними методами, тобто шляхом шифрування. VPN дозволяє також захистити мережу від несанкціонованого доступу сторонніх осіб.

Під час виконання роботи буде: проведено аналіз поточного стану технології VPN, включаючи основні принципи роботи, архітектуру, протоколи та механізми захисту; досліджено основні проблеми та виклики під час створення стійких комп'ютерних мереж, а також можливі шляхи їх розв'язання за допомогою VPN; виконано проектування макетного зразка VPN-мережі для типової технічної підсистеми об'єкту КІ; проведено порівняльний аналіз і вибір найбільш придатного обладнання та програмного забезпечення; розроблено архітектури мережі та план налаштування засобу VPN; проведено перевірку функціональності, здійснено оцінку показників стійкості отриманого VPN-рішення до різних типів атак, ефективності захисту даних та ресурсів мережі.

Застосування результатів дослідження дозволить підвищити показники живучості та резильєнтності сучасних об'єктів КІ, що використовують комп'ютеризовані, зокрема розподілені засоби обробки та обміну даними.

1. Лисенко С.М., Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія / С.М. Лисенко, В.С. Харченко, К.Ю. Бобровнікова, Р.В. Шука // Радіоелектронні і комп'ютерні системи. – 2020. – Т. 93, № 1. – С. 17-28. doi: 10.32620/reks.2020.1.02.

## ОГЛЯД СУЧАСНИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ РОБОТИ ІЗ 3D-МОДЕЛЯМИ

Актуальність теми 3D-моделювання в сучасному світі обумовлена не лише його широким застосуванням у різних галузях, але й потенційним впливом на розвиток та зміну цих галузей. Наприклад, в медицині 3D-моделі дозволяють точніше планувати та виконувати складні хірургічні втручання, що може покращити результати операцій та зменшити ризик ускладнень. У галузі архітектури та будівництва 3D-моделювання сприяє впровадженню більш точних та ефективних дизайнів споруд, що сприяє збереженню ресурсів та підвищенню стійкості до зовнішніх факторів. Крім того, актуальність 3D-моделювання також пов'язана з потенціалом у вирішенні складних завдань стосовно дизайну продуктів та створення високотехнологічних інноваційних рішень. У контексті наукових досліджень, 3D-моделювання може стати потужним інструментом для візуалізації та аналізу даних, допомагаючи дослідникам отримувати інсайти та розвивати нові методи дослідження.

У комп'ютерній графіці тривимірне моделювання – це процес розробки математичного координатного представлення будь-якої поверхні об'єкта в трьох вимірах за допомогою спеціалізованого програмного забезпечення шляхом маніпулювання ребрами, вершинами та полігонами в модельованому тривимірному просторі. 3D моделі представляють фізичне тіло за допомогою набору точок в тривимірному просторі, які з'єднані різними геометричними об'єктами, такими як трикутники, лінії, криві поверхні і т.д. Майже всі 3D-моделі можна розділити на дві категорії: тверді (визначають об'єм об'єкта, який вони представляють) та оболонкові або граничні (представляють поверхню, тобто границю, а не об'єм об'єкта) [1]. Стадія моделювання полягає у формуванні окремих об'єктів, які потім використовуються у сцені. Існує кілька технік моделювання:

- конструктивна геометрія тіл (constructive solid geometry) – використовує логічні операції (об'єднання, віднімання, перетин) для створення складних об'єктів шляхом комбінування простіших геометричних форм;
- неявні поверхні (implicit surfaces) – використовують математичні рівняння для визначення поверхні об'єкта. Це дозволяє створювати плавні і складні форми, які може бути важко створити з використанням інших методів;
- поверхні розподілу (subdivision surfaces) – використовується для створення деталізованих поверхонь, розділяючи кожен полігон на більшу кількість менших полігонів. Це дозволяє отримати гладку поверхню з дрібних деталей.

Процес створення 3D-моделі поділяється на кілька етапів, кожен із яких відіграє ключову роль у реалізації проєкту [2]:

- концептуалізація;

- розробка основної геометрії;
- модифікація полігонів та топології;
- додавання текстур, кольорів, нормалей та інших деталей;
- рендеринг;
- пост-процесинг.

В тривимірному моделюванні існує три найпопулярніші способи представлення моделі:

1. *Полігональне моделювання (polygonal modelling)* – точки в тривимірному просторі, відомі як вершини, з'єднуються відрізками, щоб утворити полігональну сітку (polygon mesh). Практично всі сучасні 3D-моделі створюються як текстуровані полігонні моделі, оскільки вони є гнучкими і дозволяють комп'ютерам швидко їх відображати. Однак полігони є плоскими і можуть наближено відтворювати криві поверхні лише за допомогою багатьох полігонів [3].

2. *Криволінійне моделювання (curve modelling)* – поверхні визначаються кривими, які контролюються ваговими контрольними точками. Крива слідує (але не обов'язково інтерполує) за точками. Збільшення ваги для точки зміщує криву ближче до цієї точки. Типи кривих включають нерівномірні раціональні B-сплайни (NURBS), сплайни, криві Безьє, та геометричні примітиви.

3. *Цифрове скульптування (digital sculpting)* – відносно новий метод моделювання, який здобув популярність протягом останніх кількох років. Існують три типи цифрового скульптування: переміщення (використовує густу модель та зберігає нові позиції вершин через використання зображення, що зберігає відкориговані позиції), об'ємне скульптування (в основі має воксели схожі можливості з дисплейсментом, але не має проблеми розтягнення полігонів, коли в певному регіоні недостатньо полігонів для деформації) та динамічна тесселяція (ділить поверхню за допомогою триангуляції для збереження гладкої поверхні та дозволяє додавати більш дрібні деталі) [4].

У ролі ілюстрації практичної цінності даної теми може бути вказано можливість створення кросплатформного програмного додатку, призначеного для роботи з тривимірними моделями з метою сприяння розвитку та вдосконалення технологій обробки та візуалізації даних у різних сферах діяльності. Програмний засіб буде забезпечувати широкий спектр функціональних можливостей, необхідних для роботи з тривимірними моделями, включаючи можливість імпорту, експорту, маніпуляції, аналізу та відображення даних на різних операційних системах.

Усе вищезазначене демонструє важливість та потенціал 3D-моделювання як інструмента для досягнення нових досягнень у різних галузях, від покращення медичних процедур до створення більш стійких та ефективних будівельних проектів та досягнення наукових відкриттів. Це свідчить про важливість подальших досліджень та розвитку цієї технології для сприяння прогресу у різних галузях індустрії та науки.

1. 3D modeling [Електронний ресурс] / Вікіпедія – Електрон. дані – Режим доступу [https://en.wikipedia.org/wiki/3D\\_modeling](https://en.wikipedia.org/wiki/3D_modeling) вільний – Назва з екрану.
2. How is a 3D Model of a Product Made? [Електронний ресурс] / Вікіпедія – Електрон. дані – Режим доступу <https://cgifurniture.com/3d-rendering-guide/3d-model-creation-workflow> вільний – Назва з екрану.
3. Polygonal modeling [Електронний ресурс] / Вікіпедія – Електрон. дані – Режим доступу [https://en.wikipedia.org/wiki/Polygonal\\_modeling](https://en.wikipedia.org/wiki/Polygonal_modeling) вільний – Назва з екрану.
4. Digital sculpting [Електронний ресурс] / Вікіпедія – Електрон. дані – Режим доступу [https://en.wikipedia.org/wiki/Digital\\_sculpting](https://en.wikipedia.org/wiki/Digital_sculpting) вільний – Назва з екрану.

## **РОЛЬ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В АВІАЦІЙНІЙ ІНДУСТРІЇ**

Інформаційно-аналітичні системи (ІАС) – це системи, у яких накопичується, обробляється та зберігається великий обсяг інформації як із зовнішнього, так і внутрішнього середовища [1].

Однією з найважливіших ІАС визначаються автоматизовані системи відеоспостереження (АСВ), що використовуються в багатьох суспільних місцях, таких як магазини, банкомати, офіси, аеропорти тощо.

Для ІАС визначають функціональну, структурну та інформаційну живучість [1]. Функціональна живучість автоматизованих систем відеоспостереження характеризується здатністю системи продовжувати працювати та виконувати свої основні функції навіть у випадку виникнення помилок, відмов апаратного забезпечення, атак чи інших небажаних подій. Структурна живучість характеризується здатністю системи виконувати цілі функціонування за умов наявності небажаних впливів за рахунок зміни поведінки системи, наприклад, адаптації [1]. Інформаційна живучість АСВ характеризується здатністю ефективно збирати, обробляти, зберігати та надавати доступ до важливої інформації в умовах можливих загроз, помилок, відмов.

Керувати та підвищувати ефективність показників живучості можна за допомогою впровадження новітніх та перспективних механізмів обробки інформації. Для автоматизованих систем відеоспостереження таким механізмом є технології комп'ютерного зору.

Підвищення живучості систем відеоспостереження за допомогою комп'ютерного зору має високу результативність. Способи підвищення живучості систем відеоспостереження за допомогою комп'ютерного зору може бути досягнуто за допомогою, наприклад, автоматизованого виявлення та аналізу аномалій (використання комп'ютерного зору для автоматичного виявлення аномальних подій або поведінки, які можуть вказувати на порушення безпеки або інші проблеми.), системи виявлення невідомих об'єктів (розробка алгоритмів комп'ютерного зору для виявлення невідомих об'єктів, що може бути важливим для реагування на нові загрози та ситуації), вдосконалення аналізу в реальному часі (використання потужних алгоритмів та обчислювальних можливостей для аналізу відеопотоку в реальному часі, що дозволяє швидко реагувати на події), резервування та обробка відмовостійких даних (розробка механізмів для резервування та обробки даних навіть у випадку відмови деяких компонентів системи, що забезпечує безперебійну роботу).

Використання комп'ютерного зору для гарантії безпеки в авіаційній галузі призвело до значних інновацій в роботі аеропортів і літаків.

Комп'ютерний зір все частіше використовується в аеропортах для обробки багажу. Системи глибокого навчання можуть автоматично зчитувати етикетки за допомогою машинного розпізнавання (оптичне розпізнавання знаків), для ідентифікації їх місцерозташування. Це допомагає підвищити ефективність процесу обробки багажу і знижує ймовірність втрати багажу. Наприклад, рішення BagsID допомагає знаходити окремі багажі за їх унікальними фізичними характеристиками, включаючи мінімальні ознаки, такі як подряпини і вм'ятини. Технологія розпізнавання гарантує захист від шахрайських дій, збереження коштів авіакомпанії, підвищення безпеки [2].

Комп'ютерний зір також можна використовувати спільно з камерами, що встановлені в стратегічно важливих місцях, що дозволить відслідковувати переміщення людей і об'єктів в аеропортах. Інформація і звіти в режимі реального часу дозволяють виявляти потенційні загрози безпеки і підвищувати операційну безпеку.

Варіанти використання для спостереження можуть включати моніторинг потенційних загроз, виявлення покинутих предметів, автоматизоване виявлення вогню та диму, тощо.

Одним з рішень є технологія тепловізійного огляду. Панорамна інфрачервона камера Spunel забезпечує безпеку аеропортів по всьому світу. В таких інфрачервоних системах використовується камера, що постійно обертається, внаслідок чого забезпечується детекція зображення на 360 градусів. Програмне забезпечення Суслоре виявляє і відстежує вторгнення в режимі реального часу, використовуючи зображення. Інфрачервоний датчик Spunel здатний виявити людину на відстані кількох кілометрів у повній темряві, незважаючи на погодні умови.

Компанія HGH Infrared System успішно вирішила проблеми нічного спостереження і охорони периметра периметру регіонального аеропорту середнього розміру Америки. Завдяки надширокому полю зору, дві камери Spunel забезпечують більш повне покриття, ніж десятки інфрачервоних PTZ-камер. А менша кількість камер означає менший час обслуговування та меншу вартість [3].

Програмне забезпечення на основі комп'ютерного зору використовується в аеропортах і для ідентифікації пасажирів. Таке програмне забезпечення, разом з технологією штучного інтелекту, порівнює обличчя пасажира з базою даних зображення попередньо завантажених в систему. Технологія аналізу обличчя використовується для того, щоб спростити процес посадки і гарантувати, що на борт зможуть потрапити тільки пасажирів, які повинні бути на визначеному рейсі. Дана технологія також може використовуватися для ідентифікації підозрюваних злочинців, або осіб, що внесені в списки заборони польотів.

Практичним рішенням такого вдосконалення є технологія DigiYatra, що в 2022 році була впроваджена в аеропортах Індії. DigiYatra – децентралізована мобільна платформа для зберігання посвідчення особистості, де авіапасажирів можуть зберігати свої посвідчення і проїзні документи. Завдяки технології

розпізнавання обличчя вхід пасажирів в аеропорт, зону попереднього огляду і виходи на посадку буде автоматизовано. Цей процес буде значно швидше, оскільки кожному пасажирові буде необхідно менше 3 секунд на кожен контакт. Обличчя пасажира стає його посадковим талоном чи посвідченням особи. Ця технологія також інтегрована з системою контролю авіакомпанії, тому тільки пасажири, що пройшли автентифікацію зможуть пройти контроль [4].

Розглянувши запропоновані концепції ми охарактеризували їх вплив саме на підвищення живучості автоматизованих систем відеоспостереження, проте необхідно розглядати їх негативний вплив.

Зокрема, необхідно зазначити, що впровадження технології DigiYatra в сучасному правовому середовищі може призвести до порушення основних прав користувачів. Він працює на основі технології розпізнавання обличчя, а тому працює з даними, за допомогою яких ідентифікується особистість. Після того, як риси обличчя записані в системі, неможливо дізнатися хто буде мати доступ до таких даних. Розглянута технологія має перспективний потенціал, але ризики для користувача є високими. В Індії, де поширена ця технологія, не діє закон про захист даних. Останній законопроект про захист персональних даних, запропонований Правлінням Союзу вибірково надає широкі повноваження по збору і використанню цифрових персональних даних окремих осіб без їх згоди в "суспільних інтересах" (пункт 18) [5]. Загострює положення те, що відповідно до Закону про інформаційні технології 2000 року управлінські організації можуть збирати інформацію без отримання згоди від джерела інформації для досягнення конкретних цілей [6].

Проблеми з захистом персональних даних можуть виникнути в усіх концептуально схожих розробках, що призводить до висновку, що спершу необхідне посилення правового захисту даних, що ідентифікують особистість. Звичайно, такі розробки значно спрощують стандартні процедури проходження контролю в аеропортах, проте водночас вони не забезпечують надійного захисту персональних даних. Саме тому, розглядаючи впровадження технологій комп'ютерного зору в автоматизовані системи відеоспостереження необхідно вказувати і їх загрозу.

1. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Живучість інформаційно-аналітичних систем: понятійний апарат, моделі аналізу та оцінки. Реєстрація, зберігання і обробка даних. 2007. № 3. Т. 9. С. 61-72.
2. BAGSID. <https://www.bagsid.com/>
3. Detect, track and classify all instructions over 360. <https://hgh-infrared.com/wide-area-surveillance/>
4. National portal of India. A New Digital Experience for Air Travellers. <https://www.india.gov.in/spotlight/digi-yatra-new-digital-experience-air-travellers>
5. The digital personal data protection bill. (2022). [https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022\\_0.pdf](https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf)
6. Ministry of law, justice and company affairs (Legislative Department). (9 June, 2000). <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwxcfmijmuixngudufg buubgubfugbububjxcgfsbdbihbgfGhdfgFHtyyhRtMjk4NzY=>

Р.М. Гамрецький, В.О. Гнатюк

## **РОЛЬ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У РЕЗИЛЬЄНТНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ**

Інформаційно-комунікаційні системи (ІКС) в сучасному світі відіграють ключову роль у функціонуванні багатьох сфер, включаючи бізнес, науку, освіту та суспільство в цілому. Забезпечення резильєнтності цих систем є важливим завданням, а ключовою складовою, яка впливає на їх роботу, є програмне забезпечення (ПЗ) та його якість.

Згідно стандарту ISO/IEC 25010:2011 якість ПЗ визначається набором характеристик, таких як функціональна придатність, ефективність виконання, сумісність, зручність використання, мобільність, безпека, ремонтпридатність та надійність [1]. Однак однією з найважливіших наведених характеристик якості ПЗ є надійність. Надійність ПЗ визначає, наскільки програма виконує свої функції без відмов і помилок у певних умовах експлуатації.

Відсутність відмов і помилок у програмному забезпеченні є ключовою для резильєнтності інформаційно-комунікаційних систем. Відмови можуть призвести до недоступності системи для користувачів, втрати даних або навіть критичних наслідків, особливо в критичних застосунках, таких як медицина, фінанси або транспорт. Збільшення залежності від цих систем робить питання їх резильєнтності критично важливим.

Резильєнтна (resilience) система – це система, яка демонструє здатність до адаптації та відновлення у відповідь на зміни, виклики або негативні впливи в своєму середовищі. Вона здатна витримувати стресові ситуації та реагувати на них шляхом швидкої адаптації до нових умов. Резильєнтні системи також мають здатність відновлювати свою працездатність після відмов, кризових подій або атак.

Ключові характеристики резильєнтних систем включають адаптацію до змін, відновлення після втрат, саморегулювання, стійкість до стресових ситуацій, модульність та заходи безпеки. Ці системи призначені для забезпечення стійкості та надійності у невизначеному середовищі та дозволяють організаціям та системам залишатися продуктивними та функціональними навіть у складних умовах [2].

Якість ПЗ впливає на резильєнтність ІКС наступними способами:

- Забезпечення надійності. Висока якість ПЗ допомагає запобігти багатьом програмним відмовам. Вона включає в себе виявлення і виправлення дефектів, тестування на стійкість та аналіз помилок. Надійне ПЗ є фундаментальною складовою для створення резильєнтної системи.



- Стійкість до відмов. Якість ПЗ впливає на те, наскільки система може стійко витримувати відмови. Планування резервного копіювання та відновлення, реалізація механізмів самовідновлення та регулярне тестування можуть забезпечити стійкість до непередбачуваних обставин.
- Автоматизація і постійна інтеграція. Використання автоматизації та постійної інтеграції дозволяє вчасно виявляти та виправляти проблеми в програмному забезпеченні, що сприяє забезпеченню надійності та відновленню системи.
- Безпека. Якість ПЗ включає в себе заходи безпеки, такі як виявлення і виправлення вразливостей. Висока якість ПЗ допомагає запобігти атакам та порушенням безпеки, що може підвищити стійкість системи.
- Швидкість відновлення. Якість програмного забезпечення впливає на швидкість відновлення системи після відмови. Якщо програмне забезпечення розроблене з урахуванням можливостей автоматичного відновлення, система може швидко відновити свою роботу після відмови.

Якість програмного забезпечення має вагомe значення для резильєнтності інформаційно-комунікаційних систем. Забезпечення високої якості ПЗ допомагає уникнути відмов, забезпечує стійкість до негативних подій та забезпечує безперервну роботу системи які мають безпосередній вплив на резильєнтність системи. Все це робить якість програмного забезпечення важливим фактором для забезпечення успішної роботи інформаційно-комунікаційних систем в сучасному світі.

1. ISO/IEC 25010 (2011). ISO/IEC 25010:2011, Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models
2. Лисенко С., Харченко В., Бобровнікова К., Щука Р. (2020). COMPUTER SYSTEMS RESILIENCE IN THE PRESENCE OF CYBER THREATS: TAXONOMY AND ONTOLOGY. *Radioelectronic and Computer Systems*, 0(1), 17-28. <https://doi.org/10.32620/reks.2020.1.02>.

## СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Сучасні об'єкти критичної інфраструктури стають не лише технологічними досягненнями, а й стратегічними активами, що є основою національної стабільності та кібербезпеки. Забезпечення їхньої захисту та стійкості стає одним з найважливіших національних викликів, що потребує комплексного підходу та глибокого аналізу. В умовах глобальних викликів і загроз, таких як кіберзагрози, природні катаклізми та геополітичні ризики, розуміння поточного стану кібербезпеки та стійкості критичної інфраструктури України є надзвичайно важливим завданням. Метою роботи є висвітлення сучасного стану забезпечення кібербезпеки критичної інфраструктури України та подальших шляхів удосконалення.

Об'єкти критичної інфраструктури є невід'ємною частиною функціонування сучасного суспільства. Їх можна класифікувати за різними критеріями, такими як важливість для національної безпеки, функціональне призначення та вплив на економіку. Основними категоріями критичної інфраструктури в Україні є:

1. *Енергетика*: електростанції, підстанції, газо- та нафтопроводи
2. *Транспорт*: аеропорти, залізничні станції, мости, дороги
3. *Інформаційні технології*: центри обробки даних, телекомунікаційні мережі, інтернет-інфраструктура
4. *Водопостачання та очищення води*: системи водопостачання, водоочисні споруди
5. *Охорона здоров'я*: лікарні, аптеки та медичні заклади [1].

Для ефективного забезпечення кібербезпеки об'єктів критичної інфраструктури необхідно ретельно аналізувати різноманітні загрози та ризики, які можуть впливати на їхню працездатність та безпеку. Серед найважливіших загроз можна виділити:

1. Природні катастрофи: Повені, землетруси, урагани та інші стихійні лиха.
2. Техногенні аварії: Вибухи, пожежі, аварії на транспорті та промислові аварії.
3. Кіберзагрози: Кібератаки на інформаційні системи та мережі.
4. Геополітичні ризики: Конфлікти та геополітичні події, що можуть вплинути на економіку та безпеку.

Після класифікації об'єктів критичної інфраструктури і виявлення потенційних ризиків, необхідно звернути увагу на засади забезпечення їхньої кібербезпеки та стійкості. Безпека критичної інфраструктури це стан захищеності критичної інфраструктури, за якого забезпечуються

функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури [2]. Стійкість об'єктів критичної інфраструктури є однією з найважливіших характеристик їхнього функціонування та кібербезпеки. Поняття стійкості визначається як стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду [3]. Україна, як країна з важливою геополітичною роллю в Східній Європі, стикається з численними викликами та загрозами, які можуть вплинути на стійкість об'єктів критичної інфраструктури. В сучасних умовах це стає особливо актуальним у зв'язку з геополітичними подіями, економічними викликами та кіберзагрозами.

Стан захищеності об'єктів критичної інфраструктури в Україні є постійною та динамічною проблемою, яка розвивається відповідно до змін в геополітичному та технічному середовищі. Для розуміння сучасного стану захищеності можна враховувати такі аспекти:

1. *Законодавство та регуляція:*

Україна має відповідне законодавство та регулятивні акти, які регулюють питання захищеності об'єктів критичної інфраструктури. Однак важливо постійно оновлювати та вдосконалювати це законодавство, оскільки загрози постійно змінюються.

2. *Технічна стійкість:*

Багато об'єктів критичної інфраструктури піддаються модернізації та підвищенню технічної стійкості. Це може включати в себе оновлення систем кібербезпеки, вдосконалення моніторингу та використання новітніх технологій для захисту.

3. *Кіберзахист:*

З підвищенням кібератак, кіберзахист стає однією з найважливіших аспектів захисту об'єктів критичної інфраструктури. Україна активно розвиває свій кіберзахист та співпрацює з міжнародними партнерами у цій сфері.

4. *Управління ризиками та реагування:*

Організаційні заходи, такі як розробка планів дій в надзвичайних ситуаціях, навчання персоналу та системи моніторингу, дозволяють ефективно управляти ризиками та вчасно реагувати на негативні події.

5. *Міжнародна співпраця:*

Україна співпрацює з міжнародними організаціями та партнерами з питань захищеності критичної інфраструктури. Це допомагає обмінюватися досвідом та отримувати підтримку у питаннях кібербезпеки.

Сучасний стан забезпечення кібербезпеки об'єктів критичної інфраструктури України може бути описаний наступним чином:

1. *Геополітичні фактори:*

Україна знаходиться в складній геополітичній ситуації, і це може створювати певні ризики для об'єктів критичної інфраструктури. Геополітичні

конфлікти та напружені відносини з окремими сусідніми країнами можуть впливати на стійкість інфраструктури.

### *2. Кіберзагрози:*

Зростаюча кількість кібератак стають однією з найбільших загроз для інформаційних систем, які обслуговують об'єкти критичної інфраструктури. Україна не є винятком, і кіберзагрози можуть викликати серйозні наслідки для кібербезпеки інфраструктури.

### *3. Техногенні аварії:*

Можливість техногенних аварій на енергетичних підприємствах, транспортних об'єктах, водопостачанні та інших галузях інфраструктури може призвести до серйозних негативних наслідків для безпеки та стійкості об'єктів.

### *4. Надійність і технічний стан інфраструктури:*

Сучасний стан інфраструктури, її технічний стан, рівень обслуговування та регулярна модернізація можуть впливати на її стійкість та безпеку. Наявність застарілої технології обладнання може робити об'єкти вразливими перед різними загрозами.

Загальний стан захищеності об'єктів критичної інфраструктури може бути оцінений як «Вимагає постійного удосконалення». Україна розвиває свої можливості та структури для забезпечення кібербезпеки об'єктів критичної інфраструктури та активно працює над покращенням заходів у цій сфері.

Важливо зазначити, що забезпечення стійкості та захищеності об'єктів критичної інфраструктури є постійним процесом, і його успішність залежить від поєднання різних заходів, координації зусиль та співпраці з міжнародними та національними партнерами [4].

Забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури залишається однією з найважливіших задач для України, і вимагає постійного моніторингу, аналізу та удосконалення заходів безпеки. Законодавство та політика, включаючи Національний план захисту та забезпечення кібербезпеки критичної інфраструктури, грають важливу роль у забезпеченні безпеки та стійкості об'єктів [4].

### **Висновки**

Сучасний стан забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури України свідчить про нагальну та складну проблему, що потребує постійного вдосконалення. Геополітична нестабільність, зростаюча кількість кіберзагроз, енергетичні проблеми та інші аспекти створюють виклики для безпеки та стійкості критичних об'єктів. Необхідно надавати пріоритет питанням кібербезпеки та стійкості об'єктів критичної інфраструктури, оскільки це безпосередньо впливає на національну безпеку та економічний розвиток. Ця проблема потребує спільних зусиль усіх сторін, щоб забезпечити найвищий рівень захисту та готовності перед можливими загрозами.

1. Постанова про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. <https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF/paran17#n17>.

2. Постанова про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України <https://zakon.rada.gov.ua/laws/show/2684-20#n8>.
3. Закон України Про критичну інфраструктуру Із змінами і доповненнями, внесеними Законом України від 18 жовтня 2022 року N 2684-IX [https://ips.ligazakon.net/document/view/t211882?an=0&ed=2022\\_10\\_18](https://ips.ligazakon.net/document/view/t211882?an=0&ed=2022_10_18).
4. Постанова про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури <https://ips.ligazakon.net/document/ KR230825>.

## **ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПІДВИЩЕННЯ ЖИВУЧОСТІ СИСТЕМ БРОНЮВАННЯ АВІАКВИТКІВ**

В сучасному світі авіаперельоти стали невід'ємною частиною життя. Системи бронювання авіабілетів пройшли довгий шлях з моменту своєї появи та впровадження. Спершу використовувались ручні процеси, що включали паперові білети і трудомісткий звіт. Але з появою комп'ютерних технологій в цій галузі відбувся зсув парадигми в сторону автоматизованих систем бронювання. Ця трансформація підвищила обслуговування клієнтів, надаючи доступ в режимі реального часу до інформації про наявність рейсів, тарифи та іншої важливої інформації.

Система бронювання авіаквитків – комп'ютеризована система, що використовується для зберігання і пошуку авіаквитків і транзакцій, а також для надання допомоги у вирішенні різних задач управління авіакомпаніями і задоволення потреб клієнтів від першочергового бронювання до завершення польоту.

Живучість системи бронювання авіаквитків – це її здатність працювати ефективно та надійно протягом тривалого періоду часу, адаптуватися до змін в галузі авіаперевезень (що включає оновлення і вдосконалення системи для впровадження нових технологій для поліпшення користувацького досвіду), виконувати потрібні функції та задовольняти потреби користувачів. Для користувачів, в свою чергу, важлива мобільність, тобто мати доступ до системи з різних пристроїв, що підвищує комфортність користування. Окрім цього, система повинна бути надійною, уникати відмов та забезпечувати стійкість в умовах високого навантаження та обсягів трафіку.

Для забезпечення живучості системи бронювання авіаквитків важливо постійно вдосконалювати її, враховуючи сучасні технологічні та бізнесові вимоги.

Одним з таких покращень є впровадження технології блокчейн, що можуть принести численні переваги, такі як підвищення безпеки, ефективності та довіри. Ось кілька ключових способів, які можна використовувати для впровадження блокчейну в систему бронювання авіаквитків:

1. Система керування квитками на блокчейні: Реєстрація квитків у блокчейні може спростити процес продажу, обліку та перевірки квитків. Кожен квиток може бути представлений у вигляді цифрового активу на блокчейні з унікальним ідентифікатором та всією необхідною інформацією.

2. Смарт-контракти для автоматизації операцій: Використання смарт-контрактів на блокчейні дозволяє автоматизувати операції, такі як відміни або повернення коштів за квитки. Це спрощує обробку випадків, коли пасажери вимушені змінити або скасувати свої плани [1].

3. Ідентифікація та безпека: Блокчейн може служити для безпечного зберігання особистих даних пасажирів та перевірки їхньої ідентифікації.

4. Прозорість цін та тарифів: Розміщення цін та тарифів на квитки в розподіленій мережі блокчейну може забезпечити більшу прозорість та відкритість для пасажирів.

5. Додаткові послуги та програми лояльності: Блокчейн може бути використаний для управління програмами лояльності та додатковими послугами, такими як преміальні програми, нагороди та знижки для пасажирів.

6. Партнерство з іншими гравцями в галузі: Співпраця з іншими авіакомпаніями, агентствами та технологічними компаніями для спільного впровадження блокчейну в систему бронювання авіаквитків може бути ефективним шляхом розвитку цієї ініціативи [2].

Необхідно також враховувати технічні, юридичні та конфіденційні аспекти впровадження блокчейну, а також забезпечити надійну та ефективну інтеграцію цієї технології в існуючу інфраструктуру системи бронювання авіаквитків.

Для впровадження технології блокчейн в систему бронювання авіаквитків використовуються різні платформи з підтримкою оплати за допомогою криптовалюти.

Так, вже у 2014 році авіакомпанія AirBaltic стала першою авіакомпанією в світі, що приймає Bitcoin та інші криптовалюти для покупки авіаквитків. Пізніше, в 2021 році, AirBaltic стала першою в світі авіакомпанією що випустила невзаємозв'язані токени (NFT). До 2021 року таким варіантом оплати скористалось близько 1000 клієнтів, що є невеликим показником, але тим не менш, пасажиром пропонується унікальний варіант оплати. Ціни на квитки вказані в євро. Коли клієнти airBaltic оплачують свій рейс, їх криптовалюта автоматично конвертується в євро по поточному обмінному курсу оператора платіжної системи BitPay [3].

BitPay – глобальний постачальник платіжних послуг, надає найбільш гнучкий спосіб оплати авіаквитків криптовалютою. Дана технологія виступає немов посередником між клієнтом і продавцем. Клієнт реалізує оплату зі свого безпечного платіжного гаманця BitPay. Після чого продавець (авіакомпанія) конвертує платіж в євро, для мінімізації ризику коливань валютних курсів.

Відповідно до статистики на кінець 2022 року дана платформа визначається наступними характеристиками:

1. Обробляє 7 транзакцій кожену секунду.
2. Доступна в 229 країнах.
3. Банкові депозити можливі в 38 країнах.
4. Характеризується успіхом транзакцій на 99.98%.
5. Приймає 16 криптовалют (що складає 70% світового ринку криптовалют) [4].

Для того щоб практично оцінити доцільність впровадження технології блокчейн в системи бронювання авіаквитків необхідно дослідити відгуки авіакомпаній. Отже:

- PrivateFly недавно вказала, що близько 1/5 її річного доходу тепер припадає на платежі в цифровій валюті [5].
- Fast Private Jet також заявила, що третина всіх транзакцій її клієнтів тепер відбувається через інноваційні криптосервіси [6].
- Mirai Flights представила новий сервіс швидкого бронювання авіаквитків з використанням криптовалюти, за допомогою якого клієнти можуть придбати квиток на чартерний рейс в один клік [7].

Примітно, що всі ці авіакомпанії заявляють про значний ріст доходів після впровадження нового способу оплати. За словами представників цих компаній, інтерес до криптовалюти різко зростає.

Відповідно до обраної теми було розглянуто загальні характеристики, що можуть підвищувати живучість системи бронювання авіаквитків, а також практичні відгуки після впровадження технології блокчейн. Загалом, технологія блокчейн відзначається підвищеним рівнем конфіденційності, більшою прозорістю та відкритістю, підвищеним рівнем автоматизації при використанні смарт-контрактів. Це і підтверджують відгуки авіакомпаній, що ввели технологію блокчейн в варіанти оплати. Проте слід враховувати труднощі, які виникають на шляху впровадження цієї технології. Необхідно звертати уваги на технічну складність, адже взаємодія з технологією блокчейн і цифровими гаманцями, для більшості користувачів, є новими функціями і можливостями, які потребують глибокого розуміння і користувацького досвіду. Окрім цього, децентралізована система бронювання квитків все ще знаходиться на стадії становлення, що призводить до обмеженої обізнаності і сприйняття.

1. Alex , Senior Travel Tech Advisor at GP Solutions, Blockchain in Travel: Prospects and Achievements. (2022), <https://www.software.travel/blog/automation/blockchain-in-travel>.
2. South Florida Caribbean News. (2023, July 22). Blockchain Revolutionizes Airline ticketing. Retrieved from <https://sflcn.com/blockchain-revolutionizes-airline-ticketing/#:~:text=Enhanced%20Transparency%20and%20Security,by%20using%20distributed%20ledger%20technology>.
3. airBaltic Bitcoin payments extended by various crypto currencies. (2021, March 29). <https://www.airbaltic.com/en/airbaltic-bitcoin-payments-extended-by-various-crypto-currencies>.
4. BitPay. Cryptocurrency Statistics, Charts & Trends. <https://bitpay.com/stats/>.
5. Bit by Bitcoin: PrivateFly says nearly 20% of its sales are paid by cryptocurrency as it launches new Bitcoin Jet Account. <https://www.privatefly.com/press-releases/bit-by-bitcoin-nearly-20-per-cent-sales-bitcoin-jet-account.html>.
6. Businesses that accept Bitcoins? Fast Private Jet confirms its leadership in the crypto flight market. (2021, December 31). <https://www.fastprivatejet.com/en/blog/businesses-that-accept-bitcoins>.
7. Mirai Flights Integrates CoinsPaid’s Crypto Payments Solutions – CryptoProcessing. (2022, December 12). <https://www.supercryptonews.com/mirai-flights-integrate-coinspays-crypto-payments-solutions-cryptoprocessing/>.



М.М. Ларін

## **КАЛЬКУЛЯТОР ШКОДИ НА ОСНОВІ ДАНИХ О ВРАЗЛИВОСТЯХ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА**

Розвиток сучасних підприємств неможливий без інтеграції інформаційних технологій. На жаль окрім переваг інформаційні технології мають і недоліки. Для оцінки шкоди потрібно розробити спеціальне ПЗ яке допоможе попередити про можливі збитки.

Калькулятор шкоди на основі даних о вразливостях інформаційного забезпечення підприємства, являє собою програмний модуль, який за рахунок послідовного експертного оцінювання здатен знаходити чисельне представлення рівня шкоди, від реалізації загрози.

### **Процес створення**

Розглянемо процес створення калькулятора шкоди поетапно:

- по-перше, розглянемо методологію побудови оцінки;
- по-друге, розглянемо програмну реалізацію калькулятора шкоди.

Калькулятор шкоди на основі даних о вразливостях інформаційного забезпечення підприємства створено на основі наступної методології оцінювання:

Оцінювання відбувається за 4 етапи:

1. На першому етапі ми робимо оцінки важливості власників бізнес процесів відносно один одного. (Приклад: ІТ відділ та відділ продажів). Оцінка відділу являє собою суму відносних оцінок власників (табл. 1).

2. На другому етапі ми робимо оцінку важливості бізнес процесів для власників процесів. (Приклад: процес продаж та процес обслуговування клієнтів). Оцінка бізнес процесу являє собою суму експертних оцінок бізнес процесу множених на відповідні оцінки власників (табл. 2).

3. На третьому етапі ми робимо оцінку важливості активів для функціонування бізнес процесів. (Приклад: веб-сервер та оборотні активи). Оцінка активу являє собою суму експертних оцінок активів множених на відповідні оцінки бізнес процесів (табл. 3).

4. На четвертому етапі ми робимо оцінку шкоди для активу від загрози. (Приклад: DDoS атаки та повінь). Оцінка шкоди являю собою суму експертних оцінок шкоди від загрози множених на відповідні оцінки активів (табл. 4).

Таблиця 1 – Приклад першого етапу оцінювання

Назва відділу	ІТ	Відділ продажів	Оцінка власника
ІТ	1	5	1.5
Відділ продажів	0.2	1	1.2

Таблиця 2 – Приклад другого етапу оцінювання

Назва відділу / Назва бізнес процесу	ІТ (1.5)	Відділ продажів (1.2)	Оцінка бізнес процесу
Процес продаж	2	10	15
Обслуговування клієнтів	2	4	7.8

Таблиця 3 – Приклад третього етапу оцінювання

Назва бізнес процесу / Назва активу	Процес продаж (15)	Обслуговування клієнтів (7.8)	Оцінка активу
Веб-сервер	4	4	91.2
Оборотні активи	8	1	127.8

Таблиця 4 – Приклад четвертого етапу оцінювання

Назва активу/ Назва загрози	Веб-сервер (91.2)	Оборотні активи (127.8)	Оцінка загрози
DDoS	8	1	857.4
Повінь	2	2	438

Перші три етапи потребують експертної оцінки для кожного окремого підприємства, проте на четвертому етапі можна використовувати бази даних вразливостей, які мають чисельні значення для рівня шкоди та можливості реалізації загрози. Прикладом такої бази може бути CVE [1].

Для програмної реалізації модуля була обрана мова програмування Python 3.10 [2] з використанням загальнодоступної бібліотеки PyQt5 [3] для користувацького інтерфейсу та візуалізації результатів оцінювання.

### Висновки

За результатом розробки ми маємо готовий програмний модуль, за допомогою якого експерт може проводити оцінювання шкоди від реалізації загроз та вразливостей підприємства.

Корисною властивістю розробленого калькулятора є можливість ефективного визначення пріоритетних загроз підприємства та загальна оцінка загрози відносно вразливих точок підприємства. Також можна виділити наступні можливості калькулятора:

- знаходити вразливі точки підприємства;
- визначати пріоритетні загрози;
- раціонально розподілити ресурси на забезпечення безпеки;

- провести загальну оцінку безпеки підприємства;
  - проводити порівняння різних баз даних загроз та визначити ту, яка найбільше підійде до підприємства;
  - проводити порівняння результатів оцінювання за різні періоди;
  - оцінити потенціальні збитки від загроз, як фінансові, так і репутаційні;
  - покращити звітність по загрозам.
1. CVE (2023, 25 вересня) Інформаційна сторінка CVE [https://cve.mitre.org/cve/data\\_sources.htm](https://cve.mitre.org/cve/data_sources.htm).
  2. Python-3.10 (2023, 25 вересня) Інформаційна сторінка релізу Python 3.10 <https://www.python.org/downloads/release/python-3100>.
  3. PyQt5 (2023, 25 вересня) Інформаційна сторінка релізу PyQt5 <https://pypi.org/project/PyQt5>.

## ІНСТРУМЕНТИ ЗАХИСТУ ВІД XSS-ВРАЗЛИВОСТЕЙ

В умовах швидкого розвитку мережі Інтернет, доступ до неї з'являється все у більшій кількості людей. Такий попит призвів до появи безлічі різних веб-застосунків, які отримали широке поширення, та стали підвищувати якість життя користувача. Але, у свою чергу, ці послуги все частіше стають об'єктом кібератак, оскільки вони є можливою точкою доступу до конфіденційної інформації та баз даних, а через велику кількість різних вразливостей, існує безліч атак, що можуть призвести до різних збитків.

Однією з найпоширеніших наряду із ін'єкцією зовнішніх сутностей XML (також відому як XXE), SQL-ін'єкцією та іншими, є атака міжсайтового скриптингу (XSS). Тому дослідження інструментів захисту від XSS-вразливостей, є актуальною задачею кібербезпеки і саме їй присвячена дана робота

XSS-атаки дозволяють зловмиснику впроваджувати шкідливі скрипти в браузері жертви, що призводить до різних побічних ефектів, таких як: компрометація даних, крадіжка cookies, паролів, номерів кредитних карток, навіть розповсюдженню шкідливого коду. Хоч на сьогоднішній день було запропоновано вже багато методів захисту від даної вразливості та її виявлення, а дослідження з цієї теми ведуться постійно, насправді дуже складно впоратися з усіма різновидами XSS-атак. У 2023 році ця атака залишається у рейтингу десяти найголовніших загроз веб-безпеці за версією Open Web Applications Security Project (OWASP) [1].

Атаки міжсайтового скриптингу (XSS) – це тип ін'єкцій, при яких шкідливий код впроваджується у вразливі веб-сайти. XSS-атаки виникають, коли зловмисник використовує веб-додаток для відправки шкідливого коду, зазвичай у вигляді сценарію на стороні браузера, іншому кінцевому користувачеві.

Недоліки, які дозволяють цим атакам бути успішними, досить широко поширені та виявляються скрізь, де веб-додаток використовує введення даних від користувача в генерованих ним результатах без їх перевірки чи кодування. Зловмисник може використовувати XSS для відправки шкідливого скрипту нічого не підозрюючому користувачеві.

Браузер кінцевого користувача не має змоги дізнатися, що скрипт не заслуговує на довіру, й виконує його. Оскільки передбачається, що сценарій прийшов із довіреного джерела, шкідливий сценарій може отримати доступ до будь-яких файлів cookie, маркерів сеансу або іншої конфіденційної інформації, збереженої браузером та використовується на цьому сайті. Ці сценарії можуть навіть переписати вміст HTML-сторінки.

Виділяють три основні типи XSS-вразливостей:

1. Постійний (збережений) XSS – «найбільш руйнівний тип атак, що

передбачає зберігання шкідливого коду на сайті або сервері, при цьому кожне звернення до оригінальної сторінки виконує у браузері впроваджений код. Класичним прикладом такої форми вразливості є форуми, на яких можна залишати коментарі в HTML-форматі без обмежень. При здійсненні некоректної фільтрації вхідні дані зберігаються в базі даних на сервері або записуються у файли, що виводяться у браузер користувачеві» [2].

2. Непостійний (відбитий) XSS – варіант атаки, що використовує користувачів, які надають у рядку запиту або HTML-форми дані для створення відповіді клієнту без обробки. При цьому користувачеві необхідно перейти по спеціально згенерованому посиланні.

3. XSS у DOM-моделі (Document Object Model) – реалізується через не програмний інтерфейс, що не залежить від платформи та мови програмування, який надає програмам та сценаріям «доступ до вмісту HTML та XML-документів і змінює їх вміст, структуру та оформлення» [3]. Прикладом даної вразливості служить «сценарій, який отримує дані з URL через «location.\*DOM» або за допомогою запиту XMLHttpRequest-запиту і використовує їх без фільтрації для створення динамічних HTML-об'єктів» [4].

Захист від XSS-вразливостей, якщо наприклад використовувати таку мову програмування як JavaScript може бути здійснений за допомогою використання функції «htmlspecialchars()» або її аналога «htmlentities()». Багато авторів вказують, що в HTML існують сутності або мнемоніки, що передбачають написання певної послідовності символів у HTML, наприклад «&copy;». При цьому браузер відобразить символ, що відповідає цій мнемоніці, наприклад, знак копірайту «©» [3].

При запуску функції «htmlspecialchars()», деякі символи (лапки, кутові дужки тощо) у рядку замінюються на відповідні їм мнемоніки, браузер при таких умовах виводить даний рядок на екран як рядок, не намагаючись виконувати його як код. Коли у форму на сайті вводиться текст «<script>alert('hello')</script>», функція «htmlspecialchars()» перекладає його в «&lt;script&gt;alert('hello')&lt;/script&gt;», при цьому браузер виведе на екран перетворений рядок, не сприйнявши такий код як JavaScript.

Проаналізувавши думки деяких фахівців з комп'ютерної безпеки, можна сформулювати правило, що дозволяє значно знизити ймовірність XSS-вразливостей: «всі дані, надані користувачем, потрібно передавати до DOM виключно у вигляді рядків» [4]. Але при цьому дане правило функціонує не у всіх додатках, так як у багатьох з них є функції, що дозволяють користувачам передавати дані в DOM. [3]. Правило можна конкретизувати як: «необхідно заборонити передачу в DOM надісланих користувачем даних, що не пройшли очищення».

Існують способи перевірки правильності інтерпретації даних, переданих у DOM, «як у клієнта, та у і за сервера» [2]. Багато авторів вказують, що розпізнавання рядків у JavaScript відбувається наступним чином: «const isString = function(x) {if (typeof x === 'string' || x instanceof String) {return true;} return false;};» [5].

Для перевірки правильності інтерпретації даних необхідно віднести числа до об'єктів, що нагадують рядки (string-like). Також можливо скористатися невідомим побічним ефектом функції: «JSON.parse(): const isStringLike = function(x){try {return JSON.stringify(JSON.parse(x)) === x;} catch (e) {console.log('not string-like'); } }»

Вбудована функція JavaScript «JSON.parse()» перетворює текст на об'єкт JSON. Зробити таке перетворення можливо для чисел та рядків, але складні об'єкти, такі як функції, не відповідають формату, сумісному з JSON, а значить, для них таке перетворення неможливе.

Другим способом виступає вивчення коректності інтерпретації рядкового об'єкта, що нагадує рядок, оскільки дані об'єкти можуть помилково інтерпретуватися функцією DOM як елементи або перетворюватися на них. Найчастіше дані користувачів впроваджуються в DOM за допомогою елементів «innerText» або «innerHTML». Але безпечніше використовувати «innerText», тому що він передає на очищення все, що виглядає як HTMLтег, представляючи його у вигляді рядка: «const userString = '<strong>hello, world!</strong>; const div = document.querySelector('#userComment'); div.innerText = userString;»

На думку відомого дослідника безпеки веб-застосунків Ендрю Хоффмана використання при додаванні рядків або схожих на рядки об'єктів у DOM елемента «innerText» замість «innerHTML» – оптимальна практика. Елемент «innerText», переглядаючи HTML-теги як рядки, виконує їх очищення, тоді як елемент «innerHTML» при завантаженні в DOM інтерпретує теги HTML як теги [6]. Але, на нашу думку оскільки у кожного браузера існує свій варіант реалізації введеної інформації, то елемент «innerText», що навіть пройшов обробку, помилково вважати повністю безпечним.

Таким чином, визначено, що ризик XSS можна зменшити в мережі або базі даних клієнта, при цьому ідеальним напрямом докладання зусиль буде клієнт, оскільки XSS-атаки зазвичай здійснюються за клієнта. Виявлено, що для запобігання реалізації всіх трьох типів XSS-вразливостей можна використовувати суто програмні методи, при цьому створений код повинен формувати централізовану функцію, яка буде автоматично додавати дані в DOM для всього додатку загалом.

1. The OWASP Foundation (2023, 10 april). The Ten Most Critical Web Application Security Risks. <https://owasp.org>.
2. Wang Q. et al. (2022). Black-box adversarial attacks on XSS attack detection model. *Computers & Security*. 11(3).1025-1028.
3. YongHao Li. Cross-Site-Scripting (XSS) – Attacking and Defending. [https://www.theseus.fi/bitstream/handle/10024/13013/Li\\_Yonghao.pdf?sequence=1](https://www.theseus.fi/bitstream/handle/10024/13013/Li_Yonghao.pdf?sequence=1).
4. Kaur, Jasleen, Urvashi Garg, and Gourav Bathla. (2022).Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review. *Artificial Intelligence Review*. 12(2). 1-45.

5. Gupta S., Gupta B.B. (2017) Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management*. № 1.512-530.
6. Hoffman A. (2020). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications* – Softcover. O'Reilly Media.

## ВИКОРИСТАННЯ СПАМУ ЯК СПОСОБУ ПОШИРЕННЯ ПРОПАГАНДИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Зі стрімким розвитком інформаційних технологій у всьому світі також розвиваються пов'язані з ними загрози. Якщо раніше пропаганда поширювалась шляхом промов, друкованих видань, то в сучасному світі існує безліч нових способів поширення певних наративів, зокрема, спам.

Спам – це надмірне надсилання небажаної або невідомої інформації, такої як комерційні пропозиції, рекламні повідомлення або шкідливий вміст, на адреси електронної пошти чи інші засоби зв'язку без згоди чи інтересу одержувачів. Це нав'язлива практика, яка часто спрямована на використання ресурсів інших осіб без їхньої згоди і може завдати шкоди як особистій приватності, так і безпеці користувачів Інтернету.

Загалом термін "спам" набув загальної популярності у 1994 році, коли два американських юристи розіслали велику кількість небажаних повідомлень на електронні адреси, де вони намагалися просунути свої послуги [1].

Існує багато визначень поняття пропаганда, оскільки це явище не нове та протягом століть розвивається, змінюється та потребує постійного дослідження.

Пропаганда відрізняється від звичайного спілкування і вільного обміну ідеями чи інформацією умисністю і акцентом на маніпуляції. У пропагандиста є конкретна мета, щоб досягти її, він навмисно відбирає факти, аргументи і символи та подає їх так, щоб досягти найбільшого ефекту [2].

В соціальних мережах практика використання спаму в коментарях, приватних повідомленнях чи у блогах є поширеним явищем в кількох причин (рис. 1):

1. Можливість досягнення великої аудиторії: Соціальні мережі привертають мільйони користувачів із всього світу, що створює умови для поширення повідомлень пропагандистами серед аудиторії різного масштабу.



Рисунок 1 – Причини поширення пропаганди в соціальних мережах

2. Зручність розповсюдження інформації: У соціальних мережах дуже легко ділитися постами, відео, зображеннями та іншими видами контенту, що



робить їх ідеальними для поширення пропаганди. Особливості поширення інформації в соцмережах – швидкість комунікаційного обміну, відсутність просторово-часових обмежень, позірна масштабність аудиторії, фільтрація інформації – посилюють вплив на користувача. Повідомлення в соцмережах поширюються на сторінках медіаресурсів, за якими користувач обрав стежити; шляхом розсилки новин від спільноти, до якої користувач долучився за власним вибором, або ж безпосередньо від користувача до користувача, який є другом або фоловером. З психологічної точки зору користувач сприймає свою сторінку як особистий простір, що обумовлює апіорі вищий рівень довіри до одержуваної в мережі інформації, ніж з інших джерел [3].

3. Можливість анонімності. Деякі пропагандисти можуть діяти анонімно або використовувати фейкові профілі, що робить їхню діяльність важкозрозумілою та ускладнює виявлення.

Отже, в розвитку технологій також розвиваються загрози з якими користувачам інтернету, зокрема соціальних мереж, доводиться стикатись щодня. Поширення пропаганди через спам у соціальних мережах зручний спосіб для досягнення великої аудиторії зі збереженням анонімності відправника. Важливо фільтрувати інформацію навіть із тих джерел, які користувач може вважати вартими довіри, а для цього необхідно розробляти системи виявлення спаму у соціальних мережах з використанням сучасних методів, зокрема методів машинного навчання.

1. Templeton B.: n.d.b, Origin of the term "spam" to mean net abuse, <http://www.templetons.com/brad/spamterm.html>.
2. Шведа Ю.Р. Політичні партії. Енциклопедичний словник. Львів. Астролябія, 2005, [https://books.google.com.ua/books?id=Dm2BEAAAQBAJ&printsec=frontcover&hl=uk&source=gbs\\_atb#v=onepage&q&f=false](https://books.google.com.ua/books?id=Dm2BEAAAQBAJ&printsec=frontcover&hl=uk&source=gbs_atb#v=onepage&q&f=false).
3. Золотар О.О. Пропаганда в соціальних мережах – загроза інформаційній безпеці держави, [https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/6139/1/konf\\_04\\_04\\_2019.pdf#page=48](https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/6139/1/konf_04_04_2019.pdf#page=48).

## РЕЗЕРВНЕ КОПІЮВАННЯ КРИТИЧНИХ ДАНИХ КОРПОРАТИВНИХ ЗАСТОСУНКІВ

Умовно користувачів комп'ютерних систем можна розділити за ознакою – користувачі, які не витрачають час на резервне копіювання і ті, хто вже знає навіщо це робити. Це відома інтернет байка, але і дійсно, навіщо люди витрачають час і ресурси на цю проблему? Сформулюємо задачу в цілому але спочатку зробимо аналіз які системи резервного копіювання вже є. Корпоративні клієнти використовують різноманітні операційні системи, серед яких вагома частина належить ОС Windows. Тому приділимо більше уваги саме таким системам.

Для зберігання резервних копій використовуються різні носії. Найчастіше – жорсткі диски і твердотільні накопичувачі (HDD і SSD) в складі різних спеціалізованих пристроїв (RAID-масивів і т.д.). Фірма Microsoft наполегливо рекомендує хмарні сховища. Можна, звичайно, використовувати інші носії, такі як DVD або накопичувачі на магнітній стрічці. Але у багатьох із них є істотні недоліки.

Сайт програми для резервного копіювання (mojo.ua) [1] пропонує нам огляд 10 програм: Redo Backup and Recovery, EASEUS Todo Backup Free, Cobian Backup, Aomei Backupper, Macrium Reflect Free, Paragon Backup & Recovery, BackUp Maker, Action Backup, DriveImage XML, Everyday Auto Backup. За інформацію авторів ресурсу вони, переважно, орієнтовані на відновлення комп'ютера, коли не завантажується Windows. Інші – на періодичне резервування особистої інформації. Всі розглянуті версії – безплатні, багато хто має платні аналоги з додатковими функціями. Проаналізуємо функціональне призначення деяких з них.

### **EASEUS Todo Backup Free [2]**

У версії програми, яка є вільному доступі, реалізовані наступні можливості:

- резервування/реанімація дисків та їх частин;
- реанімація з резервної копії пошкоджених системних розділів Windows на вихідному або іншому носії;
- вибір рівня компресії резервних копій;
- затирання інформації на диску;
- клонування дисків, обраних розділів, перенесення Windows на інший носій;
- створення передзавантажувального середовища для реанімації Windows, яка не завантажується;
- резервування у хмару;
- створення реанімуючого диска;
- перекидання на інший комп'ютер з ідентичним залізом.

Програма підтримує 3 види архівування:

1. Повний. Щоразу все перезаписується заново.

2. Інкрементний. Починаючи з другого резервування, бекаються (відбувається резервна копія даних) тільки файли, які змінились та нові.

3. Диференціальний. Аналог інкрементного методу, відмінності – більше копій та місця на диску, відновлення відбувається швидше.

### **Cobian Backup [3]**

Програма зроблена для регулярного резервування інформації у комп'ютері під Windows. Завантажувальні диски Cobian не створює, зате можна налаштувати автоматичне копіювання потрібних тек. Існує навіть вивантаження по FTP, що нетипово для безплатного ПЗ. Можна вибрати резервування зі стисненням або без, перший варіант передбачає додаткове навантаження на апаратні засоби.

Утиліта встановлюється у вигляді програми або служби. Програма має десяткі регульованих параметрів. Що зручно але потребує часу для навчання.

### **Aomei Backupper [4]**

У функції продукту компанії Aomei входить:

- резервування та відновлення дисків Windows, розділів, окремих файлів;
- починаючи з 5-ої версії, для користувачів безкоштовного програмного забезпечення доступна технологія Universal Restore, що дозволяє переносити Windows на інший комп'ютер;
- можна робити повне, інкрементне, диференціальне копіювання; запускати бекап Windows, не припиняючи роботу з документами, різними програмами; вибирати ступінь компресії копій (нульова, середня, висока);
- клонування дисків / розділів;
- синхронізація файлів.

### **BackUp Maker [5]**

Ця утиліта корисна коли потрібно налаштувати тільки резервування тек у Windows. В ній логічний інтерфейс та зрозумілий алгоритм налаштування:

- вибираємо теки для резервування;
- встановлюємо фільтри файлів, якщо це необхідно;
- вибираємо час початку копіювання або пов'язуємо старт бекапа з системною подією (запуск ОС, вихід з неї, з'єднання з флеш-накопичувачем);
- визначаємося з нюансами копіювання;
- вибираємо місце зберігання бекапа (на цьому ж комп'ютер або відправляти по FTP);
- налаштовуємо присвоєння копіям імен.

Після налаштування бекапа програма у фоновому режимі з потрібною періодичністю буде створювати копії у форматі zip. На архів можна поставити пароль. Існує можливість задати поділ бекапа на частини.

Варто додати до цього аналізу програму **Commvault Complete Backup & Recovery** [6]. Вона створює резервні копії та архівує дані з фізичних та віртуальних серверів, хмарних та гібридних середовищ, настільних комп'ютерів та ноутбуків і навіть корпоративних мобільних пристроїв. Рішення підтримує більшість операційних систем, застосунків і баз даних (Documentum, Oracle, MySQL, SAP, Microsoft), віртуальні і хмарні середовища (AWS, Microsoft Hyper-V, Red Hat Virtualization, VMware і багато інших). Під час процесу резервного копіювання дані автоматично дедуплікуються, як у джерела, так і на резервних серверах. Такий підхід значно знижує навантаження на мережу і економить місце для зберігання. Рішення дозволяє створювати резервні копії і «знімки» додатків і налаштувань обладнання без перебоїв і з мінімальним навантаженням на систему.

На основі цієї вибірки можна визначити що резервне копіювання потрібне для відновлення після збоїв дисків операційних систем, розділів та окремих файлів. Це може здійснюватися в автоматичному або ручному режимі, фоново або під час паузи в роботі системи. Розрізняють повне, інкрементне та диференціальне копіювання. На базі цього аналізу можна визначити вимоги до процедури резервного копіювання критичних даних корпоративних застосунків, а наявність багатьох рішень доводить актуальність їх розробки.

1. Програми для резервного копіювання: топ-10 кращих [електронний ресурс] режим доступу 30.09.2023 [https://www.moyo.ua/ua/news/programmy\\_dlya\\_rezervnogo\\_kopirovaniya\\_top-10\\_luchshikh.html](https://www.moyo.ua/ua/news/programmy_dlya_rezervnogo_kopirovaniya_top-10_luchshikh.html).
2. Free Backup Software – EaseUS Todo Backup [електронний ресурс] режим доступу 30.09.2023 EaseUS Todo Backup – Best Free Backup Software for Windows 11/10/8/7.
3. Cobian Backup/Cobian Reflector [електронний ресурс] режим доступу 30.09.2023 <https://www.cobiansoft.com/cobianbackup.html>.
4. AOMEI Backupper [електронний ресурс] режим доступу 30.09.2023 <https://www.aomeitech.com/aomei-backupper.html>.
5. BackUp Maker: Easy-to-use data backup for Windows [електронний ресурс] режим доступу 30.09.2023 <https://www.ascompsoftware.com/en/products/show/product/backupmaker/tab/details>.
6. Commvault Backup and Recovery [електронний ресурс] режим доступу 30.09.2023 <https://www.commvault.com/resources/commvault-backup-recovery-datasheet>.

## АНАЛІЗ ЗАСОБІВ РОЗПІЗНАВАННЯ КІБЕРАТАК

На сьогоднішній день багато галузей вимагають використання алгоритмів для класифікації даних або прогнозування подальших змін певних значень. У сфері кібербезпеки такі алгоритми широко застосовуються для виявлення атак, тобто класифікації вхідних даних як потенційно небезпечних атак певного типу. Найбільш уразливими у цьому контексті є кінцеві точки, які відносяться до Інтернету речей.

Таблиця 1 – Типи кібератак та їх характеристики

<b>Кібератаки</b>	<b>Опис</b>
DDoS	Атаки, які спрямовані на перевантаження серверів або мережі.
Фішинг	Спроби здійснити шахрайські атаки, використовуючи фальшиві веб-сайти або електронні листи.
Malware	Зловмисне програмне забезпечення, що вивчає конфіденційні дані або завдає шкоди системі.
SQL ін'єкції	Атаки, які використовують вразливості SQL для незаконного доступу до баз даних.
XSS атаки	Атаки, які вбудовують зловмисний код у веб-сторінки, що виконується на браузері користувача.
Інші атаки	Інші різновиди кібератак, які можуть включати в себе атаки на підтримку сесій, введення через форму тощо.

Розпізнавання кібератак – це процес виявлення шахрайських дій або незвичних відхилень в комп'ютерних системах, мережах та даних. Існують різні підходи до розпізнавання кібератак, які використовуються для виявлення потенційно небезпечних активностей.

Таблиця 2 – Методи розпізнавання кібератак та їх переваги та недоліки

Метод розпізнавання	Переваги	Недоліки
Сигнатурні методи	Висока точність, особливо для відомих атак.	Неефективні проти нових та невідомих атак.
Аномалійні методи	Виявлення невідомих атак та змін у системі.	Велика кількість хибних позитивів, складнощі у визначенні порогових значень.
Методи машинного навчання	Адаптуються до нових атак та патернів.	Вимагають великої кількості даних для навчання.

### Сигнатурний аналіз

Опис: Сигнатурний аналіз використовує заздалегідь відомі шаблони (сигнатури) для визначення конкретних типів кібератак. Ці сигнатури можуть включати ключові слова, хеш-відбитки файлів або конкретні послідовності байтів.

Математика: Математично цей метод можна представити як порівняння поточних даних із сигнатурами. Якщо виявлено відповідність, це може свідчити про кібератаку.

### Виявлення аномалій

Опис: Цей метод спрямований на виявлення незвичайних дій або аномалій, які не відповідають стандартному стану системи. Для цього аналізуються статистичні характеристики поведінки системи.

Математика: Математичні моделі, такі як моделі машинного навчання (наприклад, нейронні мережі чи алгоритми кластеризації), можуть використовуватися для створення нормального профілю системи. Аномалії визначаються як відхилення від цього профілю.

### Виявлення вразливостей

Опис: Цей метод полягає в пошуку слабких місць у програмному забезпеченні чи мережах, які можуть бути використані для атаки.

Математика: Математичний аналіз включає перевірку коду на вразливості, аналіз вхідних даних, перехресні атаки та інші методи для виявлення слабких місць у системі.

### Виявлення атак на основі журналів

Опис: Цей метод включає аналіз журналів подій з систем та мереж для виявлення незвичайної чи підозрілої активності.

Математика: Математичний аналіз полягає в використанні правил і порогових значень для виявлення надзвичайних подій у журналах.

#### Модельовані атаки (хакерське тестування)

Опис: Цей метод включає симуляцію атак на систему для перевірки її захищеності та можливості розпізнавання таких атак.

Існує багато статичних і динамічних методів боротьби із такими атаками:

- розробка стратегії для протистояння DDoS атак, що включає в себе план дій;
- забезпечення високого рівня безпеки мережі, використовуючи брандмауери, антивіруси, інструменти контролю вхідного та вихідного трафіку, а також сегментацію мережі;
- створення надлишковості для забезпечення надійності системи;
- використання Content Delivery Network (CDN) для оптимізації доставки контенту та розподілу навантаження;
- проведення постійного моніторингу системи для вчасного виявлення потенційних загроз і атак.

Виявлення кібератак – це складний та безперервно змінний процес, який вимагає поєднання різних методів та технологій для максимальної ефективності у виявленні можливих загроз. Один з ключових аспектів виявлення кібератак за допомогою машинного навчання – це відбір відповідних ознак, обробка великої кількості даних та навчання моделі для розпізнавання нових типів атак.

#### Відбір ознак (Feature Selection)

Проблема великої кількості ознак: У сфері кібербезпеки існує багато різних ознак, проте не всі з них є корисними для виявлення атак. Важливо відібрати лише ті ознаки, які дійсно важливі для моделі, щоб покращити її точність та швидкість реакції.

#### Велика кількість даних (Big Data)

Масштабованість: Збільшення обсягу даних вимагає потужних обчислювальних ресурсів та оптимізованих алгоритмів для ефективного навчання.

Робота з розподіленими даними: У сфері кібербезпеки дані можуть бути розподілені по різних джерелах. Важливо мати систему обробки та збору цих даних.

#### Навчання на нових типах атак

Актуалізація навчання: Навчання моделі та її адаптація до нових типів атак є надзвичайно важливою. Актуалізація моделі за допомогою нових даних та атак є ключем до ефективного виявлення нових загроз.

#### Аналіз атак

Ретельний аналіз нових типів атак та їх характеристик допомагає ефективно розпізнавати подібні загрози. Це може включати в себе аналіз аномалій та навчання на тестових даних з новими атаками.

#### Ефективність моделі

Оцінка моделі: Після навчання моделі важливо визначити її ефективність на тестових даних, використовуючи метрики, такі як точність, відновлення, F1-мера, ROC-крива та інші. Це допомагає відстежувати, наскільки добре модель

справляється з розпізнаванням атак.

Використання ансамблів та стекінгу: Для покращення ефективності можна використовувати комбінації різних моделей та методів.

Загальний підхід полягає в уважній підготовці даних, виборі правильних алгоритмів та постійному оновленні моделі для ефективного виявлення кібератак. Крім того, важливо мати команду експертів, які можуть аналізувати та реагувати на нові загрози та атаки що розвиваються.

1. Random forest. URL: [https://uk.wikipedia.org/wiki/Random\\_forest](https://uk.wikipedia.org/wiki/Random_forest).
2. Random Forest Modeling for Network Intrusion Detection System. URL: <https://www.sciencedirect.com/science/article/pii/S1877050916311127>.
3. Network Attacks and Their Detection Mechanisms. URL: [https://www.researchgate.net/publication/263052997\\_Network\\_Attacks\\_and\\_Their\\_Detection\\_Mechanisms\\_A\\_Review](https://www.researchgate.net/publication/263052997_Network_Attacks_and_Their_Detection_Mechanisms_A_Review).
4. Understanding Random Forest. How the Algorithm Works and Why it Is So Effective. URL: <https://towardsdatascience.com/understanding-random-forest-58381e0602d2>.
5. Canadian Institute for Cybersecurity. URL: <https://www.unb.ca/cic/datasets/>.



## АНАЛІЗ СУЧАСНИХ ДОСЛІДЖЕНЬ У СФЕРІ ЗАХИСТУ ОНЛАЙН-ПОВІДОМЛЕНЬ

Онлайн-повідомлення є невід'ємною частиною нашого сучасного життя. Ми використовуємо їх для спілкування з друзями та родиною, ведення бізнесу та участі у громадському житті. Однак онлайн-повідомлення також вразливі до атак кіберзлочинців.

Онлайн-повідомлення – це текстове або мультимедійне повідомлення, яке передається в електронному вигляді через Інтернет або інші цифрові канали зв'язку [1].

Важливо проаналізувати рішення, що містяться в поточних дослідженнях у цій сфері, для вирішення цих проблем, зменшення їхніх наслідків, пом'якшення питань конфіденційності та задоволення потреб користувачів Online Social Networks (OSN) у приватності. У цій сфері можна виділити багато тенденцій:

*Анонімізація.* це метод захисту конфіденційної або персональної інформації шляхом видалення або зміни даних, що ідентифікують особу, які зберігаються в наборі даних. Мета анонімізації даних – зберегти довіру до даних, що зберігаються або обмінюються, і забезпечити дотримання суворих правил конфіденційності даних. Основним критерієм анонімізації відповідно до стандарту ISO (ISO 29100:2011) є те, що інформація, яка дозволяє ідентифікувати особу (PII), незворотно змінюється таким чином, щоб особу більше не можна було ідентифікувати прямо чи опосередковано. Тому фінансова інформація, контактні дані, звіти про стан здоров'я та платіжні дані, які містять PII, повинні бути добре захищені, щоб відповідати суворим правилам конфіденційності даних [2].

*Перехід до децентралізації.* Децентралізація в безпеці онлайн-повідомлень означає процес розподілу контролю над системою обміну повідомленнями між кількома суб'єктами. Це може допомогти поліпшити конфіденційність і безпеку, ускладнюючи доступ до системи або маніпулювання нею для будь-якої однієї організації.

*Налаштування конфіденційності та управління нею.* Більшість користувачів OSN не надто переймаються налаштуваннями конфіденційності свого профілю, хоча більшість OSN надають налаштування для управління конфіденційністю, щоб користувачі могли контролювати, якою інформацією вони хочуть ділитися і з якими людьми вони хочуть зв'язуватися. Однак більшість користувачів не мають повного уявлення про інформацію, яку вони явно або неявно розкрили, і здебільшого приймають надані за замовчуванням налаштування конфіденційності, і можуть розкривати більш конфіденційну інформацію, яка представляє найвищий рівень ризику для конфіденційності користувача. Дослідження в цій галузі стосуються збільшення контролю користувачів над своїми налаштуваннями конфіденційності або спрощення

цього процесу, вони сподіваються зменшити ризик несанкціонованого доступу та нездатність користувача приховати конфіденційну інформацію від конкретних учасників, таких як друзі або група [2]. На місцях дуже важливо підвищувати обізнаність користувачів про конфіденційність.

*Шифрування.* Використовується як інструмент для забезпечення аспектів конфіденційності та як основа цілісності. Залежно від того, як застосовується шифрування, воно може бути ефективним для захисту від несанкціонованих користувачів або постачальника послуг. Воно також використовується як будівельний блок у поєднанні з іншими пропозиціями, такими як налаштування конфіденційності та інструменти управління або системи децентралізації [3]. Шифрування дуже необхідне для того, щоб приховати інформацію про користувача від OSN, використовуючи при цьому центральну інфраструктуру.

*Обізнаність, законодавство та нормативні акти.* Нетехнічні дослідження зосереджені на підвищенні обізнаності користувачів щодо питань конфіденційності в OSN, а також на дотриманні як постачальниками послуг, так і користувачами соціальних норм поведінки і встановлених законів. Більшість цих нетехнічних підходів не передбачають активного впровадження запропонованих змін. З іншого боку, політики і правила, пов'язані з конфіденційністю, не є обов'язковими, і для підвищення обізнаності зазвичай потрібен час, закони вирішують проблеми після того, як щось пішло не так, тоді як технічні рішення використовуються для запобігання порушенням.

Отже, більшість користувачів онлайн-повідомлень, як правило, не усвідомлюють важливості налаштувань конфіденційності для захисту своєї особистої інформації, тому вони не мають достатньої обізнаності, щоб усвідомити ризик низки загроз, які стоять перед їхньою конфіденційністю, тому необхідно зробити так, щоб деякі з необхідних функцій захисту автоматично управлялися додатком. Крім того, найсерйозніші загрози безпеці та конфіденційності соціальних мереж – це загрози з боку ненадійних постачальників мережевих послуг, оскільки всі дані користувачів знаходяться в їхньому розпорядженні. Також, використання концепції шифрування є основним вектором в аналізі та оцінці приватності та безпеки онлайн-повідомлень.

1. Ебінезер М. і Суреш Б. 2015 Стратегії безпеки для соціальних мереж в Інтернеті Міжнародний журнал комп'ютерних тенденцій і технологій (IJCTT).
2. Абдулла С.М. 2017 Підхід до спільного використання декількох секретів для виявлення вразливостей у соціальних мережах 1-а Міжнародна конференція з інформаційних технологій (ICoIT'17) с.45.
3. Чжан З. і Гупт Б.Б. 2016 Безпека та надійність соціальних мереж: Огляд і новий напрямок Future Generation Computer Systems 86 с.914-925.

## ЕФЕКТИВНІСТЬ РОЗПОДІЛЕНОЇ АРХІТЕКТУРИ ВІДЕОСПОСТЕРЕЖЕННЯ В АЕРОПОРТАХ

### Вступ

Сучасні аеропорти стикаються з безпрецедентними вимогами щодо безпеки та ефективності операцій. У цьому контексті, системи відеоспостереження стають важливим інструментом для забезпечення безпеки пасажирів і майна, а також ефективного управління інфраструктурою. Важливим аспектом є вибір архітектури цих систем.

Ця теза спрямована на дослідження ефективності розподіленої архітектури відеоспостереження в аеропортах. Розподілена архітектура може поліпшити масштабованість, надійність та функціональність відеоспостереження.

У нашому дослідженні ми розглянемо переваги цієї архітектури і вплив її впровадження на безпеку та ефективність аеропортових операцій.

### Постановка задачі

Задача полягає в тому, щоб дослідити ефективність розподіленої архітектури відеоспостереження в аеропортах з огляду на підвищення безпеки та оптимізацію функціональності системи

### Термінологія

*Розподілена архітектура відеоспостереження* – це складна інтегрована система, яка об'єднує в собі фізичні та програмні компоненти, що розташовані на різних географічних об'єктах та підключені через мережу передачі даних.

*Мережева інфраструктура* – це система комп'ютерних, комунікаційних та апаратних ресурсів, які дозволяють пристроям і компонентам обмінюватися даними та комунікувати між собою в рамках певної мережі.

### Опис методу

Системи відеоспостереження (VSS) є важливою частиною безпеки сучасного аеропорту. Вони відіграють важливу роль у стримуванні злочинів, моніторингу потоку пасажирів і багажу та реагуванні на інциденти. В останні роки VSS стають все більш складними з появою нових технологій, таких як штучний інтелект (AI) і машинне навчання (ML).

Традиційні VSS зазвичай централізовані, тобто всі відеодані з камер надсилаються на центральний сервер для обробки. Цей підхід може бути ефективним для малих і середніх VSS, але він може стати неефективним і дорогим для великих і складних VSS.

Розподілені VSS усувають обмеження централізованих VSS, обробляючи відеодані локально на межі мережі. Це означає, що дані обробляються безпосередньо на камерах або на пристроях, розташованих поблизу камер. Цей підхід може значно покращити продуктивність, масштабованість і стійкість VSS.

### **Ефективність розподілених VSS**

Розподілені VSS мають ряд переваг перед централізованими VSS, зокрема:

*Покращена продуктивність:* розподілені VSS можуть значно підвищити продуктивність VSS, зменшивши навантаження на центральний сервер. Це пов'язано з тим, що відеодані обробляються локально на межі мережі, що зменшує обсяг даних, які потрібно надсилати на центральний сервер.

*Підвищена масштабованість:* розподілені VSS можна легко масштабувати для задоволення потреб великих і складних VSS. Це пояснюється тим, що відеодані обробляються локально на межі мережі, що усуває потребу в потужному центральному сервері.

*Покращена стійкість:* розподілені VSS більш стійкі до збоїв, ніж централізовані VSS. Це пояснюється тим, що відеодані обробляються локально на межі мережі, що означає, що система може продовжувати працювати, навіть якщо центральний сервер виходить з ладу.

На додаток до цих переваг, розподілені VSS також можуть допомогти зменшити витрати на VSS. Це пояснюється тим, що для розподілених VSS не потрібен потужний центральний сервер.

### **Ефективність розподілених VSS в аеропортах**

Розподілені VSS можуть запропонувати низку конкретних переваг для аеропортів, зокрема:

*Покращена безпека:* розподілені VSS можуть допомогти підвищити безпеку аеропортів, забезпечуючи більш повний моніторинг пасажирів, багажу та літаків у реальному часі.

*Зменшення експлуатаційних витрат:* розподілені VSS можуть допомогти зменшити експлуатаційні витрати аеропортів, зменшивши потребу в операторах.

*Покращений досвід пасажирів:* розподілені VSS можуть допомогти покращити досвід пасажирів, забезпечуючи більш ефективну та зручну перевірку безпеки.

### **Майбутнє розподілених VSS в аеропортах**

Розподілені VSS все ще є відносно новою технологією, але вони швидко набувають популярності в аеропортах. Оскільки технологія продовжує розвиватися та розвиватися, ми можемо очікувати, що в майбутньому ще більше аеропортів приймуть розподілені VSS.

### **Висновки**

Розподілена архітектура відеоспостереження в аеропортах є важливим елементом для забезпечення безпеки та ефективності авіаційних операцій. Вона дозволяє оптимізувати моніторинг, збір і зберігання даних, а також забезпечує високий рівень надійності системи. Розробка та впровадження таких архітектур може значно підвищити ефективність відеоспостереження в аеропортах та забезпечити більшу безпеку для пасажирів і персоналу.

1. Стефанссон, Г., Янг, Г. (2018). "Application of Distributed Video Surveillance System in Airports for Enhanced Security." У: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). IEEE.
2. Джонсон, П., Міллер, К. (2020). "Optimizing Airport Security Through Distributed Video Surveillance Systems." У: 2020 International Conference on Cybersecurity and Digital Forensics (CyberSec). IEEE.
3. Сміт, А., Браун, Д. (2019). "Enhancing Airport Operations with Distributed Video Surveillance: A Case Study." У: 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC). IEEE.
4. Девіс, Р., Тейлор, С. (2021). "Improving Airport Safety and Efficiency with Distributed Video Surveillance Architecture." У: 2021 International Symposium on Safety, Security, and Rescue Robotics (SSRR). IEEE.

## ВИЯВЛЕННЯ НЕДОЗВОЛЕНИХ ПРЕДМЕТІВ НА ЗОБРАЖЕННЯХ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

В сучасному світі, підприємства стикаються з постійно зростаючим числом викликів, пов'язаних із забезпеченням безпеки своєї діяльності. Один з ключових аспектів цієї безпеки – це здатність ефективно виявляти та вилючати недозволені предмети, які можуть завдати шкоди підприємству, його активам або персоналу. Сутність проблеми полягає в потребі відсіювати потенційні загрози в умовах постійної зміни технологій та методів їх приховування.

Традиційні методи захисту, такі як відеоспостереження, ручний догляд або сигналізація, хоча й залишаються актуальними, можуть не враховувати новітні технологічні засоби маскування чи приховування недозволених предметів. Більше того, їх ефективність часто залежить від людського фактора, що може вести до пропусків або помилок.

Відсутність автоматизованого рішення для виявлення таких предметів може стати серйозним ризиком для безпеки підприємства.

Використання нейронних мереж дозволить підвищити точність та швидкість виявлення, адаптуючись до змінних обставин та нових форм загроз. На відміну від традиційних методів, такий підхід дозволить зосередитися на аналізі шаблонів та аномалій, забезпечуючи високий рівень безпеки на підприємствах без додаткового втручання з боку людини.

Аналіз проблеми виявлення недозволених предметів на підприємствах підкреслює важливість розуміння потенційних ризиків, які можуть виникнути внаслідок невиявлення таких предметів. Основними наслідками є загроза життю та здоров'ю працівників, порушення норм безпеки на робочому місці, матеріальні збитки, а також репутаційні ризики для підприємства.

Особливо важливим є виявлення холодної зброї. Холодна зброя може бути використана для вчинення насильства або залякування персоналу. Її присутність на території підприємства може свідчити про підготовку до агресивних дій або злочинної діяльності. Невиявлення такої зброї може призвести до травм, втрати життя, а також серйозних юридичних наслідків для підприємства. Тому **метою** даного дослідження є розробка програмного застосунка на основі нейронних мереж, який був би здатний аналізувати великі обсяги даних – від відеозображень до складних датасетів – і виявляти потенційно недозволені предмети, а саме, виявлення холодної зброї.

Використання нейронних мереж дозволяє автоматизувати процес розпізнавання, зменшуючи залежність від людського фактора та підвищуючи швидкість та точність виявлення. Враховуючи виклики сучасного світу і постійне розширення спектру потенційних загроз, застосування нейронних

мереж для автоматичного розпізнавання недозволених предметів на зображенні стає ключовим елементом сучасної системи безпеки на підприємствах.

Теоретична основа нейронних мереж базується на їх здатності вчитися та адаптуватися до нової інформації. Вони вивчаються шляхом корекції ваг між нейронами на основі великої кількості вхідних даних і відповідей. Після тренування мережа може робити прогнози або класифікації на основі нової інформації, яка їй подається.

Для задач виявлення холодної зброї використання нейронних мереж має декілька ключових переваг. По-перше, нейронні мережі відрізняються великою адаптивністю. Завдяки своїй здатності вчитися, вони можуть постійно оновлювати свої моделі для відповіді на нові види загроз або зміни в образах зброї. Додатково, гнучкість нейронних мереж дозволяє їм опрацьовувати великі обсяги даних і визначати зброю в різних умовах освітлення, з різних кутів, а також при різних рівнях якості зображення. Це робить їх ефективним інструментом для використання в системах безпеки, де може бути необхідно виявлення об'єктів у складних умовах.

В сфері безпеки нейронні мережі вже успішно використовуються для різних задач, включаючи виявлення вибухівки, розпізнавання осіб за відбитками пальців чи обличчям і, звісно, виявлення холодної зброї. Зокрема, сучасні системи відеоспостереження можуть інтегрувати нейронні мережі для виявлення потенційних загроз у великих натовпах людей або на контрольних пунктах безпеки.

Отже, нейронні мережі представляють величезний потенціал для підвищення рівня безпеки, забезпечуючи ефективний та адаптивний метод виявлення холодної зброї у різних ситуаціях.

Виявлення недозволених предметів на підприємствах за допомогою нейронних мереж стикається з рядом викликів, які мають вирішальне значення для ефективності таких систем (табл. 1).

Таблиця 1 – Проблеми виявлення недозволених предметів за допомогою нейронних мереж

Проблема	Опис
Обмежена гнучкість	Системи часто базуються на претренованих нейронних мережах, які можуть не ефективно розпізнавати специфічні предмети через загальний характер навчання.
Великі обчислювальні витрати	Глибокі нейронні мережі, хоча й

	високоточні, потребують багато обчислювальних ресурсів.
Проблема перенавчання	Мережа може ставати занадто "зосередженою" на конкретних деталях тренувального набору даних.
Відсутність адаптивного навчання	Система не може самостійно адаптуватися до нових умов або нових типів предметів, які не були включені до первісного тренувального набору.

В першу чергу, зустрічаємося з проблемою обмеженої гнучкості: більшість сучасних систем виявлення базуються на претренованих нейронних мережах, що, в свою чергу, можуть не ефективно розпізнавати предмети, специфічні для окремого підприємства, через їх загальний характер навчання [1]).

Також серед ключових труднощів використання глибоких нейронних мереж є великі обчислювальні витрати. Ці мережі, не дивлячись на їх високу точність, потребують значних обчислювальних ресурсів для своєї роботи, що може обмежувати їх застосування в умовах реального часу на підприємствах.

По-третє, нейронні мережі схильні до проблеми перенавчання. Це означає, що мережа може стати занадто "зосередженою" на конкретних деталях тренувального набору даних, ігноруючи загальні характеристики, що може призвести до погіршення її ефективності на нових даних.

Окрім цього, багато систем стикаються з відсутністю адаптивного навчання, коли система не може самостійно адаптуватися до нових умов або нових типів недозволених предметів, які не були включені до первісного тренувального набору.

Щодо вирішення вищезазначених проблем, можна розглядати наступні підходи (табл. 2).

Таблиця 2 – Підходи до вирішення проблем

Підхід	Опис
Персоналізоване навчання	Розробка систем для швидкої інтеграції нових даних для тренування, що допоможе адаптувати систему до конкретних умов підприємства.
Оптимізація обчислень	Використання компактних архітектур нейронних мереж або дослідження



	можливостей квантових обчислень.
Ансамблеві методи	Використання комбінацій прогнозів з кількох моделей для зменшення ризику перенавчання і підвищення точності.
Ітеративне навчання	Впровадження механізмів для постійного оновлення моделі на основі нових даних, отриманих в реальних умовах, що забезпечує систему актуальністю і адаптивністю до змінних умов.

Персоналізоване навчання передбачає розробку систем, які дозволяють швидко і легко інтегрувати нові дані для тренування, що допоможе адаптувати систему до конкретних умов підприємства. З метою оптимізації обчислень можна застосовувати компактні архітектури нейронних мереж або досліджувати можливості квантових обчислень [2]. Для зменшення ризику перенавчання і підвищення загальної точності системи можна використовувати ансамблеві методи, які комбінують прогнози з кількох моделей. Нарешті, ітеративне навчання передбачає впровадження механізмів для постійного оновлення моделі на основі нових даних, отриманих в реальних умовах, що забезпечує систему актуальністю і адаптивністю до змінних умов.

Резюмуючи, в імплементації нейронних мереж для забезпечення безпеки підприємств важливо зосередитися на оптимізації алгоритмів та адаптивності систем. Для контрастування перенавчання та підвищення загальної ефективності варто розглядати ансамблеві методи та персоналізоване навчання. Застосування ітеративного навчання та компактних архітектур може сприяти постійному оновленню моделей на основі нових даних, забезпечуючи їх актуальність і гнучкість в динамічному середовищі.

1. Image Recognition with Deep Neural Networks, 11 Dec, 2019 <https://www.altexsoft.com/blog/image-recognition-neural-networks-use-cases>.
2. Significant Object Detection Challenges and Solutions Sep 21, 2019 <https://towardsdatascience.com/5-significant-object-detection-challenges-and-solutions-924cb09de9dd>.

## СИСТЕМА МОНІТОРИНГУ КОРИСТУВАЧІВ ВЕБ-ЗАСТОСУНКІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ SSO ЗА ГЕОМЕТРІЄЮ ОБЛИЧЧЯ

### Вступ

В Україні, а також в усьому світі, використання різних систем і підсистем ідентифікації стрімко поширюється, що є важливим етапом у розвитку суспільства. Цей розвиток передбачає зростання технологічних процесів. Звичайну систему ідентифікації обличчя можна обдурити, просто поклавши фотографію перед камерою. Використовуючи систему моніторингу користувачів з використанням технології SSO (Single sign-on – технологія єдиного входу) за геометрією обличчя можна запобігти таким порушенням безпеки.

На сьогоднішній день в Україні платформою, де ми часто використовуємо біометричні дані на основі SSO, є проект Державного підприємства «ДІА», зокрема, в автоматизованій системі «ДІА».

### Постановка проблеми

Технологія єдиного входу представляє собою систему сесійної автентифікації, яка дозволяє користувачам використовувати одні й ті ж облікові дані, такі як ім'я користувача та пароль, для отримання доступу до різного програмного забезпечення.

Цей механізм автоматично перевіряє ідентифікацію користувача для кожної програми та забезпечує необхідну повторну автентифікацію при переході між різними програмами протягом одного сеансу.

**Мета дослідження** полягає в аналізі системи моніторингу користувачів веб-застосунків з використанням технології SSO за геометрією обличчя.

### Виклад основного матеріалу

Як приклад діючої системи контролю доступу на базі розпізнавання обличчя можна навести систему TrueFace, розроблену компанією Miros, яка використовується для ідентифікації відвідувачів кіосків для переведення чеків у готівку в декількох штатах США. Також у цій країні застосовується автоматизована система сканування фотографій на водійських посвідченнях. У Європі надзвичайно популярна система контролю доступу ZN-Face, розроблена компанією ZN Vision Technologies AG, і сертифікована Німецьким відомством інформаційної безпеки [1]. Головною перевагою технології SSO є можливість користувача отримувати доступ до різних систем без необхідності авторизуватися окремо в кожній з них.

Проте існують певні недоліки технології SSO. Наприклад, якщо дані для входу користувача потраплять у недоброчесні руки, це може призвести до доступу до багатьох додатків. Крім того, виробники можуть не використовувати загальноприйнятий стандарт або використовувати стандарти, які несумісні з

іншими додатками. Ще однією негативною стороною SSO є те, що багато постачальників цієї системи вимагають оплату за кожну функцію окремо, що може призвести до збільшення витрат на обслуговування такої системи.

Отже, використання системи SSO в сучасних інформаційних системах відіграє важливу роль, оскільки значно полегшує процес авторизації та ідентифікації користувачів в різних підсистемах. Авторизація у веб-застосунку з використанням технології SSO за геометрією обличчя може стати дуже популярною технологією, оскільки вона надає швидку і надійну ідентифікацію, що не вимагає від користувачів особливих зусиль. Це сприятиме вирішенню багатьох суспільних проблем, забезпечить захист інформації від несанкціонованого доступу та спростить надання адміністративних та соціальних послуг населенню.

Для забезпечення безпеки та впровадження технології SSO використовуються маркери або файли cookie, а також протокол обміну метаданими заявок про твердження (SAML). Маркери перевірки передаються через захищений канал, зазвичай з використанням протоколу SSL (Secure Sockets Layer). Для SSL використовуються серверні сертифікати, а криптографічні функції SSL надаються клієнтам через веб-браузери [2].

Серед різних біометричних технологій, що забезпечують конфіденційність образів, біометричні технології розпізнавання за геометрією обличчя є найбільш зручними. Розпізнавання за рисами обличчя має численні переваги порівняно з іншими біометричними технологіями:

- воно може виконуватися без прямого контакту людини зі сканером, за винятком ситуацій, коли розпізнавання обличчя вбудоване в стандартні електронні системи безпеки, і в цьому випадку людина дивиться прямо в камеру;
- з відповідним обладнанням розпізнавання за рисами обличчя можливе на великій відстані, в групі людей, і це не викликає підозр;
- це універсальний метод ідентифікації, який не потребує спеціалізованого обладнання;
- при ідентифікації використовується загальнодоступна біометрична характеристика, яку зазвичай не приховують.

Система моніторингу користувачів веб-застосунків з використанням технології SSO та розпізнаванням обличчя – це типова система розпізнавання образів. Вона формує набір ознак, так званий біометричний шаблон, відповідно до певної математичної моделі. Розпізнавання обличчя в системі моніторингу користувачів веб-застосунків включає кілька етапів: виявлення обличчя, оцінку якості та зразків для подальшого використання, створення шаблону, порівняння і прийняття рішення.

На етапі виявлення обличчя система автоматично визначає в потоці відеокadrів або на фотографії обличчя людей, причому діапазон ракурсів і масштабів осіб може значно варіюватися, що вкрай важливо для побудови систем безпеки.

На етапі оцінки якості здійснюється вибір з усього масиву виділених облич тільки тих зображень, які задовольняють заданим критеріям якості. При цьому оцінюються: ракурс обличчя (не повинен перевищувати 20–30 град.); розмір обличчя (оцінюється за відстанню між зіницями очей і повинен бути більше 50–80 пкс); часткове закриття обличчя (закриття не повинно бути більше 10–25% від загальної площі обличчя).

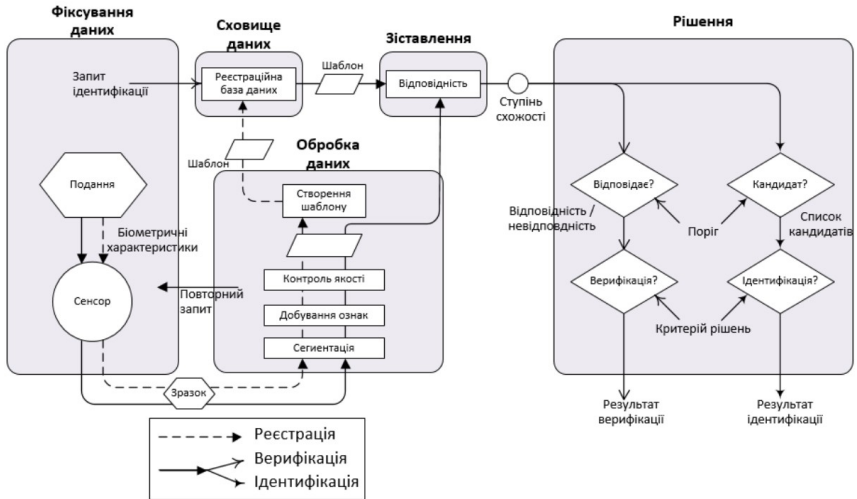


Рисунок 1 – Концептуальна схема узагальненої біометричної системи

Побудова шаблону – це один з найбільш складних і унікальних етапів розпізнавання обличчя, що становить ключове досягнення новітніх технологій. Суть даного етапу полягає в нетривіальному математичному перетворенні зображення обличчя в набір ознак, об'єднаних в біометричний шаблон. Принципи побудови біометричних шаблонів надзвичайно різноманітні. Найважливішою характеристикою біометричного шаблону є його розмір.

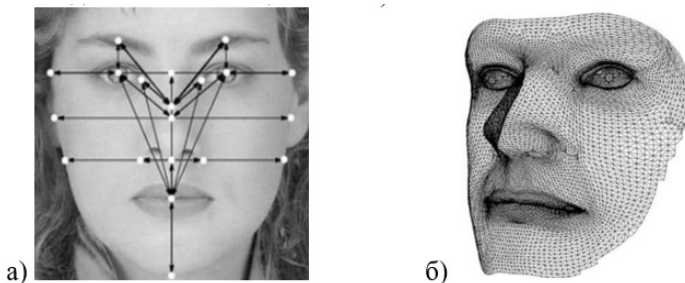


Рисунок 2 – а) 2-D та б) 3-D розпізнавання обличчя

Зіставлення і прийняття рішення – це об'єднаний етап роботи системи розпізнавання, на якому проводиться порівняння біометричного шаблону обличчя, побудованого за виділеним обличчям, з масивом шаблонів.

Система моніторингу користувачів веб-застосунків з використанням технології SSO за геометрією обличчя повинна включати кілька підсистем. Підсистема зберігання даних має містити реєстраційну базу, яка призначена для зберігання біометричних шаблонів. Кожен шаблон має бути пов'язаний з інформацією про суб'єкта реєстрації. Важливо відзначити, що перед зберіганням в реєстраційній базі формат шаблонів може бути змінений згідно з форматом обміну біометричними даними. Ці шаблони можуть бути збережені на біометричних пристроях, на переносних носіях (наприклад, смарт-картах), локально на персональних комп'ютерах або на локальних серверах, або в централізованій базі даних.

Підсистема зіставлення даних порівнює біометричні дані з даними одного чи кількох шаблонів та передає інформацію про ступінь схожості до підсистеми ухвалення рішень. Ступінь схожості визначає, наскільки ознаки відповідають шаблону, з якими проводилося порівняння. При верифікації, один запит суб'єкта реєстрації порівнюється з одним шаблоном і отримується ступінь схожості. У випадку ідентифікації, один запит може порівнюватися з декількома шаблонами, і для кожного порівняння обчислюється ступінь схожості.

Підсистема ухвалення рішень використовує ці ступені схожості, створені однією чи декількома спробами, для видачі рішення щодо запиту на верифікацію чи ідентифікацію. У випадку верифікації порівняння оцінюється як успішне, якщо ступінь схожості перевищує встановлене порогове значення. Підтвердження реєстрації суб'єкта може бути надане відповідно до правил прийняття рішень, які можуть вимагати або допускати декілька спроб верифікації. У випадку ідентифікації, зареєстрований шаблон розглядається як потенційний кандидат для суб'єкта, якщо ступінь схожості перевищує встановлене порогове значення. Правила ухвалення рішень можуть допускати або вимагати кілька спроб перед ухваленням рішення щодо ідентифікації користувачів веб-застосунків, які використовують технологію SSO і геометрію обличчя.

### **Висновки**

В роботі наголошено на перспективності моніторингу користувачів веб-застосунків з використанням технології SSO за геометрією обличчя. Вказано переваги та недоліки технології SSO та описано черговість етапів такої ідентифікації; основні кроки при створенні системи для моніторингу доступу авторизованих користувачів та розглянуто структуру такої системи. Подальші дослідження пов'язані з покращенням управлінням доступу авторизованих користувачів та моніторингу їх активності за допомогою технології SSO.

1. Бугасенко Х. А. Аналіз трьох біометричних методів автентифікації особи. Прикладна радіоелектроніка. 2012. Т. 11, № 2. С. 262–266.
2. Мироненко С. В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. Проблеми інформатизації. Черкаси: ЧДТУ; Х.: НТУ «ХП». 2020, Т. 1: секції 1–3. С. 96.

## ПРОБЛЕМАТИКА МЕТОДІВ КЛАСИФІКАЦІЇ ДЕСТРУКТИВНИХ ДАНИХ

Зростання впливу інтернету та соціальних мереж призвело до збільшення кількості деструктивних текстових матеріалів, які можуть завдати шкоди індивідам, організаціям та громадським інтересам. Ця шкідлива інформація може вплинути на репутацію, фінансовий стан, а також соціальну, психологічну та інформаційну безпеку.

Методи класифікації деструктивних текстових даних можуть допомогти соціальним мережам виявляти та блокувати шкідливий контент, забезпечуючи кращу інформаційну безпеку для користувачів. Для багатьох інтернет-платформ інформаційна безпека та захист від деструктивного контенту стали пріоритетними завданнями. Зростання потужності штучного інтелекту (AI) та машинного навчання відкриває нові можливості для розробки більш точних та автоматизованих методів класифікації деструктивних текстових даних. Використання AI може значно полегшити інформаційну безпеку та забезпечити ефективну реакцію на загрози.

У сучасному інформаційному суспільстві обмін інформацією через текстові дані став невід'ємною частиною нашого повсякденного життя. Однак разом із безмежним потоком корисної інформації, текстові дані також несуть у собі потенційну загрозу у вигляді деструктивних текстів. Деструктивні текстові дані – це будь-які текстові дані, які можуть завдати шкоди індивідам, організаціям або суспільству загалом [1].

Для ефективного запобігання та протидії поширенню таких даних необхідно мати ефективні методи їхньої класифікації. На сьогоднішній день існує широкий спектр методів класифікації деструктивних текстових даних. Однак ці методи мають ряд проблем, які обмежують їхню ефективність.

Однією з ключових проблем, пов'язаних з класифікацією деструктивних текстових даних, є недостатня точність і надійність методів [2, 3].

Наприклад, метод класифікації, який покладається на аналіз ключових слів і фраз, може помилково класифікувати як деструктивний текст, який є жартом або іронією. Або метод класифікації, який покладається на аналіз семантичної структури тексту, може помилково класифікувати як деструктивний текст, який є законним політичним дискурсом.

Необхідно розробляти нові методи класифікації деструктивних текстових даних, які мають більш високу точність і надійність [4, 5]. Точність – це міра того, наскільки часто метод класифікації правильно визначає тип тексту [2]. Надійність – це міра того, наскільки часто метод класифікації дає однаковий результат при повторному використанні [3]. Це допоможе забезпечити ефективне виявлення та блокування деструктивних текстових даних, що є важливою умовою для захисту суспільства від негативних наслідків деструктивного контенту [3].

Нездатність адаптуватися до змін – це ще одна важлива проблема, пов'язана з наявними методами класифікації деструктивних текстових даних. Деструктивні дані постійно змінюються і розвиваються. Деструктивні

користувачі постійно знаходять нові способи маскувати свої повідомлення, щоб уникнути виявлення.

Існуючі методи класифікації деструктивних текстових даних, такі як аналіз на основі машинного навчання, можуть бути неефективними для виявлення нових типів деструктивних даних [5]. Це пов'язано з тим, що такі методи схильні до упереджень, пов'язаних із даними, на яких відбувалось навчання моделей [6]. Це може призвести до того, що нові типи деструктивних даних будуть поширюватися безперешкодно.

Висока вартість і трудомісткість – це ще одна проблема, пов'язана з наявними методами класифікації деструктивних текстових даних. Багато існуючих методів класифікації деструктивних текстових даних вимагають значних витрат і зусиль. Це може ускладнити їхнє впровадження в реальних умовах [5].

Необхідно розробляти нові методи класифікації деструктивних текстових даних, які є більш доступними. Ці методи повинні бути менш доступними та зрозумілими, щоб їх можна було легко впровадити в реальних умовах [2].

Важливо, щоб методи класифікації були справедливими і недискримінаційними. Це означає, що вони не повинні класифікувати законний контент як деструктивний, а деструктивний контент – як законний [4].

Розробка нових методів класифікації деструктивних текстових даних є складною задачею. Однак ця задача є важливою, оскільки вона може допомогти захистити суспільство від негативних наслідків деструктивного контенту.

Існуючі методи класифікації деструктивних текстових даних мають свої обмеження, основними з яких є низька точність і надійність. Нові методи, засновані на розвитку штучного інтелекту та машинного навчання, відкривають широкий простір для покращення ефективності виявлення та блокування деструктивного контенту. Використання штучного інтелекту може автоматизувати процес і зробити його більш точним та швидким.

Подолання проблеми деструктивних текстових даних є важливим завданням для забезпечення інформаційної безпеки та захисту користувачів інтернету та соціальних мереж. Розробка нових методів та вдосконалення існуючих – це крок у правильному напрямку для забезпечення безпечного та конструктивного онлайн-середовища для всіх.

1. Deletion policies of social networks / Saheli Dutta, Razieh Najafabadi // Proceedings of the ACM on Human-Computer Interaction. – 2022. – Vol. 6. – P. 1-37. – DOI: 10.1145/3533117.
2. Dinakar, K., Reichart, R., Lieberman, H. (2011). Modeling the detection of text bullying. ICWSM 2011.
3. Breittfeller, L., Trott, E., Zhang, C. (2019). Finding toxic language: A spaCy toxicity classifier.
4. Nobata, C., Tetreault, J., Thomas, A., Mehdad, Y., Chang, Y. (2016). Abusive language detection in online user content. WWW 2016.
5. Badjatiya, P., Gupta, S., Gupta, M., Varma, V. (2017). Deep learning for hate speech detection in tweets. WWW 2017.

## ЗДІЙСНЕННЯ КІБЕРАТАКИ НА КОМП'ЮТЕРНУ МЕРЕЖУ

Тема кібератак на мережі є дуже актуальною в сучасному світі. Зростання залежності від технологій та підключених пристроїв створює нові можливості для кіберзлочинців та зловмисників. Кібератаки можуть призвести до серйозних наслідків, таких як крадіжка конфіденційної інформації, паралізація бізнес-операцій, пошкодження репутації компанії та навіть фінансові втрати. У зв'язку з цим, розуміння та впровадження ефективних заходів з кібербезпеки є надзвичайно важливими для захисту мереж та даних від потенційних загроз.

Мета дослідження полягає у пошуку способів, як захистити свою мережу від кібератак.

Хоча ви можете думати, що ваша мережа є безпечною, тому що ніхто не докладає зусиль зламати її, це лише омана. Хакери постійно активно відшукують слабкі місця в мережах, і якщо ви не знаєте, на що треба зважати, ви може стати черговою ціллю.

Атака на вашу мережу може мати для вас надзвичайно серйозні наслідки. Скомпрометування конфіденційних даних клієнтів або втрата доступу до важливих внутрішніх документів можуть значно підірвати вашу репутацію і мати довгострокові негативні наслідки, що можуть переслідувати вас протягом тривалого періоду часу.

Тому необхідно знати, на що слід зважати, щоб забезпечити захист вашої мережі від кібератак.

Однією з перших ознак є падіння продуктивності мережі. Атаки типу DoS та DDoS призводять до недоступності мережевих ресурсів [1]. Здебільшого це досягається через надмірне навантаження мережі трафіком або з'єднаннями, що заважає легітимному трафіку. Іноді це може суттєво знизити продуктивність мережі.

Падіння продуктивності може бути спричинене обсягом атаки. DDoS-атака [1] може містити велику кількість запитів, які надсилаються на один сервер, або спроби підключення з різних IP-адрес. Якщо сервер не налаштований на обробку цього обсягу, він не зможе відповісти досить швидко, щоб задовольнити поточні потреби користувача, що може викликати розчарування та відмову від очікування завантаження веб-сайту.

Крім того, тип атаки також може впливати на продуктивність мережі. Якщо сервер налаштований на відхилення або ігнорування запитів, що не надходять з конкретної IP-адреси або діапазону IP-адрес, то він відхиляє і справжніх користувачів, і зловмисників. Це може утруднити доступ справжніх користувачів до сайту, поки вони чекають на виконання запиту на підключення. Це може призвести до розчарування, і в результаті користувачі можуть залишити сайт без отримання потрібної інформації.

Другою ознакою є надмірна повільність роботи комп'ютера через вірус [2]. Існує кілька причин, які можуть призвести до такого сповільнення: 1) намагається



поширюватися і заражати інші частини вашого комп'ютера; 2) запускає шкідливі програми, які вимагають значних ресурсів; 3) додає шкідливий код до операційної системи. Отже, наявність вірусу на комп'ютері може спричинити помітне зниження його швидкодії та продуктивності.

Третя ознака полягає у тому, що програми, які ви регулярно використовуєте, несподівано стають недоступними. Тоді як на ваш комп'ютер потрапляє вірус, він може спричинити пошкодження або видалення файлів у вашій системі. Ці файли можуть бути важливими компонентами операційної системи Windows або інших програм, якими ви постійно користуєтесь. В результаті цих пошкоджень програми стають непридатними для використання, поки відповідні файли не будуть відновлені або замінені.

Четвертою ознакою є самостійне перезавантаження або відмова комп'ютера, яка зазвичай супроводжується перезавантаженням. Це може бути результатом кібератаки, наприклад, використання "віддаленого виконання коду" [3] або "ін'єкції DLL" [4].

У процесі використання "віддаленого виконання коду" [3] зловмисник відправляє команду на ваш комп'ютер, яка примушує його запускати зловмисне програмне забезпечення (ПЗ). Це ПЗ може отримати доступ до пам'яті вашої системи та спричинити її перезавантаження. Зловмисне ПЗ може бути встановлене шляхом використання експлойт у програмному забезпеченні.

Через використання "ін'єкції DLL" [4] зловмисник відправляє команду, яка дає дозвіл впровадити шкідливий код через експлойт, що вносить зміни в роботу вашої операційної системи Windows. Це також може спричинити перезавантаження операційної системи.

П'ята ознака полягає у отриманні повідомлень про помилки, які ви раніше не зустрічали. Це свідчить про проблеми з апаратним або програмним забезпеченням, або обома одночасно. Найкращим способом подолати дані повідомлення – це звернутися до фахівця з кібербезпеки, який допоможе вам вивчити причину проблеми та надати необхідну допомогу.

Шоста ознака полягає у зростаючій кількості спливаючих вікон на вашому пристрої з кожним днем. Це може свідчити про наявність зловмисного ПЗ. Це зловмисне ПЗ може бути встановлено на вашому пристрої без вашої згоди і викликати неприємності, такі як нав'язлива реклама та інші небажані випадкові вікна, які з'являються на екрані.

Сьоомою ознакою є спостереження дивних файлів на робочому столі або в системних папках комп'ютера, які ви не створювали та не завантажували. Це може свідчити про компрометацію вашої системи зловмисним ПЗ. Ймовірно, це ПЗ було встановлено через натискання на посилання, запуск файлу (.exe) або відкриття вкладення в електронному листі.

Зловмисне ПЗ може виконувати різноманітні дії. Воно може видаляти або зашифрувати файли, позбавляючи вас доступу до них, або користуватися вашою системою для надсилання спаму. Крім того, воно може сповільнювати роботу комп'ютера або спричиняти його збої.

Восьма ознака полягає у зміні розміру шрифту вашого браузера. Якщо розмір шрифту у вашому браузері змінився автоматично, без вашої участі або втручання, це може свідчити про можливе вторгнення в вашу систему або наявність вірусу.

Дев'ятою ознакою є зміна мовних налаштувань без вашого підтвердження. Це може свідчити про те, що ви потрапили під вплив реклами типу поп-ап. Дані рекламні оголошення спонукають користувачів натискати на них, і вони часто включають посилання, які автоматично вносять зміни в налаштування на вашому пристрої, особливо якщо ви погодилися на це, натиснувши "так".

Десята ознака полягає у постійному перенаправленні вас на незнайомі або небажані вами сайти. Це може свідчити про наявність зловмисного ПЗ на вашому комп'ютері, тому важливо якомога швидше позбутись його.

В даній роботі ми дослідили 10 ознак, які свідчать про те, що ваша мережа стала жертвою кібератаки. Отже, навчитися розпізнавати ознаки кібератаки є одним з найефективніших способів захисту вашої мережі. Це дозволяє вчасно виявити атаку та прийняти заходи для її припинення, перш ніж вона спричинить проблеми.

1. Що таке DDoS-атаки та яку мету вони переслідують. URL: <https://infocom.ua/що-таке-ddos-атаки/>. (Дата звернення: 27.06.2023).
2. КОМП'ЮТЕРНІ ВІРУСИ. URL: <https://informatics6.webnode.com.ua/zanyattyia-11/>. (Дата звернення: 27.06.2023).
3. Remote code execution (RCE). URL: <https://www.techtarget.com/searchwindowsserver/definition/remote-code-execution-RCE>. (Дата звернення: 27.06.2023).
4. DLL injection. URL: [https://en.wikipedia.org/wiki/DLL\\_injection](https://en.wikipedia.org/wiki/DLL_injection). (Дата звернення: 27.06.2023).

## **РЕЗИЛЬЄНТНІСТЬ ОПЕРАТОРІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.**

Сучасне життя майже повністю комп'ютеризовано. Але існує багато сфер з високою ступінь залучення людини в технологічному процесі [1]. Існує велика кількість професій, в яких важливою є постійна наявність фокусу уваги працівника на активній зоні програмного застосунку для забезпечення функціонування критичної інфраструктури. Нажаль існує багато прикладів коли відбувалась катастрофа в результаті недостатньою уваги працівника. Це авіакатастрофа яка обумовлена помилкою авіадиспетчера або пілота. В будь якому випадку це відбулось як наслідок втрати фокуса уваги оператором складного технологічного процесу. Вплив людського фактору нажалі може виникнути будь коли, тобто людина може втомитися чи захворіти або її можуть відволікати якісь суб'єктивні чи об'єктивні фактори. В таких випадках співробітник може втратити уважність, наприклад – заснути на робочому місці, дивитись не на монітор, а в телефон або у вікно чи на іншу людину. При цьому його фокус уваги на інформації, яка відображається на екрані комп'ютера, втрачається, що часто може бути неприпустимо. Для запобігання цьому потрібна система контролю за станом оператора. Вона може здійснюватися покрово:

- контроль фізичного та психологічного стану оператора перед допуском к роботі;
- контроль уваги оператора під час роботи;
- моніторинг та аналіз можливих впливів на оператора в неробочий час.

Таким чином ми приходимо к комплексної задачі моніторингу, аналізу та корекції працездатного стану оператора. При цьому суспільство зацікавлене в підвищені резильєнтності операторів та протидії шкідливим впливам на них. Ця задача має багато аспектів, це медицина, екологія, суспільство. В силу нашої спеціалізації розглянемо інформаційну складову яка впливає на зміні резильєнтності операторів.

На першому кроці – контроль фізичного та психологічного стану оператора перед допуском к роботі. Існують відомі проблеми, які пов'язані з захистом медичних та персональних даних.

На другому кроці – контроль уваги оператора під час роботи – існують методи контролю уваги оператора. Прикладом є наші роботи по контролю уваги оператора за допомогою аналізу біометричних параметрів елементами штучного інтелекту.

На третьому кроці – моніторинг та аналіз можливих впливів на оператора в неробочий час – найважливішим в наш час є інформаційна протидія дезінформації. Важливою для цього процесу є міжнародна підтримка, вчасності

грантова програма CRDFGlobal, відкриття Центру протидії дезінформації. Але існує науково технічна проблема організації онлайн моніторингу, знаходження, фіксації та вчасного реагування на фейки.

Рішення проблем першого кроку добре пропрацьовано, прикладом може бути програма Дія.

Проблеми другого етапу зараз активно вирішуються. Можливим підходом є використання аналізу відео потоку для розпізнавання обличчя оператора та його оточення. На основі аналізу інформації з веб-камери в режимі онлайн, здійснюють контроль наявності фокусу уваги співробітника на активній зоні критичного застосунку та відсутності неавторизованих осіб біля комп'ютера.

Для цього нами були використані нейронні мережі для визначення 3D-поверхні обличчя. Використовуючи архітектуру моделі обличчя разом із прискоренням графічного процесора протягом усього циклу обробки, функція забезпечує високу продуктивність у реальному часі. Використана модель [2] має конвеєр з двох нейронних мереж для визначення 3D-координат 468 орієнтирів на обличчі: псевдо-тривимірних координат з двовимірного зображення. Перша нейромережа «BlazeFace» знаходить розташування обличчя на основі аналізу повного зображення. BlazeFace використовує легку мережу вилучення функцій, подібну до MobileNetV1/V2 [3].

Проблеми третього кроку потребують окремого опису. Але там теж доцільно використовувати елементи штучного інтелекту.

7. Давиденко А.М., Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів. – дисертація докт. техн. наук: 05.13.21 / Національний авіаційний університет. – Київ, 2021. – 347 с.
8. Face detection guide [Electronic resource]. – Access mode: [https://developers.google.com/mediapipe/solutions/vision/face\\_detector#blazeface\\_short-range](https://developers.google.com/mediapipe/solutions/vision/face_detector#blazeface_short-range). (accessed 17.08.2023).
9. Howard, A. G. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications [Electronic resource] / A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam // Computer Vision and Pattern Recognition. – 17.04.2017. DOI: 10.48550/arXiv.1704.04861.

## **НРС ТА РЕКОНФІГУРОВНІ ЗАСОБИ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ КІБЕРФІЗИЧНИХ СИСТЕМ**

Одним з важливіших компонентів властивості резильєнтності технічних систем є адаптивність. Принцип адаптивності також є одним з принципів, покладених в основу національної системи стійкості України [1].

Адаптивність – це здатність системи пристосовуватися до кризових умов і нових обставин, які виникли під впливом загрози або кризової ситуації, забезпечувати виживання, еволюцію, можливість трансформувати негативні результати в позитивні, а також застосовувати інноваційні рішення [2].

Програмовані логічні інтегральні схеми (ПЛІС), що є основою реконфігурованих обчислювальних засобів, природним чином дозволяють реалізовувати принцип адаптивності. Сучасні НВІС програмованої логіки вже містять десятки мільйонів еквівалентних логічних елементів і надають змогу за лічені секунди створювати, тобто, фактично, виготовляти всередині себе великі та складні цифрові структури шляхом завантаження конфігураційної інформації (bitstream) з підготовленого файлу певного формату. Використання в якості апаратної платформи реконфігурованих обчислювачів (прискорювачів) за рахунок стандартизації та уніфікації дозволяють знизити загальну вартість володіння реконфігурованих систем [3]. Але залишається проблема складності задачі створення конфігурацій, тобто задачі синтезу складної цифрової схеми для завантаження в ПЛІС. Ця задача потребує значних зусиль та багато праці висококваліфікованих розробників із залучанням потужних спеціалізованих інструментальних засобів.

До кількісних показників, що дозволяють оцінити рівень резильєнтності складної системи, відносяться, зокрема, час відновлення її основних функціональних характеристик та вартість витрат на подолання наслідків зовнішнього руйнівного впливу. Тому для підвищення рівня резильєнтності системи, що базується на реконфігурованих технічних засобах, необхідно, по-перше, прискорити процедуру реконфігурації (яка включає оперативний синтез зміненої обчислювальної структури, що адаптована до нових умов функціонування), по-друге, знизити вартість цієї процедури.

Протягом кількох років в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України проводяться дослідження з розробки теоретичних засад, методів і підходів до прискорення та спрощення процедури пересинтезування складних обчислювальних засобів, побудованих на реконфігурованій платформі. Головна ідея напряму полягає у перенесенні ресурсоємної процедури розробки зміненої структури з локальних реконфігурованих засобів до централізованої системи, яка, по-перше, використовує сторонні НРС (High Performing Computing) обчислювальні ресурси (розподіленої суперкомп'ютерної мережі грід або хмарні), по-друге,

застосовує методи автоматизованого та автоматичного створення конфігурацій для ПЛІС для окремих задач та класів задач, що вирішуються локальними системами.

Прикладом подібної розробки є веб-сервіс STRAGS (Security Tasks Reconfigurable Accelerators Grid-Service), призначений для централізованого виконання процедури створення конфігурацій для засобів апаратного прискорення задач захисту інформації в комп'ютерних мережах і системах (таких як мережеві системи виявлення вторгнень (MCBB), апаратні антивіруси, спам-фільтри, системи протидії мережевим хробакам тощо) [4].

В процесі функціонування грід-сервіс STRAGS приймає від користувачів запити на синтез реконфігуровної системи захисту інформації в уніфікованому вигляді, які містять функціональні вимоги до потрібної схеми (наприклад, перелік сигнатур, що мають швидко розпізнаватися) та параметри реконфігуровного прискорювача, яким обладнана локальна система. Отримавши завдання, сервіс на віддалених вузлах грід-середовища ініціює роботу декількох агентів – віртуальних машин з попередньо встановленим і налаштованим інструментальним програмним забезпеченням, необхідним для синтезу реконфігуровних пристроїв і генерації конфігурацій. Отримуючи нові запити від клієнтів, сервіс розподіляє завдання між активними агентами, підтримуючи їх число достатнім для забезпечення готовності на необхідному рівні. Кожний агент після отримання грід-завдання запускає процеси автоматичного синтезу необхідної цифрової схеми і синтезу відповідної конфігурації для ПЛІС (використовуючи певні оригінальні методи та техніки [5]), після чого повертає результат роботи сервісу. Нарешті готові конфігураційні файли надсилаються користувачам для завантаження в ПЛІС реконфігуровних системи захисту інформації.

Сервіс має зручний інтерфейс і завдяки використанню спеціальних механізмів інтерактивної взаємодії з грід-агентами дозволяє користувачу відслідковувати процес вирішення його задачі в реальному часі.

За рахунок використання централізованого сервісу користувачі локальних систем кіберзахисту позбуваються необхідності вирішення складної проблеми синтезу та повторного синтезу в ПЛІС складних цифрових схем. Це не тільки спрощує використання потужних можливостей сучасної реконфігуровної апаратної платформи, але також зберігає час. База даних готових рішень дозволяє сервісу ще більше прискорювати процес створення систем кіберзахисту на ПЛІС за рахунок максимального використання незмінних та подібних компонентів модульних цифрових структур. Згодом сервіс було також доповнено режимом використання технології хмарних обчислень.

Даний принцип побудови централізованих систем на базі НРС може бути використаний для широкого кола ресурсоемних обчислювальних задач, що потребують апаратного прискорення. Ще одним таким прикладом є задача завадостійкого кодування інформації, що передається в каналах обміну даними всередині кіберфізичних систем (КФС) критичної інфраструктури, зокрема, в

енергетичній галузі. Найвідомішим шляхом підвищення живучості інформації в каналах передачі даних всупереч впливу завад, є використання спеціальних коригуючих кодів, здатних виправляти помилки [6]. Пошук таких кодів з найкращими характеристиками не є тривіальною задачею. Один з підходів до пошуку породжувальних матриць (які однозначно задають такий код) полягає в переборі можливих комбінацій рядків, що формують ці матриці. У зв'язку з тим, що повний перебір всіх можливих варіантів є NP-повною задачею, безпосередня реалізація такого підходу потребує неприйнятно багато часу. Але комбінування певних методів та технік у поєднанні з використанням досягнень НРС дозволяють за певних умов здобути непогані результати при помірних часових витратах [7].

В результаті проведення низки досліджень в цьому напрямку з'ясовано, що використання ресурсів НРС в спосіб, розглянутий вище, також дозволяє створювати засоби підвищення резильєнтності КФС. Розроблено методику централізованої побудови додаткових модулів забезпечення цілісності інформації, що передається в каналах обміну даними між компонентами КФС, використовуючи обчислювальні потужності грид-інфраструктури [8].

Подібно до сервісу STRAGS експериментальна централізована система збирає запити від користувачів з вимогами до коду, породжувальну матрицю для якого потрібно знайти, та параметрами реконфігурованого обладнання, на якому здійснюватиметься заводостійкий захист інформації. Нагадаємо, що в результаті руйнівного впливу на критичну інфраструктуру властивості заводостійкого каналу зв'язку можуть суттєво змінюватися. Більш того, типовою є ситуація, коли характеристики заводостійкого кодування відрізняються на різних етапах реагування системи, що захищається, на зовнішній вплив, а після повного подолання катастрофічних наслідків, повертаються до показників штатного режиму.

Як і сервіс STRGS система централізованої побудови засобів підвищення живучості КФС також зберігає результати попередніх розрахунків, що дозволяє не тільки прискорити обчислювальний процес, але в деяких випадках навіть взагалі обійтися без виконання завдання, оскільки вірогідність співпадіння всіх параметрів створення заводостійкого коду набагато вища за таку, що характеризує збіг всіх показників, наприклад, реконфігурованих МСВВ двох різних користувачів.

На додаток до результатів, отриманих в попередні роки за останній час вдалося теж отримати певні позитивні здобутки. Зокрема в результаті проведення низки обчислювальних експериментів із залученням потужностей Українського національного гриду, вдалося порівняти результати пошуку породжувальних матриць, отриманих прискореними алгоритмами, що були запропоновані раніше, із результатами пошуку матриць з такими ж характеристиками, але отриманих шляхом повного перебору можливих комбінацій. З'ясувалося, що для розмірностей, для яких вдалося за прийнятний час здійснити такий перебір, приблизно в половині випадків різниця була

відсутня, а в решті випадків складала всього один розряд довжини коду. Так, для лінійного блокового коригуючого коду, який виправляє трикратні помилки та містить 27 корисних бітів, прискорений метод знайшов породжувальну матрицю (44, 17)-коду, що використовує 17 надлишкових бітів, в той час як повний перебір дозволив покращити результат до (43, 16)-коду, який також містить 27 корисних бітів, але тільки 16 бітів надлишковості. При цьому часові витрати на повний перебір перевищили час роботи прискореного алгоритму на кілька десяткових (!) порядків. А, наприклад, для лінійного (40, 28)-коду, що виправляє до шести помилок, результати пошуку співпали з точністю до біта. При цьому різниця в часових витратах повного перебору та прискореного алгоритму сягала порівняних порядків.

1. Концепції забезпечення національної системи стійкості. Затверджено Указом Президента України від 27 вересня 2021 року № 479/2021. URL: <https://zakon.rada.gov.ua/laws/show/479/2021/print>.
2. Зубок В.Ю., Драгунцов Р.С. Проекція принципів національної системи стійкості та резильєнтність критичної інформаційної інфраструктури // Резильєнтність критичної інфраструктури – 2023 : збірник матеріалів науково-практичної конференції, м. Київ, 21 червня 2023 р., ПІМЕ ім. Г.Є. Пухова НАН України. – 2023. – С. 104-108.
3. Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор // Электронне моделювання. – 2013. – Т. 35, № 4. – С. 49-72.
4. Свідоцтво про реєстрацію авторського права на твір № 105997; Комп'ютерна програма «Веб-сервіс централізованого програмування реконфігурованих засобів захисту інформації на базі ґрідів та хмарної інфраструктури STRAGS» («Веб-сервіс STRAGS») / В.Ф. Євдокимов, А.М. Давиденко, С.Я. Гильгурт; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, дата реєстрації 7.07.2021 р.
5. Гильгурт С.Я. Метод прискореної кількісної оцінки компонентів реконфігурованих сигнатурних систем кіберзахисту // Електронне моделювання. – 2022. – Т. 44, № 5. – С. 3-24.
6. Блейхут. Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ., М.: Мир, 1986. 576 с.
7. Винничук С.Д., Давиденко А.Н., Гильгурт С.Я., Потенко А.С. Нижняя оценка максимального кодового расстояния для линейных блоковых кодов  $(n, k)$  над полем  $GF(2)$ . Тез. доп. Міжнар. наук.-техн. конф. «Моделювання-2012», Київ, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2012. – С. 150–153.
8. Винничук С.Д., Давиденко А.Н., Гильгурт С.Я., Потенко А.С. Применение грид-системы при исследовании линейных блоковых кодов. Системы обработки информации: Збірник наукових праць, Харків, Харківський університет Повітряних Сил ім. Івана Кожедуба, 2013. Вип. 7 (114). С. 1–64.





**МІЖНАРОДНА  
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ  
«ЖИВУЧІСТЬ ТА РЕЗИЛЬЄНТНІСТЬ – 2023»  
(«SURVIVABILITY & RESILIENCE – 2023»)**

**Збірник матеріалів конференції  
19 жовтня 2023 р.**

Survivability & Resilience – 2023 : collection of materials of the international scientific and practical conference, Kyiv, October 19, 2023, PIMEE of NAS of Ukraine. – 2023. – 153 p.

Живучість та резильєнтність критичної інфраструктури – 2023 : збірник матеріалів міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023 р., ПМЕ ім. Г.С. Пухова НАН України. – 2023. – 153 с.