Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Факультет комп’ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В. о. завідувача кафедрою БІСТ

Мелкозьорова О. М.

_____

« » 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Дослідження та порівняльний аналіз нормативних документів, спрямованих на реагування на кіберінциденти»

оцінка « » Керівник к.т.н. Єсіна М. В.

Голова ЕК

Лемешко О. В. _____ Рецензент к.т.н. Бобух В. А.

Виконавець: студент групи КБ-42

_____ Пелюх О. І.

Харків – 2024

РЕФЕРАТ

Обсяг пояснювальної записки до проєкту бакалавра складає 50 сторінок, у тому числі 14 рисунків і 16 таблиць. Використано 33 джерела за переліком посилань. Метою роботи є вивчення сучасного стану й перспектив розвитку систем кібербезпеки на прикладі вітчизняних і зарубіжних підходів, аналізу ефективності існуючих методик реагування на кіберінциденти, а також у розробці рекомендацій щодо покращення механізмів захисту з реагування на інциденти у кіберпросторі. У роботі використані аналітичні й порівняльні методи аналізу, документальний аналіз законодавства й експертні оцінки у сфері кібербезпеки.

У результаті дослідження виявлені прогалини у міжнародній інтеграції України та взаємодії у вирішенні кіберзагроз, а також запропоновані рекомендації щодо покращення систем кібербезпеки та реагування на кіберінциденти. Проведена оцінка реагування на реальний кіберінцидент, надані рекомендації щодо покращення процедури в майбутньому. Отримані результати можуть бути корисні як для державних інституцій, що займаються питаннями національної безпеки, так і для приватного сектору з критично важливою інфраструктурою та зберіганням персональних даних. Робота підкреслює важливість забезпечення кібербезпеки як ключової умови стабільного розвитку будь-якої держави та міжнародної системи в цілому.

Рекомендації, розроблені на основі отриманих результатів, сприятимуть підвищенню рівня кібербезпеки. Можливими напрямками розвитку є подальше вдосконалення законодавства в галузі кібербезпеки, підвищення ефективності механізмів реагування на кіберінциденти та сприяння міжнародній співпраці у цій сфері.

Ключові слова: КІБЕРБЕЗПЕКА, КІБЕРІНЦИДЕНТ, ЗАХИСТ ІНФОРМАЦІЇ, РЕАГУВАННЯ, ЗАКОНОДАВСТВО.

ABSTRACT

The length of the explanatory note to the bachelor's project is 50 pages, including 14 figures and 16 tables. The work uses 33 sources according to the list of references. The purpose of the work is to study the current state and prospects for the development of cybersecurity systems on the example of domestic and foreign approaches, to analyse the effectiveness of existing methods of responding to cyber incidents, and to develop recommendations for improving protection mechanisms for responding to incidents in cyberspace. The study used analytical and comparative methods of analysis, documentary analysis of legislation, and expert opinions in the field of cybersecurity.

The study has identified gaps in Ukraine's international integration and cooperation in addressing cyber threats, and offered recommendations for improving cybersecurity systems and responding to cyber incidents. The response to a real-life cyber incident was assessed and recommendations for improving the procedure in the future were provided. The findings can be useful for both government institutions dealing with national security issues and the private sector with critical infrastructure and personal data storage. The paper demonstrates the importance of ensuring cybersecurity as a key condition for the stable development of any state and the international system as a whole.

The recommendations developed on the basis of the findings will help improve the level of cybersecurity. Possible areas of development include further improvement of cybersecurity legislation, enhancing the effectiveness of cyber incident response mechanisms, and promoting international cooperation in this area.

Keywords: CYBERSECURITY, CYBER INCIDENT, INFORMATION PROTECTION, LEGISLATION, RESPONSE.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CERT-UA	– команда реагування на комп’ютерні надзвичайні події України
CSF	– Cyber Security Framework
CSIRT	– комп’ютерна група реагування на надзвичайні ситуації у країнах ЄС
EECC	– European Electronic Communications Code
ENISA	– The European Union Agency for Cybersecurity
NCSC	– National Cyber Security Centre
NIS	– Network and Information Systems
NIST	– National Institute of Standarts and Technology
SP	– special publication
US-CERT	– команда комп'ютерної готовності до надзвичайних ситуацій США
ЄК	– Європейська комісія
ЄС	– Європейський Союз
ІБ	– інформаційна безпека
ЗУ	– Закон України
ІКС	– інформаційно-комунікаційні системи
ІКТ	– інформаційно-комунікаційні технології
КМУ	– Кабінет міністрів України
ООН	– Організація Об’єднаних Націй
ПЗ	– програмне забезпечення
ПрАТ	– приватне акціонерне товариство
РНБО	– Рада національної безпеки і оборони України
США	– Сполучені Штати Америки

ВСТУП

У контексті стрімкого розвитку інформаційних технологій та зростаючої кібернетичної загрози, питання кібербезпеки набуває все більшого значення як для окремих країн, так і для міжнародної спільноти в цілому. Аналіз науково-технічної літератури вказує на значні досягнення в області кібербезпеки, зокрема в розробці нормативних документів, методів реагування на кіберінциденти та забезпеченні захисту інформаційних систем. Проте, попри ці успіхи, існують вагомі прогалини у знаннях, особливо щодо міжнародної інтеграції та взаємодії у вирішенні кіберзагроз, що вимагає подальших досліджень та розробки нових підходів.

Актуальність роботи обумовлена постійно зростаючою кількістю кіберінцидентів, які можуть мати серйозні наслідки для національної безпеки, економіки та приватного життя громадян. У контексті глобалізації та збільшення міжнародної інформаційної взаємозалежності, забезпечення кібербезпеки стає ключовою умовою стабільного розвитку будь-якої держави та міжнародної системи в цілому.

Мета роботи полягає у вивченні сучасного стану й перспектив розвитку систем кібербезпеки на прикладі вітчизняних і зарубіжних підходів, аналізу ефективності існуючих методик реагування на кіберінциденти, а також у розробці рекомендацій щодо покращення механізмів захисту з реагування на інциденти у кібернетичному просторі. Галузь застосування результатів дослідження охоплює не тільки державні інституції, зайняті питаннями національної безпеки, але й приватний сектор, що має критично важливу інфраструктуру та зберігає значні обсяги персональних даних.

Також доцільно перевірити відповідність якісного взаємозв’язку між внормованою стратегією з реагування на кіберінциденти в Україні з реальними схемами владнання таких ситуацій. Отже, гіпотеза для дослідження наступна: наразі наявна повна відповідність процедур реагування на масштабні кіберінциденти чинному законодавству України.

1 ОГЛЯД РЕГУЛЯТОРНОГО СЕРЕДОВИЩА СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ

Огляд, аналіз та досвід використання нормативних документів, спрямованих на реагування на кіберінциденти, на міжнародному рівні є важливим кроком до створення більш безпечного кіберпростору для всіх. Співпраця та спільні зусилля на міжнародному рівні, а також постійне відстеження тенденцій у цій сфері, допоможуть впроваджувати ефективні практики своєчасно на національному рівні.

За даними Міжнародного індексу з кібербезпеки (англ. The Global Cybersecurity Index) Міжнародної спілки електрозв'язку [1], саме Сполучені Штати Америки (США) є беззаперечним лідером і має максимально можливе значення індексу – 100, значення індексу України – 65,9, різницю наведено на рис. 1.1.

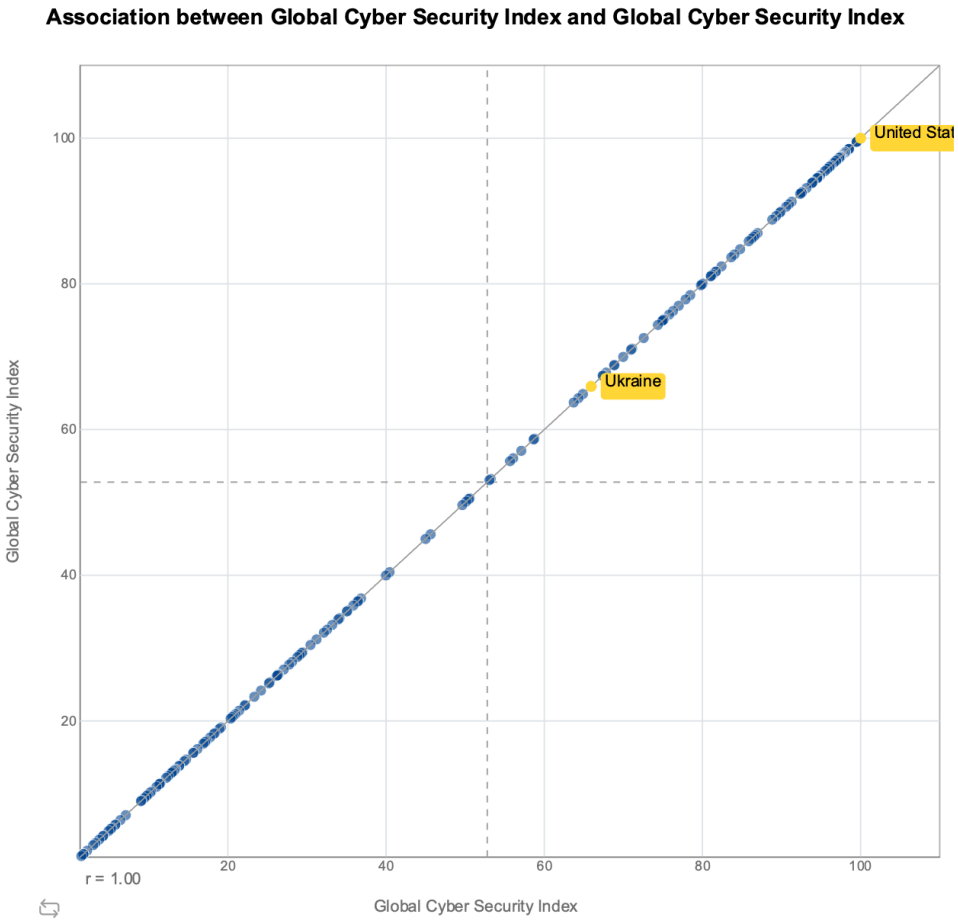

Рисунок 1.1 – Міжнародний індекс з кібербезпеки (співставлення США та України)

Відповідно першочергово варто брати до уваги нормативні документи, прийняті в країні-лідерці з впровадження принципів кібербезпеки за даними авторитетної організації.

1.1 Загальні відомості

За результатами проведення пошуку й подальшого аналізу створених як приватними, так і державними установами документів у [2] було обрано наступні фреймворки для більш детального розгляду в дипломній роботі, а саме: NIST SP 800-61, Фреймворк NIST з кібербезпеки (CSF) 2.0, Посібник з реагування на кіберінциденти в органах державної влади від Американської асоціації комунальних підприємств.

– NIST SP 800-61 [3]

Цей документ надає організаціям необхідні знання та інструменти для створення та вдосконалення систем реагування на кіберінциденти, забезпечуючи їх ефективне та результативне вирішення. Оновлене друге видання враховує динаміку кіберзагроз та інцидентів. Розуміння загроз та раннє виявлення сучасних атак є ключовими факторами запобігання подальшим випадкам компрометації. Проактивний обмін інформацією про ознаки таких атак між організаціями стає все більш дієвим способом їх виявлення. Виконання вимог та рекомендацій, представлених у цьому посібнику, має на меті допомогти федеральним департаментам та агентствам у реагуванні на кіберінциденти з максимальною ефективністю та результативністю.

NIST SP 800-61 розроблена для широкого кола фахівців, які відповідають за впровадження безпекових принципів у кіберпросторі організацій. Вона надає цінну інформацію та рекомендації для груп реагування на інциденти, системних та мережевих адміністраторів, співробітників служби безпеки, персоналу технічної підтримки, керівників служб інформаційної безпеки (ІБ), керівників інформаційних служб, керівників програм комп'ютерної безпеки та інших зацікавлених сторін.

– CSF 2.0 [4]

CSF, представлена у 2014 році [5], здобула широке визнання як дієвий інструмент протидії кіберзагрозам. Зворотний зв'язок від багатьох організацій свідчить про те, що CSF 1.1 залишається ефективною основою для подолання викликів, пов’язаних із забезпеченням принципів кібербезпеки. Водночас, існує загальна думка про необхідність оновлення програми з метою адаптації до поточних та майбутніх проблем у цій сфері, а також для спрощення її використання. NIST співпрацює з фахівцями, щоб гарантувати, що CSF 2.0 буде ефективним у майбутньому, відповідаючи при цьому початковим цілям та завданням.

CSF 2.0 – це інструментарій, який допомагає промисловості, урядовим установам та іншим організаціям знижувати ризики в області забезпечення кібербезпеки. Вона пропонує систему класифікації результатів із дотримання принципів кібербезпеки високого рівня, які можуть бути використані будь-якою організацією, незалежно від її розміру, сектору або рівня зрілості, для кращого розуміння, оцінки, пріоритезації та інформування про свої зусилля із захисту інформації в кібернетичному просторі. CSF 2.0 не описує конкретні методи досягнення результатів. Натомість, містить посилання на ресурси, які надають додаткові вказівки щодо практик і засобів контролю, які можуть бути використані для їх досягнення. Цей документ пояснює суть CSF 2.0 та його компонентів, а також описує деякі з численних способів його застосування.

– Посібник з реагування на кіберінциденти в органах державної влади від Американської асоціації комунальних підприємств [6]

Посібник надає детальні інструкції для малих та середніх комунальних підприємств щодо створення плану реагування на кіберінциденти, встановлення пріоритетів, залучення відповідних фахівців для реагування та координації обміну інформацією. Основні складові посібника містять:

1) надання рекомендацій для розробки плану реагування на кіберінциденти та визначення процедур для виявлення, розслідування, усунення та відновлення після інциденту;

2) визначення галузевих та урядових партнерів, які можуть бути залучені для обміну інформацією, отримання підтримки та аналізу наслідків інциденту, а також для координації з клієнтами та громадськістю;

3) опис процесу запиту на кібернетичну допомогу від комунальних підприємств енергетичної галузі у випадку серйозного порушення роботи або перевантаження кібернетичних ресурсів та можливостей.

Виокремлені нормативні документи та посібники є цінними ресурсами для організацій й установ, які прагнуть покращити власний рівень ІБ. Кожен з них пропонує унікальний набір рекомендацій, які можуть бути адаптовані до потреб конкретної організації, що й розглядається в подальших підрозділах.

1.2 Підхід до визначення кіберінциденту та життєвого циклу з реагування на нього

Хоча наразі поняття кіберінциденту є чітко визначеним Комітетом з питань національної безпеки США [7], кожне з обраних для дослідження нормативних документів по-своєму розширює й доповнює це поняття. Згідно [7], кіберінцидент – це дії, здійснені з використанням інформаційної системи або мережі, які призводять до фактичного або потенційного негативного впливу на інформаційну систему, мережу та/або інформацію, що в ній знаходиться. Наприклад, у NIST SP 800-61 визначено, що кіберінцидент, тобто інцидент порушення комп'ютерної безпеки, – це порушення або неминуча загроза порушення політик комп'ютерної безпеки, політик прийнятного використання або стандартних практик безпеки; крім того, наводяться деякі інші приклади [3]:

– користувачів підвели до відкриття "квартального звіту", який був надісланий електронною поштою, але насправді містив шкідливе програмне забезпечення (ПЗ). При запуску цього інструменту їх комп'ютери заражаються, і встановлюється зв'язок із зовнішнім хостом;

– користувач надає або розголошує конфіденційну інформацію через пірингові сервіси обміну файлами;

– зловмисник використовує бот-мережу для відправки великої кількості запитів на з'єднання до веб-сервера, що призводить до його відмови в обслуговуванні.

Реагування на інциденти включає кілька етапів. Перший етап – формування та навчання команди, закупівля необхідних інструментів і ресурсів. Під час підготовки організація встановлює контрольні засоби для обмеження кількості можливих інцидентів. Проте, після впровадження контрольних засобів залишковий ризик існує, тому виявлення порушень безпеки важливе для попередження інцидентів. Після факту ліквідації інциденту організація складає детальний звіт, описуючи причини, вартість та запобіжні заходи. До основних етапів процесу реагування на інцидент за NIST SP 800-61 відносяться: підготовка, виявлення і аналіз, локалізація, ліквідація та відновлення, а також подальша діяльність, що відображено на рис. 1.2.

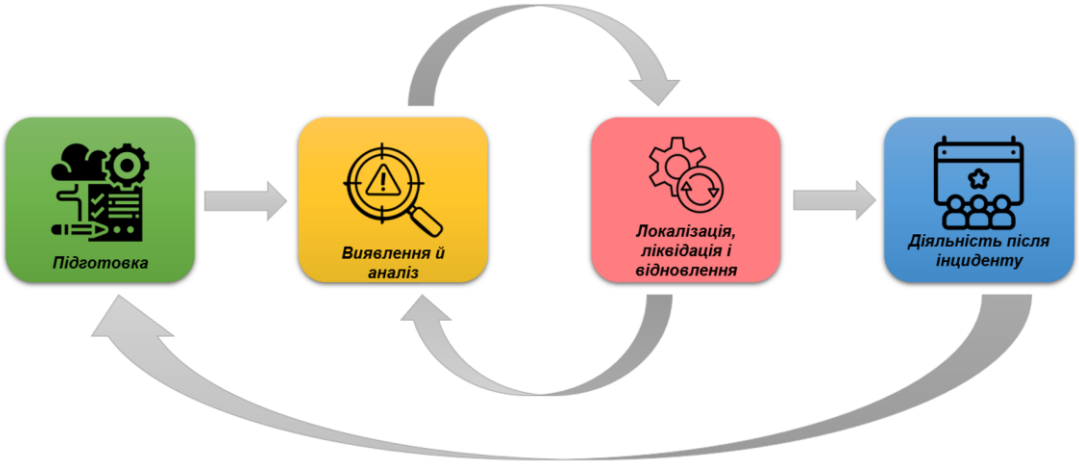

Рисунок 1.2 – Життєвий цикл реагування на кіберінцидент за NIST SP 800-61

Натомість, Рамкова концепція кібербезпеки NIST 2.0, навпаки, жодним чином не надає розширення дефініції інциденту в кіберпросторі, що, безперечно, є певним недоліком обраного документа. Проте вона дещо інакшим чином визначає порядок життєвого циклу трактуючи це шляхом «функцій» концепції, що наведені на рис. 1.3.

Рисунок 1.3 – «Функції» як життєвий цикл інциденту за CSF 2.0

Для повного розуміння питання слід розглянути кожну з функцій більш детально [4].

Управління – це процес розробки та відстеження стратегії, очікувань і політики організації з управління ризиками виникнення кіберінцидентів. Ця функція має всеохоплюючий характер і забезпечує результати, які вказують, як організація досягатиме та визначатиме пріоритети для інших функцій у контексті її діяльності та очікувань зацікавлених сторін. Діяльність з управління є критичною для включення принципів кібербезпеки в загальну стратегію управління ризиками організації. Управління виконує процес організаційного контексту; розробку стратегії та управління ризиками; визначення ролей, обов'язків та повноважень; формулювання політик, процесів та процедур; а також контроль за стратегією з дотримання принципів з кібербезпеки.

Ідентифікація – це процес, що допомагає визначити поточний рівень ризику в галузі кібербезпеки для організації. Розуміння власних ресурсів (таких як дані, обладнання, програмне забезпечення, системи, об'єкти, послуги, персонал) і пов'язаних з ними ризиків, дозволяє організації концентрувати та визначати пріоритети для своїх зусиль у відповідності до стратегії управління ризиками та потреб місії, визначених у попередній компоненті. Ця функція також включає виявлення необхідних удосконалень у політиках, процесах, процедурах та практиках організації, що підтримують управління ризиками в

галузі кібербезпеки, з метою інформування про зусилля за всіма шістьма функціями.

Захист – це процес використання заходів захисту для запобігання або зниження ризиків у контексті питання забезпечення ІБ. Після того, як активи та ризики ідентифіковані та пріоритизовані, ця функція підтримує можливість їх захисту, щоб запобігти або зменшити ймовірність і вплив кіберінцидентів. Результати цієї функції включають у себе: підвищення рівня кваліфікації персоналу шляхом навчання; безпеку даних; управління ідентифікацією, автентифікацією та контролем доступу; безпеку платформи; стійкість технологічної інфраструктури.

Виявлення – це процес виявлення та аналізу можливих атак та компрометації даних у кіберпросторі. Ця функція дозволяє вчасно виявляти та аналізувати аномалії, індикатори компрометації та інші потенційно небажані події, які можуть свідчити про активні атаки та кіберінциденти.

Реагування – це процес вжиття заходів щодо виявленого кіберінциденту. Функція підтримує можливість контролювати вплив кіберінцидентів. Результати цієї функції охоплюють управління інцидентами, аналіз, пом'якшення наслідків, звітність та комунікацію.

Відновлення – це процес ревіталізації активів та операцій, що постраждали внаслідок кіберінциденту. Функція підтримує вчасне відновлення нормальної роботи з метою зменшення впливу кібератак та забезпечення належної комунікації під час відновлювальних робіт.

Важливо зазначити, що у випадку CSF 2.0, реагування є одним із розділів документу, що показує його комплексний підхід до кіберінциденту в цілому. Документ від Американської асоціації комунальних підприємств загалом поділяє погляди NIST, тому керується 4 основними стадіями «життєвого циклу» інциденту в кіберпросторі, а саме:

1) виявлення;
2) локалізація;
3) ліквідація;
4) відновлення.

На нашу думку такий підхід є дещо базовим і не розглядає поняття кіберінциденту, як явища, ймовірність появи якого слід мінімізувати й лише потім розглядати інші стадії.

1.3 Трактування рівнів серйозності кіберінцидентів

Ефективне визначення пріоритетів обробки інцидентів є критично важливим в управлінні безпекою в кібернетичному середовищі. З огляду на обмеженість ресурсів, не можна обробляти інциденти випадковим чином або у порядку черги. Виходячи з цього, постає важливість визначення рівнів серйозності інцидентів у просторі ІБ, задля їх подальшої ефективної класифікації.

Автори NIST SP 800-61 вважають, що питання визначення пріоритету лежить у площині з оцінки трьох факторів, а саме:

– Функціональний вплив. Інциденти, спрямовані на ІТ-системи, зазвичай мають вплив на бізнес-процеси, що вони обслуговують, призводячи до негативних наслідків для користувачів. При обробці інцидентів необхідно враховувати, як вони впливають на функціональність систем. Потрібно враховувати не лише поточний, а й можливий майбутній вплив, якщо інцидент не буде негайно локалізовано.

– Інформаційний вплив. Кіберінцидент за визначенням спрямований на порушення тріади з ІБ: доступності, цілісності й конфіденційності інформації. Під час обробки інцидентів важливо враховувати, як цей витік інформації впливає на місію організації в цілому. Врахування можливих наслідків є важливим, оскільки інцидент, що призвів до витоку конфіденційних даних, може також вплинути на інші організації, якщо відповідні дані стосуються партнерів.

– Ресурси, необхідні на відновлення після інциденту. Розмір і характер інциденту визначають обсяг часу та ресурсів, потрібних для відновлення. Спеціалісти з управління інцидентами повинні уважно оцінювати зусилля, необхідні для відновлення після інциденту, і порівнювати їх з очікуваними перевагами від цього відновлення, а також з усіма вимогами, пов'язаними з обробкою інциденту.

Виходячи з наведеної вище характеристики факторів, можна впорядкувати рівні серйозності за кожним з факторів, що й наведено у табл. 1.1–1.3 [3].

Таблиця 1.1 – Рівні серйозності кіберінциденту за важливістю функціонального впливу

Рівень	Приклад
Високий	Відсутня можливість надання всіх або деяких з критичних послуг усім користувачам організації.
Середній	Організація втратила можливість надавати критично важливі послуги певній підгрупі користувачів системи.
Низький	Здійснює мінімальний ефект; організація досі здатна надавати всі важливі послуги, але помітна тенденція значного зниження рівня ефективності.
Відсутній	Жодним чином не впливає на здатність системи надавати повний перелік послуг усім користувачам.

Таблиця 1.2 – Класифікація серйозності кіберінциденту за категоріями впливу на дані

Категорія	Приклад
Втрата цілісності	Конфіденційну інформацію, або інформацію, що є власністю компанії, змінено або знищено.
Порушення конфіденційності	Було отримано доступ до конфіденційної інформації, що ідентифікує особи клієнтів та/або працівників організації.
Порушення прав власності	Відкрився доступ або стався витік несекретної службової інформації про критичну інфраструктуру організації.
Відсутній	Жодна інформація не була викрадена, змінена, видалена або скомпрометована іншим чином.

Слід акцентувати на тому, що категорії «Втрата цілісності», «Порушення конфіденційності» і «Порушення прав власності» не є взаємозамінними, тому не слід виключати можливий перетин вказаних категорій.

На жаль, CSF 2.0 не надає власної класифікації інцидентів у кіберпросторі, адже основна увага акцентована на визначенні рівнів відповідальності команди з реагування на кіберінциденти, мова про які буде йти у наступних розділах цієї роботи.

Таблиця 1.3 – Рівні серйозності кіберінциденту відповідно до зусиль для відновлення

Рівень	Приклад
Гіпотетичний	Час відновлення є передбачуваним, усі необхідні ресурси наявні.

Продовження табл. 1.3

Рівень	Приклад
Доповнений	Час відновлення є передбачуваним, необхідне залучення додаткових ресурсів для відновлення після інциденту.
Розширений	Час відновлення не є передбачуваним, необхідне залучення додаткових ресурсів для відновлення після інциденту, включаючи залучення зовнішньої допомоги.
Не підлягає відновленню	Відновлення після інциденту не є можливим.

Натомість Посібник з реагування на кіберінциденти в органах державної влади [6] надає доволі вичерпний і зрозумілий розподіл рівнів серйозності кіберінцидентів із наведенням чітких прикладів зі сфери діяльності комунальних підприємств. Крім того, наведено деталізований опис інцидентів, їх сутність, передбачувані наслідки та ресурси для ліквідації. Узагальнена інформація наведена у табл. 1.4.

Таблиця 1.4 – Рівні серйозності кіберінцидентів за версією Американської асоціації комунальних підприємств

Рівень	Опис	Сутність	Ресурси для ліквідації	Потенційні наслідки
5	Подія, яка безпосередньо впливає на постачання електроенергії на одному або декількох об'єктах	Критично важлива інформація про електроенергетичну інфраструктуру була скомпрометована	Непередбачувані; потрібні додаткові ресурси та зовнішня допомога	Створення безпосередньої загрози для надання широкомасштабних послуг критично важливої інфраструктури
4	Компрометація мережі або системи, яка контролює виробництво та постачання електроенергії			Може призвести до значного впливу на здоров'я або безпеку населення, нацбезпеку, економічну безпеку тощо
3	Компрометація або відмова в доступі до критично важливої для бізнесу корпоративної системи або послуги	Доступ до конфіденційної інформації, ІзОД або інформації, що є власністю компанії, було отримано, змінено, викрадено, видалено або зроблено недоступною	Непередбачувані; можуть бути потрібні додаткові ресурси та зовнішня допомога	

Продовження табл. 1.4.

Рівень	Опис	Сутність	Ресурси для ліквідації	Потенційні наслідки
2	Порушення безпеки некритичних бізнес-систем підприємства	Доступ до інформації, що не є персональними даними або інформацією про власність, став можливим або був здійснений	Передбачувані з наявними або додатковими ресурсами	Може вплинути на здоров'я/безпеку населення, національну/економічну безпеку, довіру суспільства тощо.
1	Підозра загрози безпеці або локальний інцидент з мінімальним впливом	Конфіденційна інформація під загрозою, але без факту її витоку	Передбачувані з наявними або додатковими ресурсами	Малоймовірний вплив на здоров'я/безпеку населення, нацбезпеку тощо
0	Повідомлення про підозрілу поведінку	Жодна інформація не була викрита, змінена або видалена	--	Відсутні

Доволі очевидним є те, що класифікація від Американської асоціації комунальних підприємств найбільш узагальнена, комплексна й всеохоплююча, порівняно з класифікаціями від NIST. Проте, разом з тим, доволі галузево направлена, що ставить під сумнів легке використання її для широкого вжитку.

1.4 Приклади практичного застосування

Розгляд прикладів практичного застосування документів з реагування на кіберінциденти є критично важливим для організацій з точки зору розвитку навичок та стратегій управління інцидентами. Такий підхід дозволяє вивчити кращі практики, що може бути важливо для запобігання майбутнім інцидентам. Розгляд прикладів також допомагає у виробленні ефективних стратегій реагування та планів дій, що враховують реальні сценарії. Крім того, цей підхід сприяє вдосконаленню документації з реагування на кіберінциденти, забезпечуючи більшу ефективність та адаптованість до потреб конкретної організації.

NIST SP 800-61 визнаний фундаментальним ресурсом у сфері кібербезпеки. Його вплив на кращі практики реагування на інциденти неоціненний, що робить документ надзвичайно цінним інструментом для організацій будь-якого розміру та галузі. Варто зазначити, що провідні

організації з кібербезпеки такі як ISACA та OAS, включають NIST SP 800-61 у свої сертифікаційні програми та рекомендації [8]. Багато урядів по всьому світу, включаючи США, Канаду, Австралію та Велику Британію, рекомендують або вимагають використовувати NIST SP 800-61 як основу для планів реагування на інциденти, зокрема Міністерство оборони США.

NIST SP 800-61 широко використовується в наукових дослідженнях з кібербезпеки, що свідчить про його наукову обґрунтованість та практичну цінність, наприклад, декілька років тому у Стокгольмському університеті відбувся захист наукової дисертації, що базувалася на розгляді питання кіберінцидентів, зокрема використовувався й матеріал NIST SP 800-61 [9].

Департамент технологій Каліфорнії прийняв NIST SP 800-61 як основу для своєї загальноштатної структури кібербезпеки. Це допомагає гарантувати послідовні практики реагування на інциденти в різних державних установах на рівні штату, покращуючи загальний стан кібербезпеки [10].

Варто зауважити, що інші розглянуті документи також широко використовуються. Розглянемо кейси використання CSF 2.0. Найпершим із них є використання документу для управління ризиками в кібернетичному просторі Банку Америки [11]. Крім того, управління службами кібербезпеки та інфраструктури США (CISA) використовує CSF 2.0 для виявлення кібератак.

Важливо зазначити, що CSF 2.0 – це не жорсткий набір правил, а гнучка система, яка може бути адаптована до потреб будь-якої організації, тому немає сумнівів щодо активного використання цього документу широкими масами в майбутньому, адже з моменту оприлюднення не пройшло навіть і року.

Останній із розглянутих документів у цьому розділі є менш популярним, тому доволі важко знайти конкретні приклади використання матеріалів Посібнику з реагування на кіберінциденти в органах державної влади. Проте, описані принципи використовуються рядом компаній з енергетичного сектору США, а саме: Duke Energy, American Electric Power, Національна асоціація електричних кооперативів у приміській місцевості, тощо.

Узагальнюючи інформацію, наведену в поточному розділі, можна сказати, що кожний із розглянутих документів має як свої переваги, так і недоліки, наведені нижче у табл. 1.5.

Таблиця 1.5 – Переваги та недоліки розглянутих нормативних документів США

Назва документа	Переваги	Недоліки
NIST SP 800-61	– Універсальність – Гнучкість – Практичність – Всесвітнє визнання	– Відсутність деталей – Необхідність великої кількості ресурсів – Відсутність усталеної версії документу
Рамкова концепція кібербезпеки NIST 2.0	– Фокус на кіберстійкості – Включення ризиків у кібернетичному просторі – Широкий спектр практик	– Складність впровадження – Відсутність усталеної версії документу
Посібник з реагування на кіберінциденти в органах державної влади	– Розроблений спеціально для органів державної влади – Містить чіткі та практичні інструкції	– Складний у використанні для сторонніх організацій

Отже, перший розділ кваліфікаційної роботи був присвячений огляду регуляторного середовища США у питанні кіберінцидентів та шляхів реагування на них, далі наведені основні висновки по розділу.

Обрані документи, такі як Спеціальна публікація NIST 800-61, Рамкова концепція кібербезпеки 2.0 і Посібник з реагування на кіберінциденти, є цінними ресурсами для організацій, які прагнуть підвищити свій рівень ІБ. Ці документи містять рекомендації і інструкції щодо реагування на кіберінциденти та планування безпекових заходів. Вони адресовані різним групам фахівців у цій галузі і надають конкретні інструменти та методики для ефективного управління ризиками.

Вибрані нормативні документи розширюють розуміння кіберінциденту, яке визначено Комітетом з питань національної безпеки США, додавши власні аспекти. NIST SP 800-61 визначає кіберінцидент як порушення політик безпеки та прийнятих стандартів безпеки, надаючи приклади. У свою чергу, CSF 2.0 не розширює визначення, проте пропонує комплексний підхід до реагування на інциденти, включаючи виявлення, локалізацію, ліквідацію та відновлення. На

нашу думку, цей підхід базується на мінімізації ризиків та має потенційні обмеження в розумінні кіберінциденту як феномену, що потребує подальшого вивчення та превентивних заходів.

Визначення пріоритетів обробки кіберінцидентів є критично важливим для ефективного управління кібербезпекою. Автори NIST SP 800-61 вказують на три фактори для оцінки пріоритету: функціональний вплив, інформаційний вплив та ресурси на відновлення. Ці фактори можуть служити основою для класифікації рівнів серйозності кіберінцидентів. Посібник з реагування на кіберінциденти в органах державної влади надає більш деталізовану класифікацію, але може бути галузево спрямованим. Таким чином, для ефективного управління кібербезпекою варто використовувати комплексний підхід, узгоджуючи його з особливостями конкретного середовища організації.

Розгляд прикладів практичного застосування документів з реагування на кіберінциденти є важливим для розвитку навичок та стратегій управління інцидентами. Такий підхід допомагає вивчити кращі практики та розробити ефективні стратегії реагування. Наприклад, NIST SP 800-61 широко використовується у наукових дослідженнях та державних програмах, що підтверджує його цінність. Крім того, CSF 2.0 та Посібник з реагування на кіберінциденти також використовуються в індустрії та державних установах, забезпечуючи адаптованість до потреб різних організацій. Кожен з цих документів має свої переваги та недоліки, які важливо враховувати при їх використанні. У табл. 1.6 наведено порівняльний аналіз обраних документів.

Таблиця 1.6 – Узагальнений порівняльний аналіз документів США

Властивість/метрика	NIST SP 800-61	NIST CSF 2.0	Посібник з реагування на кіберінциденти в органах державної влади
Мета	Надати детальні інструкції щодо створення та вдосконалення систем реагування на кіберінциденти	Запропонувати систему класифікації результатів із дотримання принципів кібербезпеки високого рівня	Надати детальні інструкції для комунальних підприємств щодо створення плану реагування на кіберінциденти
Гнучкість	Висока	Висока	Низька

Продовження табл. 1.6

Властивість/метрика	NIST SP 800-61	NIST CSF 2.0	Посібник з реагування на кіберінциденти в органах державної влади
Деталізація, обсяг та вміст	Детальні інструкції та рекомендації	Система класифікації результатів та рекомендації	Детальні інструкції та шаблони
Цільова аудиторія	Широке коло фахівців з кібербезпеки	Керівники та фахівці з кібербезпеки	Малі і середні комунальні підприємства
Актуальність	Остання версія оновлена у 2021 році	Остання версія оновлена у 2023 році	Опублікований у 2019 році
Визначення рівнів складності кіберінцидентів	Так, 3 метрики з чітким описом кожної	Відсутні	Так, 6 рівнів, наявна узагальнююча таблиця
Визначення «життєвого циклу» кіберінциденту	Наявне	Наявне у непрямому вигляді	Відсутнє
Поточне використання у світі	Широке	Широке	Майже відсутнє
Наявність інструкцій з реагування на кіберінциденти	+	+	+
Посилання на додаткові ресурси	Стандарти, рекомендації, кращі практики	Практики та засоби контролю	Галузеві та урядові партнери, державні установи
Доступність	Наявні у відкритому доступі		
Необхідні ресурси для впровадження	Значні	Середні	Незначні
Орієнтовний час на впровадження	Тривалий	Тривалий	Залежить від рівня підприємства

Усі три документи є цінними ресурсами для організацій й установ, які прагнуть покращити власний рівень ІБ, у подальших розділах кваліфікаційної роботи наявна адаптація та синтез документів для створення оптимальних покрокових інструкцій з реагування на кіберінциденти.

2 ПИТАННЯ КІБЕРІНЦИДЕНТУ В КОНТЕКСТІ УКРАЇНИ ТА ІНШИХ КРАЇН ЄВРОПИ

В Україні питання кібербезпеки стало особливо гострим після початку російської агресії у 2014 році. Наразі спостерігається активне використання кібератаки як інструменту гібридної війни для намагань дестабілізувати українську економіку та політичну систему. Інші країни Європи також стикаються зі зростанням кіберзагроз. Згідно з даними Європейського агентства з кібербезпеки, у 2022 році кількість кіберінцидентів у Європейському Союзі (ЄС) зросла на 17% [12].

Розгляд питання кіберінциденту на національному рівні паралельно з європейським є важливим через активну інтеграцію нашої держави в ЄС, остаточне обрання прозахідного вектора розвитку, а також необхідність адаптації українського законодавства до єдиних норм кібербезпеки ЄС. Це сприятиме гармонізації законодавства, створенню єдиного цифрового ринку, підвищенню рівня кібербезпеки та кращій співпраці з європейськими партнерами.

Для початку варто зауважити на дані Міжнародного індексу кібербезпеки на рис. 2.1 [1].

Рисунок 2.1 – Міжнародний індекс з кібербезпеки (співставлення країн ЄС, Великобританії та України)

Рис. 2.1 показує, що переважна більшість країн має вищі значення індексу, ніж Україна. Крім того, до уваги також взята Великобританія, яка вже не є частиною Європейського Союзу, проте займає 2-гу сходинку в цьому рейтингу після США. Отже, у розділі розглядатимуться документи та практики з реагування на кіберінциденти не лише України й країн-членкинь ЄС, а й Великобританії.

2.1 Загальні відомості

Варто зазначити, що на відміну від США, європейський простір є дуже багатогранним, відповідно, таким є і окреслення меж предметної області кіберінциденту й процедури реагування на нього. Далі наведені узагальнені дані про структуру висвітлення цього питання в окреслених країнах/альянсах.

– Великобританія;

Велика Британія має комплексний підхід до кібербезпеки, який ґрунтується на трьох основних стовпах: законодавстві, Національному центрі кібербезпеки й принципах співпраці. Розглянемо кожен з них детальніше:

1) Законодавство [13]

Закон про зловживання комп'ютерами 1990 року (The Computer Misuse Act) зі змінами, внесеними Законом про тяжкі злочини 2015 року (Serious Crime Act): цей закон визначає основні рамки для кібербезпеки в країні, включаючи криміналізацію кіберзлочинів, захист інфраструктури та повноваження правоохоронних органів.

Директива про мережеву та інформаційну безпеку (Network and Information Systems Directive, NIS) 2018 року: Регламент NIS спрямований на забезпечення підвищення безпеки мережевих та інформаційних систем, що надають основні послуги, такі як водопостачання, транспорт, енергетика, охорона здоров'я, а також цифрові послуги, які охоплюють пошукові системи, онлайн-маркетплейси та хмарні обчислення. Після виходу Великої Британії з ЄС, вона не буде впроваджувати Директиву NIS 2, але замість цього планує оновити й розширити існуючий Регламент NIS. Оновлення має включати постачальників керованих послуг, що пропонують послуги з управління даними, IT-інфраструктурою,

мережами та/або системами між бізнесом і бізнесом. Крім того, планується дозволити міністрам уряду вносити зміни до Положення про NIS без схвалення Парламенту, включаючи введення нових секторів/підсекторів або оновлення Положення про NIS. У випадку інцидентів, що впливають на надання основних та цифрових послуг, потрібно буде повідомити про це регуляторам.

2) Національний центр кібербезпеки (National Cyber Security Centre, NCSC)

Заснований у жовтні 2016 року, Національний центр кібербезпеки Великої Британії розташований у Лондоні і об'єднує експертів з підрозділу Головного управління зв'язку правлячого штабу, Центру кібернетичної оцінки CERT-UK та Національного центру захисту національної інфраструктури (який став Національним органом з питань захисту та безпеки у березні 2023 року).

NCSC виступає як єдиний контактний центр для представників малих та середніх підприємств, великих організацій, державних установ, громадськості та інших агентств. Крім того, він співпрацює з іншими правоохоронними, оборонними, розвідувальними та безпековими структурами Великої Британії та міжнародними партнерами.

3) Співпраця

Уряд Великобританії співпрацює як з приватним сектором, так і з іншими країнами та міжнародними організаціями для боротьби з кіберзлочинністю.

– країни ЄС;

Варто зазначити, що ЄС має більш розгалужену структуру в питанні кіберінцидентів і реагування на них, проте можна виділити 2 основні риси: потужна законодавча база, політика розділення задач між різними органами й структурами. Вивчимо вказані 2 риси більш якісно:

1) Законодавча база

Фундаментом цієї системи слугує NIS, прийнята у 2016 році [14]. Вона встановлює вимоги та мінімальні стандарти до кібербезпеки для операторів важливих систем: енергетика, транспорт, фінанси; та постачальників цифрових послуг: пошукові системи, онлайн-магазини.

Директива NIS окреслює детальні технічні вимоги, а також процеси повідомлення та реагування на кіберінциденти. Вона зобов'язує держави-члени ЄС призначити національні органи з кібербезпеки та створити мережу груп реагування на кіберінциденти. У контексті цієї кваліфікаційної роботи основними статтями Директиви є 14 та 16, які стосуються безпекових вимог та повідомлення про інцидент.

Також, у 2019 році був введений «Закон про кібербезпеку» [15], який розширює сферу дії Директиви NIS, встановлює більш суворі вимоги щодо безпеки, надає Агенції Європейського Союзу з питань кібербезпеки (ENISA) більш широкі повноваження та створює мережу національних координаційних органів.

Окрім вищезазначених актів, важливу роль відіграє Європейський кодекс електронних комунікацій (EECC) 2018/1972 [16], який має на меті встановити оновлені правила регулювання мереж, послуг та засобів електронних комунікацій в ЄС. Директива сприяє розвитку зв'язку та мереж високої пропускної здатності для всіх громадян і підприємств ЄС, просуваючи інтереси громадян через ефективну конкуренцію, підтримуючи безпеку мереж і послуг, а також задовольняючи потреби конкретних соціальних груп. Щодо питання кіберінцидентів, слід звернути увагу на статтю 40, що стосується зокрема безпеки мереж і послуг.

2) Органи, пов’язані з реагуванням на кіберінциденти

Наразі основними структурами, що активно задіяні у сферу кіберінцидентів є ENISA і Європейська комісія (ЄК).

ENISA – це агенція ЄС, яке прагне сприяти високому рівню кібербезпеки в Європі. Заснована в 2004 році, ENISA є силою, яка керує політикою ЄС у кібернетичному просторі, а її підтримку надає Закон ЄС про Кібербезпеку. Агенція підтримує розробку продуктів, послуг і процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки для підвищення їх надійності. Організація також співпрацює з державами-членкинями та установами ЄС, допомагаючи Європі підготуватися до майбутніх кібервикликів. Зусилля ENISA щодо підвищення обізнаності шляхом обміну

знаннями, нарощування потенціалу та підвищення обізнаності спрямовані на посилення стійкості інфраструктури в Європі, одночасно забезпечуючи цифрову безпеку громадян і європейського суспільства загалом.

Європейська комісія – один із визначальних органів, який сприяє загальному добробуту ЄС шляхом запровадження та імплементації законодавства, визначення політики й бюджету ЄС.

Згідно зі ст. 40 ЕЕСС «Агенція Європейського Союзу з питань кібербезпеки ("ENISA") має сприяти підвищенню рівня безпеки електронних комунікацій, зокрема, шляхом надання експертної допомоги та консультацій, а також сприяння обміну передовим досвідом» [17]. Крім того, за цією статтею регламентується й процес повідомлення про кіберінциденти, що наведено на рис. 2.2.

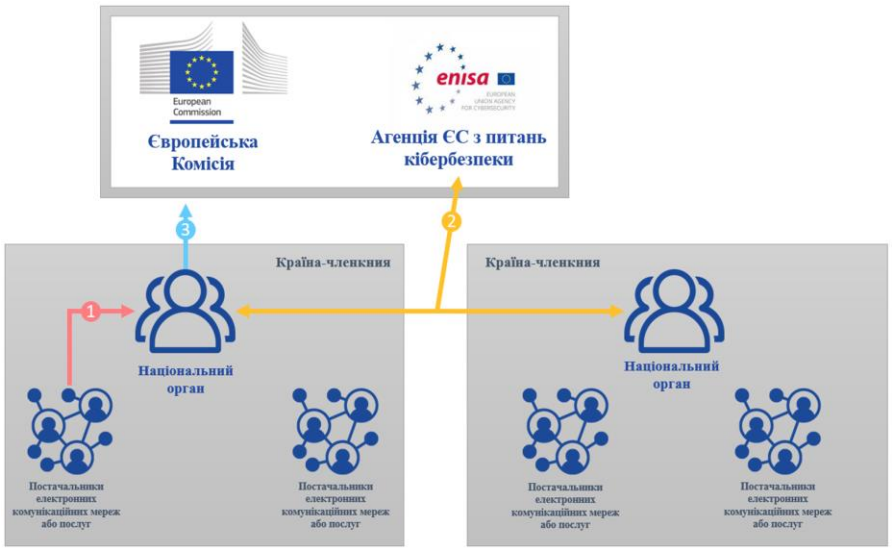

Рисунок 2.2 – Типи повідомлень про кіберінциденти, передбачені статтею 40 Європейського кодексу електронних комунікацій

З рис. 2.2 виходить, що впроваджено 3 типи повідомлень про інциденти:

а) звітування про інциденти від організацій національним органам;

б) спеціальне звітування між національними органами та ENISA;

в) щорічне підсумкове звітування національних органів ENISA і ЄК.

– Україна;

1) Законодавча база

В Україні існує певна нормативно-правова база у сфері кібербезпеки, однак зростаючі та мінливі виклики вимагають швидкого і всебічного перегляду та вдосконалення технічних і операційних аспектів кібербезпеки (нормативно-правова база, ключові зацікавлені сторони, механізми співпраці, технічна база).

Розглянемо її по порядку. Основоположним документом у цій області є Закон України (ЗУ) «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VII (останні зміни на момент написання кваліфікаційної роботи були внесені 28.07.2022).

Цим Законом створено правові та організаційні основи для забезпечення національних інтересів України, суспільства і громадян, а також архіважливих інтересів у кіберпросторі. У документі також встановлені основні цілі, прагнення й принципи державної політики у сфері кібербезпеки, зокрема розподіл повноважень між різними суб'єктами: державними установами, організаціями (установами), фізичними особами тощо. Крім того, Закон визначає ключові принципи організації їх діяльності щодо забезпечення кібербезпеки [18].

Важливими й, безперечно, визначальними статтями в Законі є ст.1, яка визначає основну термінологію (зокрема поняття кіберінциденту) і ст. 8-9, у яких наведене окреслення Національної системи кібербезпеки й визначення завдань урядової команди реагування на комп’ютерні надзвичайні події в державі CERT-UA.

На підставі статті 4 зазначеного вище ЗУ (Об’єкти кібербезпеки та кіберзахисту), Кабінет Міністрів України (КМУ) затвердив ще один важливий документ – Постанову «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, складовою якого є Порядок функціонування системи вразливостей і реагування на кіберінциденти та кібератаки від 23.12.2020 № 1295 (останні зміни на момент написання кваліфікаційної роботи були внесені 02.09.2022) [19].

Іншою гілкою ЗУ є затвердження іншого нормативного документа КМУ, а саме: Постанова «Деякі питання реагування суб’єктам забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 № 299 [20]. До Постанови затверджений відповідний Порядок, який визначає основні етапи

реагування й рівні критичності, які будуть проаналізовані в подальших підрозділах поточного розділу кваліфікаційної роботи.

На основі [18, 20], Державна служба спеціального зв'язку та захисту інформації України видала Наказ «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 03.07.2023 № 570 [21]. Варто зауважити, що рекомендації будувалися на основі нормативної бази США та ЄС, яку вже розглянуто у поточній роботі.

Завершальним документом, що регулює питання кіберінциденту та реагування на нього в Україні є Рішення Ради національної безпеки і оборони України (РНБО) «Про План реалізації Стратегії кібербезпеки України» від 01.02.2022 [22]. У контексті даної кваліфікаційної роботи важливою складовою Плану є ціль К.1 «Національна кіберготовність та надійний кіберзахист», а саме п. 36, 37 і 40, адже саме вони напряму стосуються менеджменту кіберінцидентами. Також, варто зауважити, що План є одним із нормативно-правових засад для створення згаданих вище Методичних рекомендацій. Загалом, нормативно-правову базу в питанні управління кіберінцидентами можна представити у вигляді схеми, що наявна на рис. 2.3.

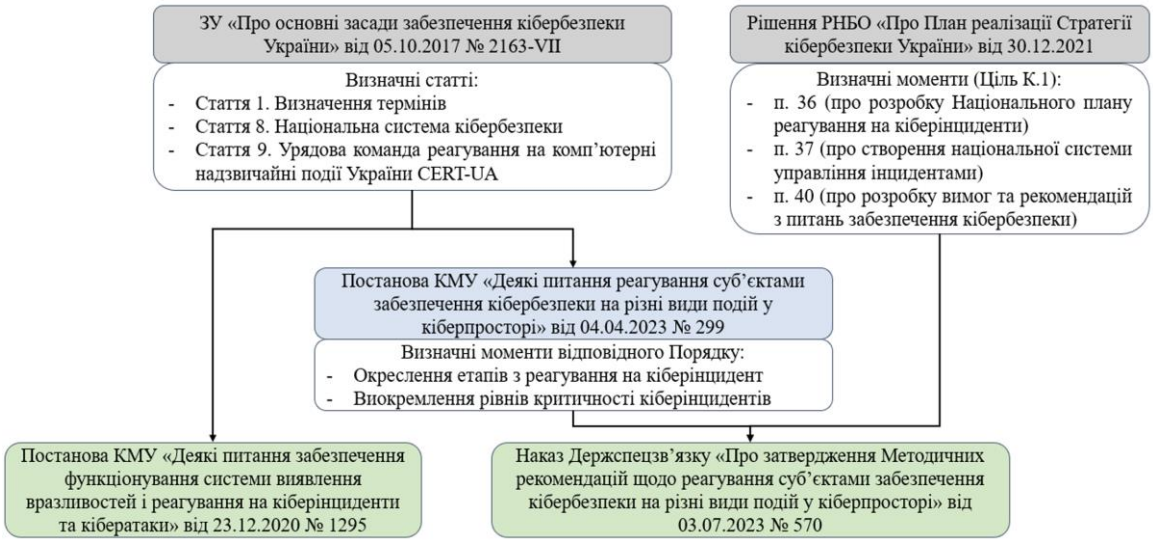

Рисунок 2.3 – Узагальнена структура нормативно-правової бази України в питанні управління кіберінцидентами

2) Орган, пов'язаний з реагуванням на кіберінциденти

Іншим невід’ємним аспектом менеджменту кіберінцидентів в Україні є наявність Команди реагування на комп'ютерні надзвичайні події України (CERT-UA). CERT-UA – це організація, що підтримується урядом і надає консультації з реагування на інциденти та безпеки організаціям в Україні. Вона була заснована в 2007 році і з 2009 року є членом Форуму команд реагування на інциденти та безпеки (FIRST) [23]. Послуги CERT-UA включають:

- реагування на інциденти: CERT-UA може допомогти організаціям розслідувати та реагувати на кіберінциденти;
- консультування з питань безпеки: Команда реагування може надати організаціям поради щодо покращення їхньої системи безпеки;
- навчання: CERT-UA пропонує навчальні курси з різних тем безпеки;
- публікації: Команда реагування регулярно публікує різноманітні матеріали, пов'язані з безпекою, включаючи інформаційні бюлетені, звіти та технічні документи;
- CERT-UA є цінним ресурсом для організацій в Україні, які шукають допомоги з реагування на інциденти та забезпечення безпеки. Послуги організації доступні як державним, так і приватним організаціям.

Можна з упевненістю стверджувати, що CERT-UA є національним аналогом як Команди комп'ютерної готовності до надзвичайних ситуацій США (US-CERT), так і організацій на європейських теренах: Національного центру кібербезпеки Великобританії і Комп’ютерних груп реагування на надзвичайні ситуації у країнах-членкинях ЄС (CSIRT).

2.2 Окреслення кіберінциденту й етапів його циклу

Різниця в підходах до опису та вирішення кіберінцидентів у різних країнах Європейського простору обумовлена різними факторами, такими як юридична система, рівень технологічного розвитку, відношення до кібербезпеки, доступність ресурсів та експертиза в цій галузі, тому постає необхідність розгляду цього питання для кожної з країн/групи країн, що розглядаються в поточному розділі кваліфікаційної роботи.

– Великобританія

NCSC визначає кіберінцидент як порушення політики безпеки системи з метою впливу на її цілісність або доступність та/або несанкціонований доступ або спробу доступу до системи або систем; відповідно до Закону про зловживання комп'ютерами [13].

Загалом, типи діяльності, які зазвичай визнаються порушенням типової політики безпеки, є такими:

1) Спроби отримати несанкціонований доступ до системи та/або даних.

2) Несанкціоноване використання систем для обробки або зберігання даних.

3) Внесення змін у прошивку, програмне або апаратне забезпечення системи без згоди власника системи.

4) Зловмисне порушення та/або відмова в обслуговуванні.

Загалом, нормативні документи уряду Великої Британії визначають 3 основні етапи у якості «життєвого циклу» реагування на кіберінцидент [23].

- Етап 1.

Підготовка до кіберінциденту передбачає проведення оцінки критичності, аналіз загроз, вирішення проблем, пов’язаних з людьми, процесами, технологіями та інформацією, а також створення базової основи.

- Етап 2.

Реагування на інцидент кібербезпеки передбачає його ідентифікацію, дослідження ситуації (включаючи визначення пріоритетів), вжиття відповідних заходів для вирішення проблеми (таких як локалізація та усунення її походження) та відновлення після інциденту.

- Етап 3.

Подальші дії після кіберінциденту. Наступні кроки можна вжити для більш ретельного розслідування інцидентів кібербезпеки, звітування про будь-які помилки чи недоліки, проведення аналізів після інцидентів, вивчення ситуації та оновлення важливої інформації, засобів контролю та процесів. У разі потреби

також буде надана допомога. Визначення етапів у вирішенні проблеми кіберінциденту показаний у схемі на рис. 2.4.

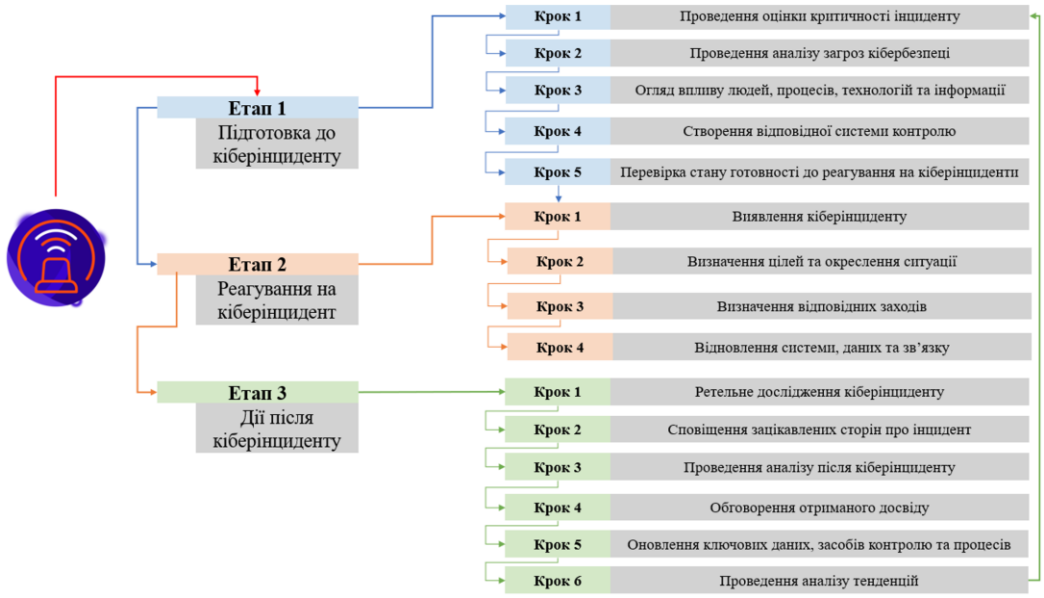

Рисунок 2.4 – Етапи й кроки вирішення кіберінциденту у Великобританії

– країни Європейського Союзу

Наразі визначення інциденту комп'ютерної безпеки наведене в EECC, а саме в пункті 42 статті 2 [15]: «"інцидент безпеки" означає подію, що має фактичний негативний вплив на безпеку електронних комунікаційних мереж або послуг». Паралельно з цим, пункт 7 статті 4 Директиви про мережеву та інформаційну безпеку визначає кіберінцидент як «будь-яку подію, що має фактичний негативний вплив на безпеку мережевих та інформаційних систем» [14].

Життєвий цикл кіберінциденту складається з наступних фаз [25]:

- виникнення – незаплановане порушення узгодженої послуги;
- виявлення – процес, який відбувається через деякий час після виникнення події;
- діагностика – визначення характеристик інциденту;
- усунення – процес реконфігурації об'єктів, що зазнали атаки;
- відновлення – процес відновлення елементів, що вийшли з ладу, до їх останнього відновлюваного стану;
- поновлення – процес надання очікуваного сервісу користувачеві;

- згортання – завершальний етап життєвого циклу інциденту, під час якого користувач та обробник інциденту перевіряють, що сервіс повністю доступний.

Рисунок 2.5 – Визначення життєвого циклу кіберінциденту в ЄС-Україна

Згаданий вище ЗУ чітко окреслює поняття інциденту кібербезпеки, або ж кіберінциденту. А саме, п. 3 ст. 1 говорить, що інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку електронних інформаційних ресурсів [18].

Також, цікавим моментом є додаткове визначення кібератаки, а саме: спрямовані дії, які націлені на порушення конфіденційності, цілісності та доступності інформації, отримання несанкціонованого доступу та порушення безпеки систем для їх функціонування, а також на використання їх для кібератак на інші системи кіберзахисту [18]. Варто зауважити, що решта нормативно-правової бази з цього питання у країні використовує поняття «кіберінцидент» та «кібератака» одночасно, це може свідчити про певне нівелювання принциповою різницею термінів.

У свою чергу, Постанова КМУ «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 № 299 визначає 6 етапів реагування на кіберінциденти: підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з

реагування [20]. Спираючись на Методичні рекомендації від Держспецзв'язку [21], можна виділити основні цілі й задачі кожного з етапів, що узагальнені у табл. 2.1.

Таблиця 2.1 – Цілі етапів реагування на кіберінциденти/кібератаки в Україні

Етап	Ціль
Підготовка	Проведення заходів з вивчення та дослідження сучасних видів кіберінцидентів і розроблення методів/механізмів для запобігання ним.
Виявлення та аналіз	Виявлення кіберінциденту, визначення рівня його критичності.
Стримування	Зведення до мінімуму серйозності та зменшення кіберінциденту шляхом обмеження або усунення можливостей зловмисника та блокування його доступу.
Усунення	Відновлення нормальної роботи шляхом ефективного видалення артефактів інциденту.
Відновлення	Пом'якшення наслідків кіберінциденту.
Аналіз ефективності заходів з реагування	Документування кіберінцидентів, інформування керівництва організації з кібербезпеки, покращення системного захисту, перегляд стратегій для запобігання подібним інцидентам у майбутньому й застосування отриманих уроків для кращого управління інцидентами.

Проте, іншою визначальною рисою врегулювання цього питання в Україні є оптимізація послідовності заходів з реагування шляхом впровадження двох питань, а саме:

- Чи наявні нові ознаки шкідливих дій?
- Чи виявлена зловмисна діяльність?

Виходячи з відповідей на ці питання, докорінно змінюється стратегія подолання кіберінциденту, схема зображена на рис. 2.6.

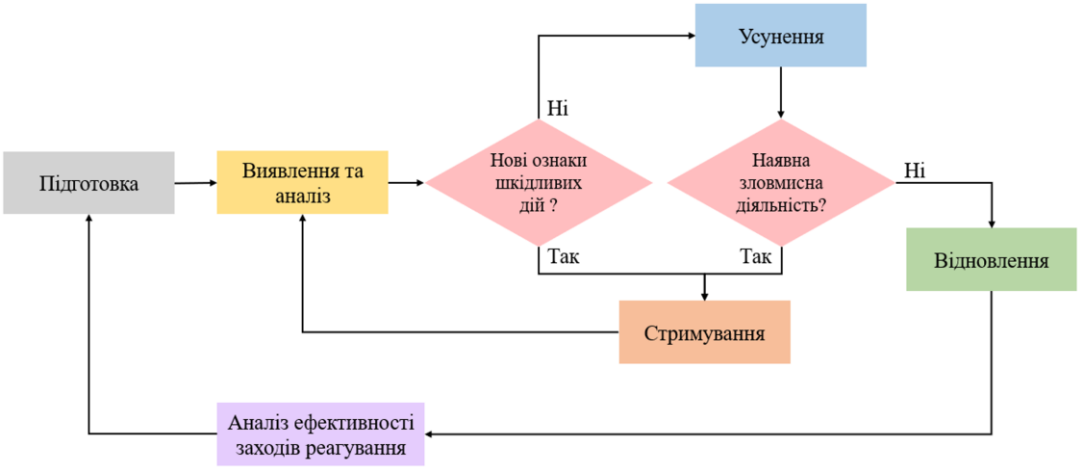

Рисунок 2.6 – Схема реагування на кіберінциденти в Україні

2.3 Таксономія кіберінцидентів і класифікація їх впливу

На відміну від США, країни європейського простору мають доволі різну класифікацію рівнів кіберінцидентів. Очевидно, що цей факт зумовлений різним розвитком і підходами до проблеми та її вирішення. Розглянемо питання таксономії кіберінцидентів і класифікацію їх впливу в окреслених раніше країнах (союзах країн) детальніше.

– Велика Британія

У Великобританії вважають, що основна відмінність між типами кіберінцидентів полягає безпосередньо в джерелі інциденту [24]. Саме тому спочатку класифікують кіберінцидент на основі типу зловмисника, його можливостей і намірів. Деякі з найпоширеніших наведені у табл. 2.2.

Таблиця 2.2 – Британська таксономія кіберінцидентів

Метрика	«Типовий» кіберінцидент	«Складний» кіберінцидент
Тип зловмисника	➢ дрібні злочинці; ➢ хактивісти; ➢ інсайдери.	➢ серйозна організована злочинність; ➢ екстремістські угрупування.
Ціль атаки	➢ широка громадськість; ➢ приватний сектор; ➢ нестратегічні урядові відомства.	➢ великі корпорації; ➢ критична національна інфраструктура; ➢ національна безпека/оборона.
Мета атаки	➢ матеріальна вигода; ➢ частковий збій у роботі.	➢ велика фінансова вигода; ➢ широкомасштабні зриви; ➢ розкриття державних таємниць; ➢ тероризм.
Можливості зловмисника	➢ низький рівень компетенції; ➢ обмежені ресурси; ➢ загальновідомі інструменти атаки.	➢ високий рівень кваліфікації; ➢ гарне ресурсне забезпечення; ➢ використання спеціальних інструментів.
Вимоги до реагування	➢ відновлення послуг; ➢ спеціальний моніторинг; ➢ обмін деякою галузевою інформацією.	➢ індивідуальні рекомендації для спеціалізованих галузей; ➢ наслідки для державних служб безпеки.

Крім того, минулого року Національний центр кібербезпеки видав пояснення моделі категоризації кіберінцидентів NCSC та правоохоронних органів Великої Британії, де визначив модель, що розділена на шість рівнів серйозності та однаково пристосована до уряду, національної інфраструктури, благодійних організацій, закладів освіти, малого бізнесу та приватних осіб [26]. Дані про кожен з рівнів наведені у табл. 2.3.

Таблиця 2.3 – Рівні серйозності кіберінцидентів за версією Національного центру кібербезпеки Великої Британії

Категорія	Опис	Орган з реагування	Типові дії
Надзвичайна ситуація національного рівня	Кібератака, яка спричиняє тривале порушення роботи основних служб країни або впливає на її національну безпеку, що призводить до серйозних економічних чи соціальних наслідків або до людських жертв.	Негайне, швидке та скоординоване міжурядове реагування. Стратегічне керівництво з боку Кабінету міністрів, технічна міжурядова координація на чолі з NCSC, тісна співпраця з правоохоронними органами.	NCSC взаємодіє з потерпілими для надання консультацій і допомагає спрямовувати запити від уряду. NCSC надає рекомендації щодо подальших заходів з реагування на кіберінциденти.
Дуже значний інцидент	Кібератака, яка має серйозний вплив на центральний уряд, основні служби Великої Британії, значну частину населення або економіку країни.	NCSC очолює реагування, тісно співпрацюючи з правоохоронними органами, якщо це необхідно.	NCSC організовує зустрічі для постраждалих організацій. При необхідності NCSC надає підтримку взаємодії з відповідним урядовим департаментом. NCSC також надає рекомендації щодо подальших заходів з реагування.
Значний інцидент	Кібератака, яка має серйозний вплив на велику організацію або на місцеві органи влади; становить значний ризик для центрального уряду чи основних служб країни.		NCSC організовує зустрічі для надання потерпілим організаціям порад. Там, де це доречно, NCSC надає рекомендації щодо подальших дій з реагування на інцидент.
Суттєвий інцидент	Кібератака, яка має серйозний вплив на організацію середнього розміру або становить значний ризик для великої організації чи місцевої влади.	Залежно від інциденту, реагуванням керує NCSC або правоохоронні органи.	Потерпілим надаються поради для сприяння їхньому реагуванню.
Незначний інцидент	Кібератака на невелику організацію або така, що становить значний ризик для організації середнього розміру, або попередні сигнали про кібератаку на велику організацію чи уряд.	Правоохоронні органи.	
Локальний інцидент	Кібератака на приватну особу або попередні ознаки кібератаки на малу чи середню організацію.	Місцева поліція очолює реагування.	

Варто зазначити, що Велика Британія на найменш значній категорії залучає місцеву поліцію, що засвідчує високий рівень підготовки навіть на такому рівні.

– Європейський союз

Як зазначалося раніше, важливими органами у питанні реагування на кіберінциденти є ЄК і ENISA, проте для визначення таксономії і класифікації інцидентів у кібернетичному просторі за їх підтримки була створена Група з питань співробітництва.

Підхід будується на характері, серйозності та впливі інциденту, масштабі національному рівні та перспективі впливу [27]. Багато європейських CSIRT або відповідних органів вже використовують цю таксономію, часто в поєднанні зі шкалою "категорій" інцидентів, що базується на серйозності. Узагальнено таксономія надана на рис. 2.7.

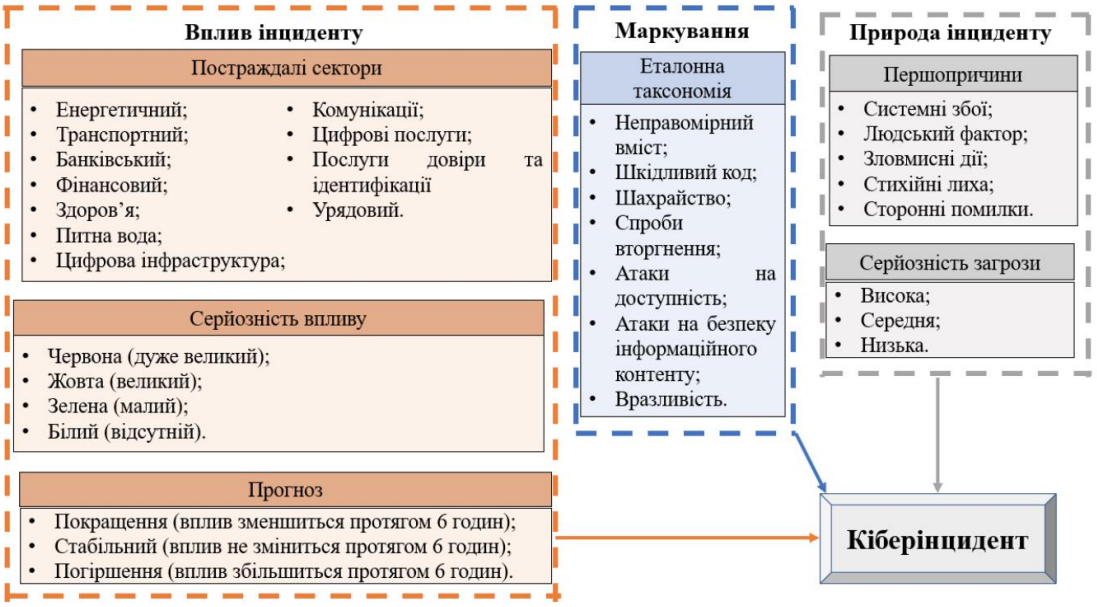

Рисунок 2.7 – Таксономія кіберінцидентів, створена Групою з питань співробітництва

Проте, окрім детальної таксономії, кожна країна-членкиня ЄС має право на визначення власної системи класифікації інцидентів. Наприклад, Франція включає порівняння свої критерії з тими, що використовуються в системі США, встановлює критерії впливу (від незначного до екстремального) і оцінює інцидент з точки зору того, чи є він збройним нападом відповідно до статті 51

Статуту Організації Об'єднаних Націй (ООН). Для присвоєння пріоритету інциденту використовується кольорова (від білого до червоного) і нумераційна (0-5) схема пріоритету інциденту [28], що показано у табл. 2.4.

Таблиця 2.4 – Характеристика рівнів кіберінцидентів у Франції

Рівень	Відповідність категорії США	Вплив	Чи характеризується як збройна агресія відповідно до ст. 51 Статуту ООН
Екстремальний (надзвичайна ситуація)	Надзвичайна ситуація 5-го рівня (чорний)	Екстремальний вплив	Ймовірно, підлягає (розглядається в кожному конкретному випадку).
Серйозна криза	Рівень 4 «Серйозний» (червоний)	Значний вплив	
Криза	Рівень 3 «Високий» (помаранчевий)	Сильний і масштабний вплив	Ймовірно, не підлягає: дії, що відповідають цим рівням, можуть становити інші міжнародно-протиправні діяння (інтервенцію, порушення суверенітету, застосування сили і т.д.).
Серйозний інцидент	Рівень 2 «Середній» (жовтий)	Сильний та обмежений вплив	
Інцидент	Рівень 1 «Низький» (зелений)	Середній та обмежений вплив	
Значна подія		Низький вплив	
Подія	Рівень 0 «Базовий» (білий)	Незначний вплив	

– Україна

Варто зазначити, що наша держава має доволі високу й деталізовану систему класифікації кіберінцидентів. Початково рівні критичності кіберінцидентів були визначені у Постанові КМУ від 04.04.2023 № 299 «Деякі питання реагування суб'єктами кібербезпеки на різні види подій у кіберпросторі». Пункт 6 прикріпленого Порядку до Постанови визначає 6 рівнів критичності: чорний, червоний, помаранчевий, жовтий, зелений і білий [20]. Як і у випадку з французькою класифікацією, помітні явні запозичення у США. Детальний опис кожного з рівнів наведений у табл. 2.5.

Таблиця 2.5 – Рівні серйозності кіберінцидентів в Україні

Рівень	Опис	Ймовірні наслідки та особливості
Надзвичайний (5)	Кіберінцидент безпосередньо ставить під загрозу стабільне, надійне та нормальне функціонування значної кількості ІКТ.	Порушення захищеності інформації та даних, що обробляються, що створює невідворотні загрози для повноцінного функціонування держави/загрози життю громадян. Можливий транскордонний вплив.

Продовження табл. 2.5

Рівень	Опис	Ймовірні наслідки та особливості
Критичний (4)	Кіберінцидент безпосередньо ставить під загрозу стабільне, надійне та нормальне функціонування значної кількості ІКТ.	Порушується захищеність інформації та даних, що обробляються, що призводить до реальних загроз для визначних елементів у функціонуванні держави. Можливе припинення виконання функцій /надання послуг критичною інфраструктурою, можливий транскордонний вплив.
Високий (3)	Кіберінцидент прямо загрожує стійкому, надійному та нормальному функціонуванню ІКТ.	Порушується захищеність інформації та даних, що обробляються, що створює потенційні загрози для важливих елементів у функціонуванні держави. Можливе припинення надання послуг критичної інфраструктури.
Середній (2)		Створюються передумови для порушення конфіденційності, цілісності, доступності інформації і даних, що обробляються, які можуть призвести до припинення надання послуг критичної інфраструктури
Низький (1)	Кіберінцидент прямо впливає на стійкість, надійність та нормальний режим роботи ІКТ.	Відсутнє порушення захищеності інформації та даних, що обробляються системами.
Некритичний (0)	Кіберінцидент не порушує стійкість, надійність та нормальний режим роботи ІКТ. Наслідки відсутні.	

Слід додати, що Методичні рекомендації від Держспецзв'язку значно розширюють цю класифікацію, адже для оптимізації процесу оцінки критичності кіберінциденту додаються критерії для визначення за трьома категоріями, опис яких наведений у табл. 2.6 [21]:

А – загроза порушення сталого, надійного та штатного режиму функціонування систем;

Б – загроза порушення захищеності інформації та даних, що обробляються в системах;

В – загрози для нацбезпеки і оборони, соціальної сфери, національної економіки, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури тощо.

Таблиця 2.6 – Значення категорій для оцінки рівня критичності кіберінцидентів

Значення	А	Б	В
1	Загроза відсутня		
2	Безпосередня загроза (для конкретної системи).	Наявні сигнали порушення.	Наявні передумови для припинення виконання функцій об'єктами критичної інфраструктури.

Продовження табл. 2.6.

Значення	А	Б	В
3	Безпосередня загроза (для декількох системи).	Спостерігається порушення.	Потенційні загрози для нацбезпеки і оборони, державної економіки тощо.
4	Безпосередня загроза (для значної кількості систем).	--	Реальні загрози для нацбезпеки і оборони, національної економіки тощо.
5	Транскордонний вплив загрози.	--	Невідворотна загроза для країни або життя громадян.

Крім оптимізації процесу визначення критичності кіберінциденту, Методичні рекомендації надають і таксономію кіберінцидентів, що наведена в узагальненому вигляді на рис. 2.8.

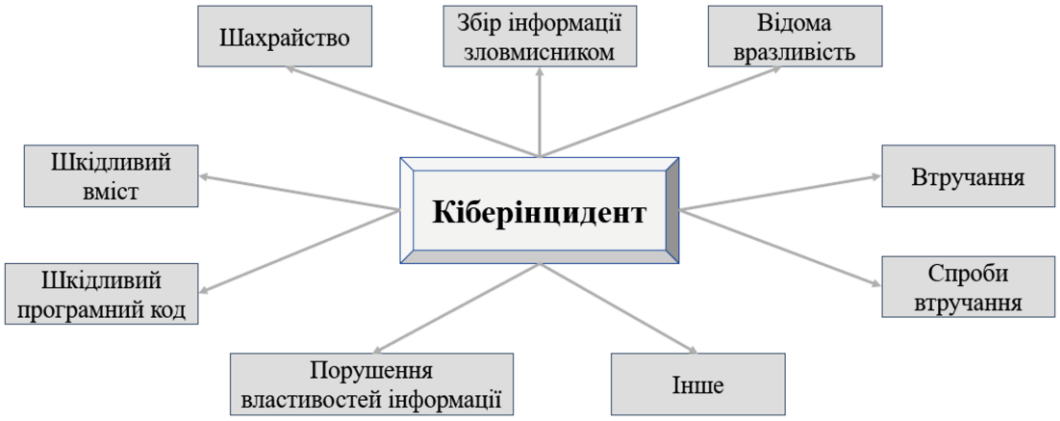

Рисунок 2.8 – Таксономія кіберінцидентів в Україні

Проаналізувавши визначення рівнів кіберінцидентів, можна з упевненістю стверджувати, що найбільш комплексним і універсальним є українське представлення. Проте, також цікавою метрикою є чітке окреслення органів для реагування на кіберінциденти за версією Національного центру кібербезпеки Великобританії (табл. 2.3). Згідно з Рішенням РНБО від 20.12.2021 [22], забезпечення розвитку мережі центрів реагування на кіберінциденти планується втілити до другого півріччя 2025 року, після чого є доцільним модернізація класифікації інцидентів у кібернетичному просторі шляхом впровадження розподілення задач з реагування між новостворених центрами.

Отже, у розділі детально розглянуто нормативно-правові й регуляторні засади/рекомендації щодо реагування на кіберінциденти в країнах-членкинях ЄС, Великої Британії та України. Можна сказати, що загалом деякі аспекти базуються на документах США. На нашу думку, це пояснюється більшим

розвитком цього питання як в контексті досвіду, так і в питанні початку дослідження проблеми, саме в США.

Нижче наведені узагальнені дані щодо різниці й унікальності процесу реагування на інциденти у кібернетичному просторі кожної з розглянутих країн у поточному розділі кваліфікаційної роботи, а саме у табл. 2.7.

Таблиця 2.7 – Узагальнений порівняльний аналіз документів ЄС, Великобританії та України

Властивість /метрика	Країни ЄС	Україна	Великобританія
Законодавча база	Директива про мережеву та інформаційну безпеку; Європейський кодекс електронних комунікацій 2018/1972.	ЗУ «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VII; Постанови КМУ «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23.12.2020 № 1295, «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 № 299; Рішення РНБО «Про План реалізації Стратегії кібербезпеки України» від 30.12.2021.	Закон «Про зловживання комп'ютерами»; Директива NIS; Закон «Про тяжкі злочини».
Дата прийняття	2016	2017	2016
Ціль	Підвищити рівень кібербезпеки в ЄС.	Захистити Україну від кіберінцидентів.	Захистити Великобританію від кіберзагроз.
Сфера дії	Оператори обов'язкових послуг.	Усі органи державної влади, місцевого самоврядування, юридичні особи та фізичні особи – підприємці.	Усі організації.
Головні органи реагування	Європейська комісія, ENISA.	Держспецзв'язок (CERT-UA).	Національний центр кібербезпеки.
Визначення поняття кіберінциденту	Наявне, закріплене законодавчо.		Наявне, не закріплене законодавчо.
Етапи з реагування на інцидент	6 етапів.	6 етапів + розгалуження в залежності від ситуації.	3 послідовні етапи.
Рівні інцидентів	Кожна країна-членкиня визначає самостійно.	6 рівнів + наявна додаткова категоризація для них.	6 рівнів.
Таксономія інцидентів	Наявна, проте не закріплена законодавчо.		
Доступність	Наявні у відкритому доступі.		

Усі три документи мають схожі цілі, але відрізняються за сферою дії, заходами та зовнішніми зв'язками. Важливо зазначити, усі документи є важливими кроками у розвитку кібербезпеки в ЄС, Великобританії та Україні.

3 ДОСЛІДЖЕННЯ ТА ОЦІНКА КІБЕРІНЦИДЕНТУ

За даними Державного центру кіберзахисту Держспецзв'язку [29] за 2023 рік кількість зареєстрованих кіберінцидентів зросла на 62,5%, порівняно з аналогічним проміжком часу в 2022 році (з 415 до 1105). Така статистика має чіткий взаємозв'язок із роботою низки законів у цій предметній галузі і показує, що проблема реагування на інциденти у кіберпросторі поступово вирішується.

Проте постає питання щодо ефективності реагування (відкритих даних з кількості успішно вирішених кіберінцидентів в Україні немає). Отже, у розділі проводитиметься оцінка кіберінциденту, що стався в Україні, за синтезом метрик і методів з попередніх розділів роботи. У якості досліджуваного інциденту вирішено розглядати кібератаку на ПрАТ «Київстар», що сталася 12.12.2023. Аналіз інциденту буде проводитися виключно з аналізу відкритих джерел інформації, адже технічні деталі є інформацією з обмеженим доступом.

3.1 Аналіз початку та класифікація інциденту

Перші дані про аномальну активність були зафіксовані о 5:26 ранку співробітниками компанії, тому в подальшому визначатимемо 5:26 12.12.2023 – датою початку кіберінциденту, що відповідає початку фази виявлення. За 1,5 години компанія почала перші сповіщення користувачів, проте не розкриваючи деталей інциденту. Ще за 5 годин, приблизно о 13:00 мережеве покриття впало до 12%, що показано на рис. 3.1 [30].

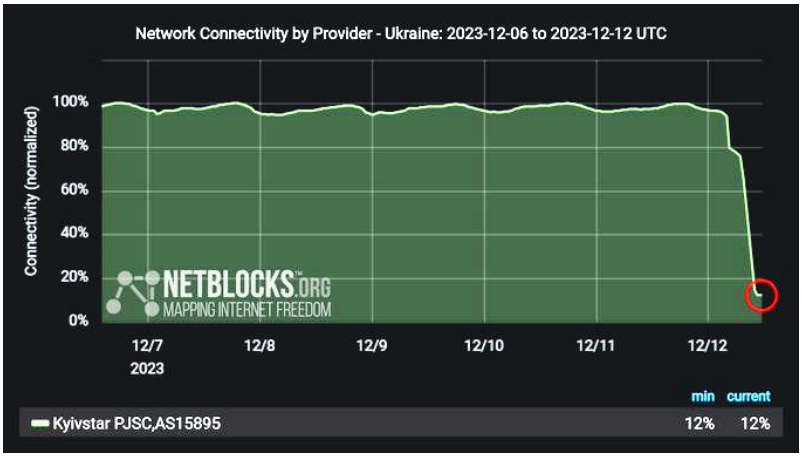

Рисунок 3.1 – Стан мережі ПрАТ «Київстар» на 13:00 12.12.2023

Згодом ситуація різко погіршилася в усіх регіонах України (покриття становило від 0% до 35%), про що свідчать дані з рис. 3.2 [30]. Варто зазначити, що паралельно з падінням стільникової мережі, різко погіршилася якість супутніх послуг і сервісів: сповіщення про повітряну тривогу, банківський сектор тощо. Після чого «Київстар» офіційно сповістив про масштабну кібератаку. Також з'явилися дані про ймовірну причину: атака на ядро мережі з каскадним падінням елементів його інфраструктури [31].

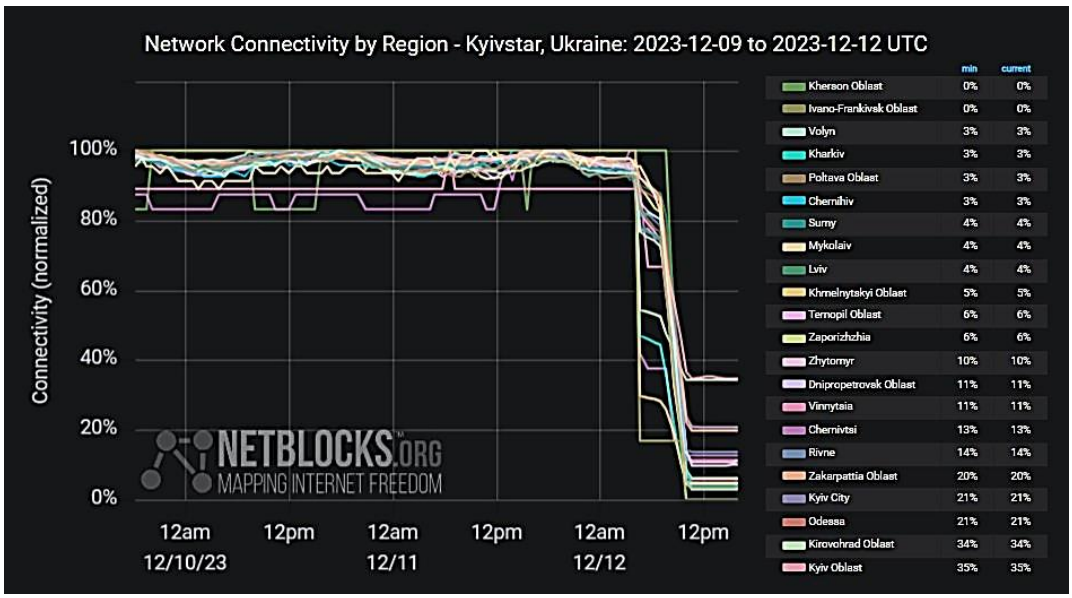

Рисунок 3.2 – Стан мережі ПрАТ «Київстар» за регіонами на 13:00 12.12.2023

Відповідно до розглянутих нормативних документів та посібників, можливо й необхідно визначити рівень серйозності кіберінциденту та його тип, виходячи з даних, які наявні за першу третину доби після виявлення.

Таблиця 3.1 – Оцінка рівня серйозності кіберінциденту за різними практиками

Документ (-и)	Країна	Рівень	Пояснення
NIST SP 800-61 [3]	США	Високий (функціональний), відсутній (вплив на дані), розширений (зусилля для відновлення).	Майже нульова можливість надання послуг, інформація про витік даних та час відновлення відсутня.
Американська асоціація комунальних підприємств [6]		4. «Рожевий» (компрометація мережі, яка є об'єктом критичної інфраструктури).	Потенційний значний вплив на інші сектори, наявний факт компрометації мережі, ресурси для відновлення непередбачувані.

Продовження табл. 3.1.

Документ (-и)	Країна	Рівень	Пояснення
Посібник від Національного центру кібербезпеки [24]	Велика Британія	Дуже значний інцидент (кібератака має серйозний вплив значну частину населення та економіку країни).	Наявний серйозний вплив на основну службу й значну частину населення країни.
Стратегія з кіберзахисту [28]	Франція	3. «Високий» (помаранчевий).	Сильний і масштабний вплив, проте не характеризується як збройна агресія відповідно до ст. 51 Статуту ООН.
Технічний посібник з інформування про інциденти в рамках ЕЕСС [17]	ЄС	А (тип), зловмисні дії (природа інциденту), дуже великий (вплив).	Перебої в наданні мережевих послуг, заявлено про хакерську атаку, вплив на більше 1 млн. користувачів.
Таксономія кіберінцидентів [27]		Постраждалі сектори: цифрова інфраструктура, комунікації; серйозність впливу: червона; прогноз: стабільний; еталонна таксономія: спроби вторгнення; першопричина: зловмисні дії; серйозність загрози: висока.	Враховані послуги компанії, заявка про довгий термін відновлення (можливо більше тижня).
Постанова КМУ від 04.04.2023 № 299 [20]; Рекомендації від Держспецзв'язку [21]	Україна	4. «Критичний» (червоний).	Загроза надійного та нормального функціонування ІКС. Значення А – 4, Б – 1, В – 4.

З табл. 3.1 видно, що рівень інциденту загалом відповідає одному з найсерйозніших у всіх без виключення системах оцінки. Цей факт свідчить про необхідність залучення сторонніх ресурсів для локалізації та подальшої ліквідації наслідків інциденту. Також відповідно до [18] інцидент може бути класифікований як «кібератака», що також є важливим для подальшого владнання ситуації та оцінки її наслідків.

3.2 Оцінка локалізації та ліквідації інциденту

Відповідно до визначеного рівня інциденту й класифікації у якості «кібератаки», ситуація має віршуватися за допомогою залучення сторонніх ресурсів, зокрема державних.

Варто зауважити, що компанія залучила до реагування на інцидент як державні органи: Службу Безпеки України для розслідування, CERT-UA для експертизи й допомоги у ліквідації, так і міжнародні корпорації: Cisco (постачання систем кіберзахисту), Microsoft (розслідування: визначення першоджерела проблеми), Ericsson (відновлення інфраструктури) [31].

У процесі локалізації спільною командою було визначено: першопричину [31], ймовірних винуватців (російське хакерське угрупування) [32], статті у відповідній відкритій кримінальній справі (ст. 361, ст. 361-1, ст. 110, ст. 111, ст. 113, ст. 437, ст. 438, ст. 255 Кримінального кодексу України) [32]. Отже, можна сказати, що складова локалізації кіберінциденту в загальній процедурі реагування проведена цілком успішно.

Етап ліквідації інциденту у цьому випадку визначається початком відновлення послуг компанії: як основних, так і додаткових. Зважаючи на специфіку (надання послуг зв'язку), за основу взята саме метрика мережевого покриття, інші послуги компанії вважаються додатковими і не є критичними.

Таблиця 3.2 – Хронологія відновлення послуг [30, 31, 33]

Дата і час	Послуга
Близько 20:00 12.12.2023	Фіксований зв'язок.
Близько 18:00 13.12.2023	Голосові дзвінки за допомогою мобільного зв'язку (частково).
14.12.2023	Голосові дзвінки за допомогою мобільного зв'язку (повністю).
	Домашній Інтернет (частково, 93%).
15.12.2023	Мобільний Інтернет (на підконтрольній Україні території).
19.12.2023	Усі критичні послуги відновлені.
21.12.2023	Майже всі додаткові послуги.

Також процес відновлення мережевих послуг компанії наведений на рис. 3.3 [30]. З рисунку видно, що протягом 48 годин мережеве покриття відновлене на 65% (з 12% до 77%) на загальній території держави.

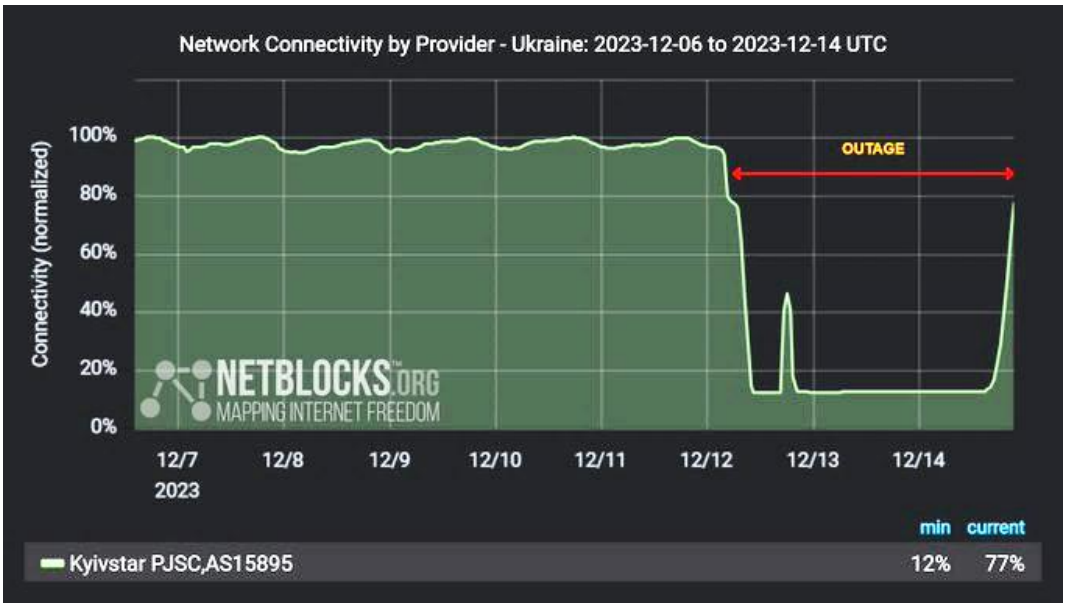

Рисунок 3.3 – Динаміка зміни мережевого покриття ПрАТ «Київстар» станом на 13:00 14.12.2023

Таким чином, на відновлення критичних послуг компанія із зовнішньою допомогою витратила близько 96 годин. Виходячи з цього можна припустити, що цей кіберінцидент був однією з наймасовіших атак на компанії-надавачі послуг зв'язку у світі. Станом на 19.12.2023 усі критичні послуги у повній мірі були відновлені, а за наступні 48 годин, тобто 21.12.2023, стали доступними майже всі додаткові послуги. Таким чином, загальний час на виявлення, ліквідацію та локалізацію інциденту склав приблизно 9 днів (близько 216 годин).

Наслідками інциденту є великі фінансові втрати на ліквідацію інциденту й відновлення втрачених потужностей (близько 100 млн. доларів США) [31], очевидне зниження рівня довіри до компанії й зменшення обсягу клієнтської бази. Відповідно до цього стає нагальною потреба до розробки рекомендації, задля превентивних дій або фази «Підготовка» у питанні реагування на кіберінцидент відповідно до [21].

Виходячи з наведеного опису кіберінциденту й проведеного аналізу доцільними є рекомендації, узагальнені в табл. 3.3.

Таблиця 3.3 – Рекомендації для компанії на основі інциденту від 12.12.2023

Рекомендація	Покращення за умови впровадження	Причина висування рекомендації
Проведення аналізу вразливостей мережі, її аудиту.	Зниження потенційного ризику майбутніх інцидентів, підвищення стійкості до них.	Факт того, що кіберінцидент взагалі стався.

Продовження табл. 3.3.

Рекомендація	Покращення за умови впровадження	Причина висування рекомендації
Розробка стратегії постійного моніторингу та аналізу мережевої активності.	Пришвидшення виявлення кіберінцидентів у майбутньому.	–
Розробка політики спеціалізованого навчання персоналу на основі атакованих складових інфраструктури компанії.	Покращення ефективності реагування.	Великий час повної ліквідації кіберінциденту.
Розробка плану реагування на подібні сценарії.		Великий час процедури реагування на кіберінцидент.
Створення резервних ліній, ресурсів тощо.	Пришвидшення відновлення послуг.	

Отже, у цьому розділі роботи проаналізовано нещодавній кіберінцидент, розгляд якого на поточний момент є дуже актуальним: визначено його рівень на основі розглянутих джерел, проведена оцінка процедур локалізації та ліквідації, висунуті рекомендації щодо покращення деяких складових з узагальненої процедури реагування на інциденти в компанії.

Можна сказати, що гіпотеза щодо повної відповідності процедур реагування на масштабні кіберінциденти чинному законодавству України є частково підтвердженою, тому що з одного боку реагування є успішним, проте прослідковується непідготовленість політики з реагування: дещо імпульсивні рішення, відсутність чіткої стратегії, значний затрачений час на відновлення критично важливих послуг, тим паче враховуючи поточні обставини в країні.

ВИСНОВКИ

У першому розділі роботи розглядалася нормативно-правова база США. За результатами пошуку та аналізу різноманітних документів, які були створені як приватними, так і державними установами, були вибрані наступні фреймворки для детального розгляду в дипломній роботі: NIST SP 800-61, CSF 2.0, посібник з реагування на кіберінциденти в органах державної влади від Американської асоціації комунальних підприємств.

Ці документи є цінними ресурсами для організацій, які прагнуть покращити свій рівень ІБ, і пропонують унікальний набір рекомендацій, що можуть бути адаптовані до конкретних потреб кожної організації. Згідно з висновками, обрані нормативні документи доповнюють і розширюють визначення кіберінциденту, яке надане Комітетом з питань національної безпеки США. Кожен з цих документів пропонує свої унікальні визначення та приклади кіберінцидентів, що враховує різноманітність та складність цього явища в сучасному кіберпросторі.

Наприклад, NIST SP 800-61 розглядає кіберінцидент як порушення або загрозу порушення політик комп'ютерної безпеки, а також наводить конкретні приклади таких інцидентів, наприклад, відкриття шкідливого ПЗ через електронну пошту. У той час як CSF 2.0 не розширює визначення кіберінциденту, його функції вживають заходів щодо попередження або зменшення ризиків у контексті забезпечення ІБ, що відображається на прикладах інцидентів, розглянутих у його рамках.

Зрозуміло, що кожен з обраних документів має свою власну методологію та підхід до реагування на кіберінциденти. NIST SP 800-61 пропонує життєвий цикл реагування на інцидент, а CSF 2.0 базується на функціях, що включають управління, ідентифікацію, захист, виявлення, реагування та відновлення. Ці відмінності в підходах до реагування на кіберінциденти вказують на різноманітність та комплексність самого поняття кіберінциденту, а також важливість розгляду кожного конкретного випадку з урахуванням специфіки організації та її потреб.

Розглянуто важливість визначення рівнів серйозності кіберінцидентів для ефективного управління безпекою в кібернетичному середовищі. Зазначено, що обмеженість ресурсів вимагає установлення пріоритетів обробки інцидентів, а це можливо завдяки оцінці трьох факторів: функціонального та інформаційного впливу і ресурсів для відновлення. Наведено приклади класифікацій з різних документів, вказано на їхні переваги та недоліки.

Результати аналізу показали, що визначення рівнів серйозності кіберінцидентів допомагає у забезпеченні негайного й ефективного реагування на інциденти відповідно до їхньої важливості. Оцінка функціонального й інформаційного впливу, а також ресурсів для відновлення, дозволяє встановити пріоритети та залучити необхідні ресурси. Також виділено, що класифікації можуть варіюватися в залежності від галузевих особливостей та вимог організацій, і немає універсального підходу, що підходить для всіх сценаріїв.

Отже, управління кібербезпекою передбачає ретельне визначення рівнів серйозності кіберінцидентів, яке забезпечує ефективне реагування та оптимальне використання ресурсів для ліквідації інцидентів. Розробка та впровадження таких систем класифікації є важливим етапом у побудові надійної стратегії забезпечення ІБ.

Другий розділ дипломної роботи був присвячений Україні та країнам європейського простору. У ході аналізу визначено, що різні країни мають різні підходи до кібербезпеки. Велика Британія використовує комплексний підхід, що ґрунтується на законодавстві, NCSC та співпраці. ЄС має більш розгалужену систему з потужною законодавчою базою та розподілом задач між різними органами, такими як ENISA та ЄК. Україна має певну нормативно-правову базу, але вона потребує вдосконалення.

У кожній країні Європейського простору підходи до опису та вирішення кіберінцидентів різняться через різноманітні фактори, такі як юридична система, рівень технологічного розвитку, відношення до кібербезпеки, доступність ресурсів та експертиза в цій галузі. У Великобританії NCSC визначає кіберінцидент як порушення політики безпеки системи, а законодавство чітко регламентує життєвий цикл реагування на інциденти. У країнах ЄС і Україні

терміни "кіберінцидент" та "кібератака" мають різне визначення, що свідчить про різні підходи у законодавстві.

Визначено основні етапи реагування на кіберінциденти в кожній країні. У кожній країні це питання регулюється відповідно до національних законодавчих актів та документів, що враховує особливості країни і гарантує ефективне управління кібербезпекою. Враховуючи складність кіберзагроз і швидкі темпи технологічного розвитку, ця тенденція до індивідуального підходу є необхідною для забезпечення ефективного захисту кіберпростору та критичної інфраструктури кожної країни.

Розглянуті країни, зокрема Велика Британія та ЄС, використовують різні методи та критерії для класифікації кіберінцидентів. У Великобританії основний акцент робиться на типі зловмисника, цілі атаки та можливостях зловмисника, в той час як ЄС спрямовує увагу на серйозність та масштаб інциденту. Ця різноманітність свідчить про важливість адаптації класифікаційних систем до конкретних потреб та контексту кожної країни. Європейські країни демонструють гнучкість у визначенні власних систем класифікації кіберінцидентів, що дозволяє їм враховувати різні аспекти впливу інцидентів на національну безпеку, економіку та суспільство. Така пристосованість сприяє ефективнішому управлінню ІБ та реагуванню на загрози.

Україна має високий рівень деталізації та систематизації системи класифікації кіберінцидентів. Це відображається у встановленні шести рівнів критичності, що дозволяє точно визначити серйозність інцидентів та вживати адекватних заходів реагування. Українська система класифікації кіберінцидентів включає елементи, які були запозичені з американської та інших систем класифікації, але вона також адаптована до внутрішніх потреб і контексту держави. Методичні рекомендації від Держспецзв’язку додатково розширюють класифікацію кіберінцидентів і надають критерії для оцінки критичності. Це сприяє оптимізації процесу реагування на кіберінциденти та дозволяє ефективніше управляти цими загрозами.

У цілому, українська система класифікації кіберінцидентів є комплексною, деталізованою та добре адаптованою до внутрішніх потреб країни. Проте,

важливо продовжувати вдосконалювати цю систему, враховуючи мінливий характер кіберзагроз та навколишній контекст.

В останньому розділі роботи, з метою оцінки ефективності реагування на кіберінциденти в Україні, проведений аналіз конкретного інциденту – кібератаки на оператора мобільного зв'язку «Київстар». Аналіз дозволив з'ясувати наявні проблеми та запропонувати шляхи їх вирішення. За допомогою різних методик та метрик проведена оцінка серйозності кіберінциденту. У результаті аналізу встановлено, що кібератака відповідає одному з найсерйозніших рівнів в усіх системах класифікації, що вимагає негайних заходів з реагування.

Компанія успішно залучила до реагування державні органи та міжнародні корпорації, що є важливим кроком для ефективного ліквідації наслідків інциденту. За допомогою спільної команди було визначено першопричину, винуватців, та вжиті заходи для відновлення інфраструктури компанії. Процес відновлення послуг був успішним, хоча зайняв значний час (близько 216 годин) і потребував значних фінансових витрат (близько 100 млн. доларів). Це вказує на серйозність та масштабність кібератаки.

На основі аналізу інциденту запропоновано ряд рекомендацій для покращення кіберзахисту компанії, включаючи проведення аналізу вразливостей мережі, розробку стратегії моніторингу та аналізу активності, навчання персоналу, розробку плану реагування на подібні сценарії та створення резервних ресурсів.

Зокрема у результаті отримане часткове підтвердження гіпотези, висунутої у вступі. Вважаємо матеріал у дипломній роботі чітко викладеним і добре систематизованим. Результати роботи можуть бути застосовані в галузі кібербезпеки, зокрема в урядових організаціях, приватному секторі, освітніх і наукових установах для розробки та удосконалення стратегій управління кіберінцидентами. Варто зазначити, що необхідно продовжувати рух у цьому напрямку, адже він є перспективним і актуальним.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Global Cybersecurity Index 2020 | International Telecommunication Union. (2021). Режим доступу: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf .

2. Олександр Пелюх Порівняльна оцінка систем реагування на кіберінциденти в Сполучених Штатах Америки | Олександр Пелюх, Марина Єсіна, Дмитро Голубничий | Computer science and cybersecurity. – Харківський національний університет імені В. Н. Каразіна, 2023, Випуск 1(23) – С. 34–40. – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/23091/21101.

3. NIST SP 800-61 | NIST. (2021, Квітень 23). Режим доступу: https://www.nist.gov/privacy-framework/nist-sp-800-61.

4. The NIST Cybersecurity Framework 2.0. | NIST. (2023, Серпень 8). Режим доступу: https://doi.org/10.6028/nist.cswp.29.ipd.

5. Framework Documents | NIST. (2014, Лютий). Режим доступу: https://www.nist.gov/cyberframework/framework.

6. Public Power Cyber Incident Response Playbook | American Public Power Association. (2019, Серпень). Режим доступу: https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook.

7. CNSSI 4009 | Committee on National Security Systems. (2022, Березень 2). Режим доступу: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

8. Maritime cybernetic security in the western hemisphere. | Organization of American States. (2021). Режим доступу: https://www.oas.org/es/sms/cicte/docs/La-seguridad-cibernetica-maritima-en-el-Hemisferio-Occidental-introduccion-y-directrices.pdf.

9. Cybersecurity Incident Response: A Socio-Technical Approach| Al Sabbagh, B., Stockholm University (2019, Червень 7). Режим доступу: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-167873.

10. California, S. O. Security Policy - CDT. CDT. Режим доступу: https://cdt.ca.gov/security/policy/.

11. Key governance topics. Bank of America. Режим доступу: https://about.bankofamerica.com/en/making-an-impact/key-governance-topics.

12. ENISA Threat Landscape 2023. (2023, Жовтень 19). ENISA. Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

13. Massey, R., Machin, E., & Bond, R. B. (2023, Листопад 14). Cybersecurity Laws and Regulations England & Wales. Режим доступу: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/england-and-wales.

14. Directive - 2016/1148 - EUR-LEX. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1707927214161.

15. Regulation - 2019/881 - EUR-LEX. Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

16. Directive - 2018/1972 - EUR- LEX. Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972&qid=1707927623379.

17. Technical Guideline on Incident Reporting under the EECC. (2021, Березень 22). ENISA. Режим доступу: https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc?v2=1.

18. ЗУ «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VII. Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#n56.

19. Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23.12.2020 № 1295. Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#n11.

20. Постанова Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 № 299. Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF/print.

21. Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі». Режим доступу: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

22. Рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України» від 30.12.2021. Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/n0087525-21#n16.

23. Пелюх, О., Єсіна, М., Голубничий, Д. (2023). Оцінка CERT-UA на основі Моделі зрілості CSIRT ENISA. Радіотехніка, 2(213), 41–48. Режим доступу: https://doi.org/10.30837/rt.2023.2.213.04.

24. CREST International. (2013). Cyber Security Incident Response Guide Version 1. Режим доступу: https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf.

25. Good Practice Guide for Incident Management. (2010, Грудень 20). ENISA. Режим доступу: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

26. National Cyber Security Centre. (2023, Серпень 23). Categorising UK cyber incidents. Режим доступу: https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents.

27. NIS Cooperation Group. Cybersecurity Incident Taxonomy. (2018, Липень). Режим доступу: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf .

28. Revue stratégique de cyberdéfense | SGDSN. (2018, Лютий 12). SGDSN. Режим доступу: https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf.

29. Державний центр кіберзахисту Держспецзв’язку. (2024, Січень 08). Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. Режим доступу: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a.

30. NetBlocks (@netblocks) (2023, Грудень, 12-14). X (Formerly Twitter). Режим доступу: https://twitter.com/netblocks.

31. Forbes Україна. (2023, Грудень 12). «Перше інтерв'ю президента «Київстару» після кібератаки, яка паралізувала оператора». Режим доступу: https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855.

32. Служба Безпеки України. (2023, Грудень 12). «СБУ відкрила кримінальне провадження за фактом кібератаки на «Київстар»». Режим доступу: https://ssu.gov.ua/novyny/sbu-vidkryla-kryminalne-provadzhennia-za-faktom-kiberataky-na-kyivstar.

33. ПрАТ «Київстар». (2023, Грудень 19). «Робимо все, щоб відновити наші сервіси після хакерської атаки». Режим доступу: https://kyivstar.ua/news/id191220231000.