Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп’ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Ольга

МЕЛКОЗЬОРОВА

_____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Дослідження та аналіз методів та заходів кібербезпеки для критичної інфраструктури»

оцінка « »

Голова ЕК

Олександр ЛЕМЕШКО _____

Керівник : к.т.н., доцент Єсіна М.В.

Рецензент : к.т.н. Бобух В. А

Виконавець : студент(ка) групи КБ-61

Самойленко О.А.

Харків – 2023

РЕФЕРАТ

Темою магістерської дисертації є дослідження та аналіз методів та заходів кібербезпеки для критичної інфраструктури. Робота містить 95 сторінки, зокрема 7 ілюстрацій, 5 таблиць та 49 джерел інформації.

Тема магістерської дисертації є актуальною, оскільки полягає у синтезі теоретичних та практичних аспектів кібербезпеки, адаптації сучасних методів аналізу загроз та ризиків для потреб критичної інфраструктури, а також у розробці комплексного підходу до прогнозування і запобігання кібератакам.

Магістерська робота присвячена дослідженню та аналізу методів та заходів кібербезпеки для захисту критичної інфраструктури. Робота розглядає різні підходи до забезпечення безпеки критичних систем, включаючи виявлення загроз, заходи захисту, відновлення після інцидентів та моніторинг. У ході дослідження використовуються сучасні технології та стандарти кібербезпеки, щоб надати рекомендації щодо оптимального застосування цих методів до критичної інфраструктури. Особлива увага приділяється забезпеченню ефективного функціонування систем у умовах потенційних кіберзагроз. Результати цього дослідження сприятимуть підвищенню рівня захищеності критичних об'єктів та сприяють зміцненню заходів кібербезпеки для забезпечення надійності та стійкості критичної інфраструктури.

Ключові слова: КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, ЗАХИСТ ВІД КІБЕРЗАГРОЗ, МЕТОДИ КІБЕРБЕЗПЕКИ, АНАЛІЗ ЗАГРОЗ, ВІДНОВЛЕННЯ ПІСЛЯ ІНЦИДЕНТІВ, МОНІТОРИНГ БЕЗПЕКИ.

ABSTRACT

The topic of the master's thesis is the research and analysis of cybersecurity methods and measures for critical infrastructure. The work contains 95 pages, including 7 illustrations, 5 tables and 49 sources of information.

The topic of the master's thesis is relevant, as it consists in synthesising theoretical and practical aspects of cybersecurity, adapting modern methods of threat and risk analysis for the needs of critical infrastructure, and developing a comprehensive approach to predicting and preventing cyberattacks.

Master's thesis is devoted to the research and analysis of cybersecurity methods and measures to protect critical infrastructure. The work examines various approaches to securing critical systems, including threat detection, protection measures, incident recovery and monitoring. The study uses modern cybersecurity technologies and standards to provide guidance on the optimal application of these methods to critical infrastructure. Particular attention is paid to ensuring the effective functioning of systems in the face of potential cyber threats. The results of this study will help to increase the level of security of critical facilities and contribute to strengthening cybersecurity measures to ensure the reliability and resilience of critical infrastructure.

Keywords: CYBERSECURITY, CRITICAL INFRASTRUCTURE, PROTECTION AGAINST CYBER THREATS, CYBERSECURITY METHODS, THREAT ANALYSIS, INCIDENT RECOVERY, SECURITY MONITORING.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

NTT	-	Nippon Telegraph and Telephone.
ISO	-	International Organization for Standardization, Міжнародна організація зі стандартизації.
ІС	-	інформаційні системи.
СУІБ	-	системи управління інформаційною безпекою.
ІКТ	-	інформаційно комунікаційні технології.
NIST	-	National Institute of Standards and Technology, Національний інститут стандартів та технологій.
ДСТУ	-	Державні стандарти України.
НАТО	-	Організація Північноатлантичного договору.
CWIX	-	Coalition Warrior Interoperability Exercise.
FIRST	-	Forum for Incident Response and Security Teams.
CERT	-	Computer Emergency Response Team, Команда реагування на надзвичайні ситуації.
СКУД	-	системи керування та управління доступом.
IEC	-	International Electrotechnical Commission, міжнародна організація зі стандартизації.

ВСТУП

У сучасному світі, де інформаційні технології проникають у всі сфери людського життя, питання кібербезпеки набуває особливої актуальності. Розвиток цифрових технологій, з одного боку, суттєво підвищує ефективність та гнучкість процесів управління критичними інфраструктурами, а з іншого – збільшує ризики виникнення кіберінцидентів, які можуть мати катастрофічні наслідки.

Забезпечення кібербезпеки критичної інфраструктури є надважливим завданням для будь-якої держави, адже від стійкості таких систем залежить не тільки економічна стабільність, але й здоров'я та благополуччя громадян, національна безпека, і навіть стійкість державного управління.

Метою даної магістерської роботи є аналіз існуючих методів та заходів кібербезпеки, призначених для захисту критичної інфраструктури, а також створення рекомендацій щодо нових підходів, що відповідають сучасним викликам та загрозам. Об'єктом дослідження виступають системи критичної інфраструктури, а предметом – методи та заходи забезпечення їх кібербезпеки.

Для досягнення поставленої мети у роботі вирішуються наступні завдання:

- Аналіз поточного стану кіберзахисту систем критичної інфраструктури.
- Вивчення міжнародного досвіду в сфері кіберзахисту систем критичної інфраструктури.
- Оцінка ризиків та ідентифікація потенційних загроз.
- Розробка рекомендацій щодо підвищення ефективності існуючих методів кібербезпеки.
- Розробка узагальненої моделі потенційного порушника та визначення оптимальних заходів протидії.

Методологія дослідження базується на комплексному підході, який включає як теоретичний аналіз наукової літератури та нормативних актів, так і практичне дослідження існуючих систем кібербезпеки. Використовуються кількісні та якісні методи аналізу, в тому числі моделювання загроз, оцінка ризиків, експертні опитування, а також сценарійне планування для ідентифікації та аналізу можливих векторів атак. Емпірична база дослідження включає в себе дані від відповідних установ та організацій, а також результати комп'ютерного моделювання.

Наукова новизна роботи полягає у синтезі теоретичних та практичних аспектів кібербезпеки, адаптації сучасних методів аналізу загроз та ризиків для потреб критичної інфраструктури, а також у розробці комплексного підходу до прогнозування і запобігання кібератакам. Практична значимість дослідження обумовлена розробкою рекомендацій, які можуть бути використані органами державного управління, підприємствами та організаціями для зміцнення безпеки своїх інформаційних систем.

Робота виконана на кафедрі безпеки інформаційних систем і технологій, що забезпечило доступ до сучасних наукових матеріалів, методів аналізу та оцінки, а також дозволило взаємодіяти з провідними фахівцями в області кібербезпеки.

Таким чином, дана магістерська робота є актуальним та значущим внеском у сферу забезпечення безпеки критичної інфраструктури, що відповідає сучасним вимогам та викликам.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У даному розділі ми детально розглянемо концепцію та ключові компоненти критичної інфраструктури, акцентуючи на її значенні для національної безпеки та стабільності. У цьому розділі буде здійснено аналіз існуючих систем критичної інфраструктури, оцінюючи їхню важливість та вразливість перед обличчям сучасних кіберзагроз. Також до нього буде включено аналіз ризиків та загроз, з якими стикається критична інфраструктура, включаючи потенційні кібератаки та інші види втручань.

Розділ також містить дослідження важливих стандартів та нормативних документів, які регулюють забезпечення безпеки критичної інфраструктури, з особливим фокусом на міжнародних та національних стандартах кібербезпеки. При цьому враховуються різноманітні аспекти, від технічних до організаційних, які формують комплексний підхід до кібербезпеки. Окремий розділ присвячено аналізу правового регулювання кібербезпеки, як в Україні, так і в інших країнах, з акцентом на останніх змінах та тенденціях в цій сфері.

1.1 Аналіз концепції критичної інфраструктури

У сучасному світі, де технології та глобалізація невпинно просуваються вперед, поняття критичної інфраструктури набуває все більшої ваги. У даному підрозділі розглянемо визначення критичної інфраструктури, розглядаючи її ключові компоненти та сектори, які мають вирішальне значення для забезпечення національної безпеки, економічного благополуччя, громадського здоров'я та безпеки.

Концепція критичної інфраструктури наразі перебуває у процесі формування, при цьому зростає активність у сферах законодавства та наукових досліджень, пов'язаних з цим поняттям. У деяких регуляторних документах вже висловлені

спроби визначити це поняття. Зокрема, у Постанові Кабінету Міністрів України від 23 серпня 2016 року № 563 критична інфраструктура трактується як набір найважливіших об'єктів для економіки, промисловості, функціонування суспільства та безпеки населення, руйнація або порушення функціонування яких може вплинути на національну безпеку та оборону, навколишнє середовище, призвести до великих фінансових збитків та людських втрат [2]. У розпорядженні Кабінету Міністрів України від 6 грудня 2017 року № 1009-р критична інфраструктура визначена як сукупність об'єктів, які мають стратегічне значення для економіки та безпеки держави та суспільства, і порушення яких може завдати шкоди життєво важливим національним інтересам України [3].

Визначення "критичної інфраструктури" включає в себе об'єкти, системи, мережі або їх складові, неполадки чи знищення яких можуть призвести до серйозних негативних наслідків для соціального та економічного стану держави, а також негативно вплинути на рівень її обороноздатності та національної безпеки. У мирний час робота критичної інфраструктури асоціюється з забезпеченням життєво необхідних функцій у суспільстві, охороною базових потреб його членів та наданням відчуття безпеки та захищеності. Критична інфраструктура України охоплює такі системи та ресурси, як фізичні, так і віртуальні, критично важливі для підтримки суспільних функцій та послуг, порушення яких може мати драматичні наслідки для життя суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

Підсумовуючи можна зазначити, що поняття критичної інфраструктури визначають, враховуючи такі елементи:

1) загальне визначення критичної інфраструктури як сукупності об’єктів;

2) ознаки, за якими об’єкти критичної інфраструктури визначаються як такі;

3) можливі впливи на об’єкти критичної інфраструктури та їх наслідки;

4) державні, суспільні інтереси та відносини, яким може бути завдано шкоди.

Проте змістове наповнення цих елементів неоднакове, адже трансформація поняття критичної інфраструктури відбувається під впливом об’єктивних чинників й обставин, що визначають пріоритетність тих чи тих проблем, пов’язаних із забезпеченням нормального функціонування та захисту певних об’єктів [4].

Об’єкти критичної інфраструктури – об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1]. Об'єкти критичної інфраструктури є ключовими стратегічними об'єктами, які забезпечують життєдіяльність країни та її економічну стабільність. Вони включають основні підприємства та установи, чия раптова зупинка або знищення може призвести до серйозних наслідків, включно із загрозами національній безпеці, пошкодженню навколишнього середовища, зменшенню обороноздатності, а також матеріальним та фінансовим збиткам. Крім того, такі інциденти можуть мати трагічні наслідки, включаючи втрати людських життів. У табл. 1.1 наведено різні підходи до визначення поняття об'єкти критичної інфраструктури, що допоможуть зрозуміти їх важливість для світу в цілому.

Таблиця 1.1 – Підходи до визначення поняття об'єкти критичної інфраструктури

Підхід	Організація/Країна	Визначення
Міжнародний	Європейський Союз	Об'єкти, чия непрацездатність або руйнування матиме серйозний вплив на здоров'я, безпеку, економічне або соціальне благополуччя громадян, або на ефективне функціонування урядів держав-членів.
Національний	США	Ключові ресурси, послуги та функції, відмова або знищення яких матиме значний негативний вплив на національну безпеку, національну економічну безпеку, національне громадське здоров'я або безпеку, або будь-яке поєднання цих елементів.
Академічний	Наукові дослідження	Системи та активи, незамінні для підтримки рівня життя, чия втрата б вплинула на національну безпеку, економіку, громадське здоров'я або безпеку.

Продовження табл. 1.1 – Підходи до визначення поняття «б'єкти критичної інфраструктури

Промисловий	Різні галузеві джерела	Критичні активи, системи та мережі, фізичні або віртуальні, життєво важливі для Сполучених Штатів таким чином, що їх непрацездатність або руйнування матиме вирішальний вплив на національну безпеку, національну економічну безпеку, громадське здоров'я або безпеку, або будь-яку комбінацію цих аспектів.
Національний	Україна	Об'єкти, які є важливими для забезпечення життєво необхідних функцій держави, здоров'я та безпеки населення, та чия дезорганізація або знищення може мати серйозні наслідки для національної безпеки країни та її громадян.

1.1.1 Огляд існуючих систем критичної інфраструктури

Критична інфраструктура охоплює широкий спектр систем і служб, які є фундаментальними для забезпечення нормального функціонування суспільства, його економічного зростання та забезпечення безпеки населення. У даному підрозділі розглянемо основні системи критичної інфраструктури, включаючи їхні основні компоненти та важливість.

Віднесення об’єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Віднесення об’єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами.

Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них,

можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об’єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість таких об’єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури [1].

Секторальні органи у сфері захисту критичної інфраструктури, використовуючи перелік секторів критичної інфраструктури, ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури [23]. У додатку А наведено перелік секторів критичної інфраструктури відповідно до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109.

1.2 Аналіз ризиків та загроз для безпеки критичної інфраструктури

У Звіті про глобальні ризики [6] Всесвітнього економічного форуму за 2020 рік кібератаки на об'єкти критичної інфраструктури визначені як один з головних пріоритетів. За даними ВЕФ, атаки на об'єкти критичної інфраструктури стали звичним явищем у багатьох галузях, включаючи енергетику, охорону здоров'я та транспорт.

Нова реальність полягає в тому, що майже всі об'єкти критичної інфраструктури працюють в цифровому середовищі, а оскільки інформаційні технології продовжують розвиватися, вразливості також розвиваються. Глобальний зв'язок, Інтернет речей і поява "розумних" міст ще більше збільшують глобальну поверхню загроз і створюють нові можливості для зловмисників. Суб'єкти загроз, включаючи національні держави, терористів і організовану злочинність, стали більш витонченими і розглядають критичну інфраструктуру як пріоритетну ціль.

Кілька нещодавніх прикладів кібератак на об'єкти критичної інфраструктури:

– Ізраїль – національне кібер-агентство успішно зупинило проспонсовану Іраном державну атаку на системи водопостачання.

– Тайвань – національна енергетична компанія зазнала атаки з використанням програми-вимагача, а великий провайдер зв'язку NTT зазнав збою в роботі мережі.

– США – атака з вимогою викупу була спрямована на об'єкти критичної інфраструктури, що належать до установки для стиснення природного газу. Влада також оголосила про атаку іноземного уряду на два муніципалітети США.

– США – в результаті безпрецедентної атаки хакери скомпрометували систему водопостачання міста у Флориді і спробували ввести у воду гідроксид натрію в кількості, яка може загрожувати життю людей.

Ризик для об'єктів критичної інфраструктури можна визначити як порушення у їх функціонуванні, яке становить загрозу для населення, власності, навколишнього середовища, життєво важливих ресурсів, репутації, інформаційної безпеки, територіальної цілісності та соціальних відносин.

У контексті управління ризиками для об’єктів критичної інфраструктури, можна виділити наступні групи механізмів:

1) Правові механізми – розробка законодавчої бази для визначення концепцій, правового регулювання виявлення загроз та управління забезпеченням безпеки об’єктів критичної інфраструктури.

2) Організаційні механізми – встановлення організацій, відповідальних за забезпечення безпеки об’єктів критичної інфраструктури, координація їх діяльності та співпраця з іншими установами, підприємствами та особами.

3) Техніко-технологічні та програмні механізми – розробка системи технічних, технологічних і програмних засобів, що забезпечують запобігання або зменшення негативного впливу загроз та ризиків для об’єктів критичної інфраструктури.

4) Фінансові механізми – визначення фінансових ресурсів для запобігання ризикам і створення резервного фонду на випадок виникнення ризикових ситуацій, пов’язаних з об’єктами критичної інфраструктури.

5) Наукові механізми – наукове обґрунтування принципів, методів, форм, інструментів і заходів для запобігання та захисту об’єктів критичної інфраструктури.

6) Військово-оборонні та розвідувально-агентурні механізми – застосування спеціальних засобів для протидії ворожим і зловмисним діям, спрямованим проти об’єктів критичної інфраструктури.

7) Інформаційні механізми – розробка та розповсюдження інформаційних повідомлень про форми, прояви та наслідки посилення ризиків та загроз для об'єктів критичної інфраструктури.

8) Освітні механізми – навчання та підготовка фахівців у сфері управління ризиками для об'єктів критичної інфраструктури.

9) Дипломатичні механізми – встановлення дипломатичних рамок втручання у соціально та суспільно значущі системи та активи, врегулювання конфліктів, які можуть посилювати загрози для об'єктів критичної інфраструктури.

Існують різноманітні методи визначення ризиків. Однак, загальноприйнятий підхід до оцінювання ризиків для критичної інфраструктури включає наступні кроки:

- виявлення та розподіл загроз за категоріями, а також оцінка ймовірності (або більш точно, частоти) кожної окремої загрози;

- аналіз вразливостей до різних типів подій або атак (це, разом із оцінкою частоти загроз, визначає ризик нанесення шкоди);

- оцінка потенційних наслідків (заснована на найгіршому можливому сценарії розвитку подій).

Варто відзначити, що хоча цей ризик-орієнтований підхід використовується у сфері управління техногенно-екологічною безпекою, іноді неможливо кількісно оцінити та адекватно порівняти ризики, пов'язані з критичною інфраструктурою. Це може бути зумовлено невизначеністю, включно з неточністю та неповнотою інформації, необхідної для точного визначення частоти загроз (особливо це відчутно в контексті оцінки терористичних загроз), а також складністю та відмінностями потенційних наслідків. Дослідження стандартів та нормативних документів щодо забезпечення безпеки критичної інфраструктури.

Відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287/2015, загрозами безпеці критичної інфраструктури (КІ) визначено [5]:

- критична зношеність основних фондів об’єктів інфраструктури України та недостатній рівень їх фізичного захисту;
- недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій;
- неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

Загрози, з якими стикається критична інфраструктура, зазвичай поділяють на три основні категорії: аварії та технічні несправності, природні катастрофи та небезпечні природні явища, а також ворожі дії, здійснювані групами або індивідуумами, такими як терористи, злочинці, диверсанти, агенти промислового шпигунства, та військові дії. Особливо серйозні загрози становлять комбіновані загрози або такі, які можуть призвести до катастрофічних та різноманітних каскадних наслідків через взаємозалежність компонентів критичної інфраструктури.

При аналізі аварій та технічних збоїв, слід зазначити, що в Україні існує висока ймовірність аварій на об'єктах з підвищеним ризиком, енергетичних об'єктах

та системах життєвого забезпечення через значний ступінь зношення основних активів. Згідно з даними Державного комітету статистики, зношеність основних активів промислових підприємств у середньому складає 60,3%. Високий ризик техногенних аварій також пов'язаний з присутністю на українській території багатьох об'єктів з підвищеною небезпекою, які використовують у своїй діяльності значну кількість небезпечних речовин. Відповідно до інформації від Державної служби надзвичайних ситуацій, аварії на 955 таких об'єктах можуть спричинити надзвичайну ситуацію.

У секторі житлово-комунального господарства проблема старіння інфраструктури залишається невирішеною. Наприклад, в Україні близько 34% водопровідних мереж та понад 18% теплових та парових мереж є застарілими або аварійними відносно загальної довжини цих мереж. Це призводить до значних втрат води та теплової енергії під час їх транспортування до споживачів, підвищення тарифів, що, в свою чергу, спричиняє соціальну напруженість, надзвичайні ситуації державного або регіонального масштабу.

У категорії загроз, пов'язаних з природними катастрофами та небезпечними природними явищами, особливо слід звернути увагу на наступні: екстремальні погодні умови, включаючи сильні снігопади, ожеледицю, буревії, зливи, град, заморозки, періоди посухи та спеки, а також урагани та торнадо; гідрологічні явища, такі як повені, зсуви ґрунту, підтоплення та цунамі; геологічні процеси, включаючи зсуви, просідання ґрунту та карстові процеси, а також епідемії та пандемії. Серед цих загроз, метеорологічні явища, частота яких в Україні значно зросла в останні десятиліття, заслуговують особливої уваги, особливо такі як обледеніння, підтоплення та посухи. Паводки вважаються однією з найбільш руйнівних гідрологічних загроз для критичної інфраструктури.

1.3 Дослідження стандартів та нормативних документів щодо забезпечення безпеки критичної інфраструктури

Безпека критичної інфраструктури є вирішальним аспектом національної безпеки, економічного добробуту та соціальної стабільності будь-якої держави. У цьому розділі зосередимося на дослідженні стандартів і нормативних документів, які формують основу для ефективного управління безпекою критичної інфраструктури. З урахуванням різноманітності загроз, що постійно еволюціонують, важливо забезпечити, щоб політики та процедури безпеки були відповідно оновлені та відповідали сучасним викликам.

У цьому контексті, будемо аналізувати національні та міжнародні регулятивні рамки, стандарти безпеки, нормативно-правові акти та керівні принципи, які регулюють захист критичної інфраструктури. Вивчення цих документів дозволить оцінити, як вони сприяють створенню міцного, гнучкого та адаптивного підходу до управління ризиками та загрозами, з якими стикаються різні сектори критичної інфраструктури.

Також розглянемо, як ці стандарти та регуляції впливають на планування, впровадження та перегляд заходів безпеки, а також як вони взаємодіють із засадами корпоративного управління, технологічними інноваціями та міжсекторальною координацією. Це дозволить глибше зрозуміти, як краще адаптувати стандарти та практики до змінюваних умов та нових викликів у сфері безпеки критичної інфраструктури.

1.3.1 Міжнародні та національні стандарти та практики кібербезпеки

Міжнародні стандарти та практики кібербезпеки відіграють ключову роль у забезпеченні безпеки критичної інфраструктури в умовах, коли кіберпростір стає все більш складним та вразливим до атак. Ці стандарти та практики розроблені для того, щоби надавати організаціям керівні вказівки щодо захисту їхніх мереж та систем від різноманітних кіберзагроз.

Одним з ключових аспектів міжнародних стандартів є їх універсальність та адаптивність до різних секторів індустрії та бізнесу. Вони включають рекомендації

щодо управління ризиками, ідентифікації вразливостей, захисту інформаційних активів, реагування на інциденти та відновлення після атак.

Міжнародна організація зі стандартизації (ISO) – це всесвітня організація, членами якої є національні товариства, які встановлюють і контролюють стандарти для комерції, торгівлі та зв'язку в більш, ніж у 150 країнах світу. ISO розробила тисячі міжнародно визнаних добровільних міжнародних стандартів.

ISO/IEC 27001 був розроблений для захисту інформаційних активів організацій [8]. Те, наскільки інформаційні активи є "життєдайною силою" бізнесу, можна виміряти різними способами. Один з показників критичності ІС для бізнесу відображений в емпіричних даних про те, що 50% компаній, які втрачають критично важливі для бізнесу системи більш, ніж на 10 днів, ніколи не відновлюються і припиняють свою діяльність [10]. Впровадження СУІБ допомагає компанії розробити контрзаходи проти вразливостей, пов'язаних з ІС. Інший показник відображається у відсоток ВВП у постіндустріальних суспільствах послуг, що генерується інформаційно-інтенсивними галузями послуг. Ще одним індикатором є вага інформаційних активів та роль патентів і прав інтелектуальної власності (ПІВ) у сучасному глобальному бізнес-середовищі. Оскільки все більше інформації створюється, обробляється та зберігається в цифровому форматі, а більший відсоток доходів компаній генерується інформаційно-критичними процесами, тим ціннішим активом стає стандарт ISO/IEC. ISO/IEC 27001 можна розглядати як комплексну програму, що поєднує управління ризиками, безпеку управління ризиками, безпеку, управління та відповідність вимогам. Він допомагає фірмі забезпечити наявність потрібних людей, процесів і технологій, а також сприяє проактивному підходу до управління безпекою та ризиками [7].

Враховуючи центральне значення ІС/ІКТ для бізнесу, публікація стандарту ISO/IEC 27001 була зустрінута як велика подія у світі інформаційної безпеки [8]. Стандарт ISO/IEC 27001 СУІБ є переглянутою версією надзвичайно успішного

британського стандарту BS 7799-2, перша версія якого з'явилася ще у 1998. Ще до публікації ISO/IEC 27001, відгуки, що надходили з усього світу, свідчили про те, що бізнес з нетерпінням чекав на появу стандарту – показник очікуваного зростання сертифікації бізнесу після успіху ISO 9001 та ISO 14001 [9].

Серед основних міжнародних методичних документів, що визначають підходи до кіберзахисту автоматизованих систем управління технологічними процесами, виділяються стандарт NIST SP 800-82, розроблений американським Національним інститутом стандартизації (NIST), та серія стандартів ISA/IEC 62443 (колишній ISA 99), що була випущена Міжнародною електротехнічною комісією (IEC) у 2018 році [11].

Ціллю серії стандартів ISA/IEC 62443 (рис. 1.1) є створення уніфікованої системи термінології для опису процесів введення та підтримки функціонування систем управління технологічними процесами, а також встановлення норм та вимог для забезпечення кібербезпеки та захисту цих систем від кібератак. Серія стандартів ISA/IEC 62443 представляє собою міжсекторальну ініціативу, що застосовується у всіх ключових галузях промисловості критичної інфраструктури. Розроблені на основі знань і досвіду міжнародних експертів у галузі кібербезпеки, вони пропонують всеосяжний підхід до кіберзахисту та представляють його як безперервний процес [12].

Загальні	Політика та процедури	Система	Компоненти
ISA-62443-1-1 Концепції та моделі	ISA-62443-2-1 Вимоги до програми безпеки для власників активів IACS	ISA-TR62443-3-1 Технологія безпеки IACS	ISA-62443-4-1 Вимоги безпеки до життєвого циклу розробки продукту
ISA-TR62443-1-2 Словник термінів та скорочень	ISA-62443-2-2 Рівні захисту IACS	ISA-62443-3-2 Оцінка ризиків безпеки та проектування системи	ISA-62443-4-2 Технічні вимоги безпеки для компонентів IACS
ISA-62443-1-3 Показники відповідності безпеки системи	ISA-TR62443-2-3 Управління версіями в середовищі IACS	ISA-62443-3-3 Вимоги до системної безпеки та рівні безпеки	
ISA-TR62443-1-4 Життєвий цикл безпеки IACS та випадки використання	ISA-62443-2-4 Вимоги до програми безпеки постачальника послуг IACS		
	ISA-TR62443-2-5 Керівництво з впровадження для власників активів IACS		

Рисунок 1.1 – Серія стандартів ISA/IEC 62443

Стандарти та технічні звіти ISA/IEC 62443 поділяються на чотири категорії: загальні положення, політика та процедури, системні та компонентні аспекти. Серед основних стандартів серії IEC 62443 варто відзначити наступні чотири:

1) ISA/IEC 62443-2-4 – присвячений політиці та практиці інтеграції систем;
2) ISA/IEC 62443-3-3 – що стосується вимог та рівнів безпеки;
3) ISA/IEC 62443-4-1 – визначає вимоги безпечного життєвого циклу розвитку;
4) ISA/IEC 62443-4-2 – описує технічні характеристики безпеки компонентів автоматизованих систем.

Важливо зазначити, що Україна, будучи членом та партнером Міжнародної електротехнічної комісії (IEC), переклала та впровадила лише один стандарт з цієї серії – ДСТУ EN IEC 62443-4-1:2019 [13], який встановлює вимоги до безпечного життєвого циклу розроблення продукції, затвердженого наказом ДП «УкрНДНЦ» № 249 від 13.08.2019 року [14].

Національні стандарти та практики кібербезпеки в Україні складаються з комплексу законодавчих і нормативних актів, спрямованих на захист інформаційних систем, критичної інфраструктури та персональних даних громадян від кіберзагроз. Україна, стикаючись із зростанням кіберзагроз, активно розвиває та адаптує свої національні стандарти та практики, щоб відповідати міжнародним вимогам та забезпечити надійний захист.

У рамках національних стандартів, Україна також працює над впровадженням міжнародних стандартів, таких як ISO/IEC 27001, що стосується управління інформаційною безпекою. Також важливим є ДСТУ ISO/IEC 27002 [16, 17], який надає рекомендації щодо управління інформаційною безпекою.

Національна стратегія кібербезпеки та план її реалізації передбачають розробку та впровадження політик безпеки, проведення регулярних аудитів, тренінгів та інших заходів для підвищення рівня освіти та обізнаності у сфері кібербезпеки.

Україна також активно співпрацює з міжнародними організаціями та партнерами у сфері кібербезпеки для обміну інформацією про загрози, розробку спільних ініціатив та участь у міжнародних програмах підвищення кібербезпеки.

Все це вказує на те, що Україна серйозно ставиться до питань кібербезпеки та приділяє значну увагу розвитку відповідних національних стандартів і практик.

Важливість цих стандартів та практик полягає також у їхній здатності сприяти глобальній уніфікації підходів до кібербезпеки, що є важливим для міжнародних організацій та компаній, які працюють у різних юрисдикціях. Вони також сприяють обміну кращими практиками та вдосконаленню знань про загрози і вразливості у кіберпросторі.

1.3.2 Правове регулювання кібербезпеки в Україні та світі

Правове регулювання кібербезпеки на глобальному рівні є різноманітним і включає широкий спектр законодавчих і нормативних актів, прийнятих на національному та міжнародному рівнях. Ці заходи спрямовані на захист інформаційних систем, мереж та даних від кіберзагроз, а також на встановлення відповідальності за кіберзлочини.

Більшість країн розробили власне законодавство, яке регулює питання кібербезпеки. Це може включати закони, що стосуються кіберзлочинності, захисту даних, кібертероризму, захисту критичної інфраструктури тощо.

На міжнародному рівні існують угоди, такі як Конвенція про кіберзлочинність (відома як Будапештська конвенція), яка є першою міжнародною угодою, спрямованою на боротьбу з кіберзлочинністю, встановлюючи єдині стандарти, які дозволяють країнам-членам криміналізувати різні види кіберзлочинів.

Різні регіони, такі як Європейський Союз, Азіатсько-Тихоокеанський регіон, Африка тощо, розробили свої власні рамки та стандарти кібербезпеки. Наприклад, у Європі діє Загальний регламент про захист даних (GDPR) [24], який встановлює стандарти захисту персональних даних.

Міжнародні стандарти, такі як ISO/IEC 27001, встановлюють вимоги до систем управління інформаційною безпекою, які широко використовуються у всьому світі.

Ефективне правове регулювання кібербезпеки вимагає співпраці між урядовими органами, приватним сектором та громадянським суспільством для обміну інформацією про загрози, координації дій та розробки спільних стратегій.

Правове регулювання кібербезпеки в світі постійно розвивається, реагуючи на нові виклики та загрози в цифровому просторі. Воно охоплює широкий спектр питань від кіберзлочинності до захисту інфраструктури та даних, і залежить від співпраці та взаємодії між різними країнами та регіонами.

Правове регулювання кібербезпеки в Україні охоплює ряд законодавчих і нормативних актів, спрямованих на захист інформаційних систем, державної та приватної інформації, а також критичної інфраструктури від кіберзагроз.

Основним законом, що регулює цю сферу, є Закон України "Про основні засади забезпечення кібербезпеки України" [15]. Цей закон встановлює правові основи для захисту національного кіберпростору, організації державного управління у сфері кібербезпеки, а також розподіл відповідальності між різними державними органами.

Крім того, в Україні діють інші законодавчі акти, які безпосередньо або опосердковано стосуються питань кібербезпеки. Серед них:

- Закон України "Про інформацію" [18];

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [19];

- Закон України "Про захист персональних даних" [20];

- Закон України "Про телекомунікації" [21];

- Закон України "Про основні засади забезпечення кібербезпеки України" [31].

Також важливим є впровадження стандартів ISO/IEC у сфері інформаційної безпеки, таких як ISO/IEC 27001, що регулює системи управління інформаційною безпекою

Для координації дій у сфері кібербезпеки і відповіді на кіберінциденти в Україні створено Державну службу спеціального зв'язку та захисту інформації [22], яка відповідає за реалізацію державної політики у цій області.

Крім того, Україна активно співпрацює з міжнародними партнерами і організаціями для забезпечення кібербезпеки, в тому числі через участь у міжнародних програмах та ініціативах.

Таким чином, правове регулювання кібербезпеки в Україні є комплексним і постійно розвивається для адаптації до нових викликів та загроз у цифровому світі.

1.4 Висновки до розділу 1

На основі аналізу концепції критичної інфраструктури та її ключових компонентів, можна зробити висновок, що забезпечення кібербезпеки критичної інфраструктури є надзвичайно важливим завданням для забезпечення національної безпеки та стабільності. Розглянуті існуючі системи критичної інфраструктури та їх вразливість перед кіберзагрозами, а також ризики та загрози, з якими стикається критична інфраструктура, вказують на необхідність вдосконалення методів та заходів кібербезпеки. Дослідження стандартів та нормативних документів щодо забезпечення безпеки критичної інфраструктури дозволяє розробити оптимальні рекомендації щодо застосування методів кібербезпеки до критичної інфраструктури. Також важливим аспектом забезпечення кібербезпеки критичної інфраструктури є виявлення та аналіз загроз, що можуть виникнути в результаті кібератак або інших видів втручань. Для цього необхідно розробити ефективні методи та засоби моніторингу та виявлення вразливостей критичної інфраструктури. Крім того, важливим завданням є розробка заходів захисту та відновлення після інцидентів, що дозволить забезпечити найвищий рівень

кібербезпеки критичної інфраструктури. У цілому, даний розділ надає важливу інформацію для розуміння проблем та викликів, що стоять перед забезпеченням кібербезпеки критичної інфраструктури, та вказує на необхідність подальших досліджень та розробок у цій галузі.

2 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У даному розділі дослідження здійснюється глибокий аналіз сучасних методів та заходів, що спрямовані на забезпечення кібербезпеки критичної інфраструктури. У сучасному світі, де залежність від інформаційних технологій стрімко зростає, питання кібербезпеки набуває особливої актуальності. Це особливо важливо для критичної інфраструктури, такої як енергетика, транспорт, банківська система та охорона здоров'я, яка відіграє життєво важливу роль у функціонуванні держави та її економіки.

У рамках цього розділу будуть розглянуті передові технології та методики, що використовуються для захисту критичних інфраструктур від кіберзагроз. Будуть детально проаналізовані сучасні системи виявлення інцидентів, методи шифрування та автентифікації, а також стратегії застосування штучного інтелекту для підвищення кібербезпеки. Значну увагу буде приділено також розгляду практик управління ризиками та реагування на інциденти. Особливий акцент буде зроблено на важливості розробки та впровадження комплексних стратегій кібербезпеки, які включають не лише технічні аспекти, але й організаційні та нормативно-правові моменти.

Також буде розглянуто вплив міжнародних стандартів та регуляцій на розвиток систем кібербезпеки, зокрема, аналізуючи досвід Європейського Союзу та НАТО. Важливим аспектом є інтеграція міжнародних норм у національне законодавство та практику, а також вивчення успішних підходів інших країн. Цей розділ виокремлює основні виклики та перспективи розвитку кібербезпеки

критичної інфраструктури, надаючи погляд на майбутнє цієї важливої та динамічної сфери.

2.1 Огляд сучасних заходів кібербезпеки

Наразі суспільство все частіше стикається з різними типами кібератак. Це включає неполадки у електронних сервісах, перешкоди у роботі державних установ, фішинг через електронну пошту, кіберзлочинність, порушення захисту та приватності даних. Також це стосується інформаційно-психологічного впливу на населення, кібертероризму, кібершпигунства, інформаційного вторгнення в національний інформаційний простір країни. Окрім того, існують загрози блокування чи знищення ключових для економіки та безпеки держави підприємств, систем життєзабезпечення та об’єктів високої небезпеки. Україна вжила комплексних заходів для забезпечення готовності до кібербезпеки та протидії агресії в кіберпросторі. Ці заходи включають вирішення стратегічних, правових, політичних, технічних та організаційних аспектів, щоб гарантувати безпеку в роботі кіберпростору (рис. 2.1) [25].

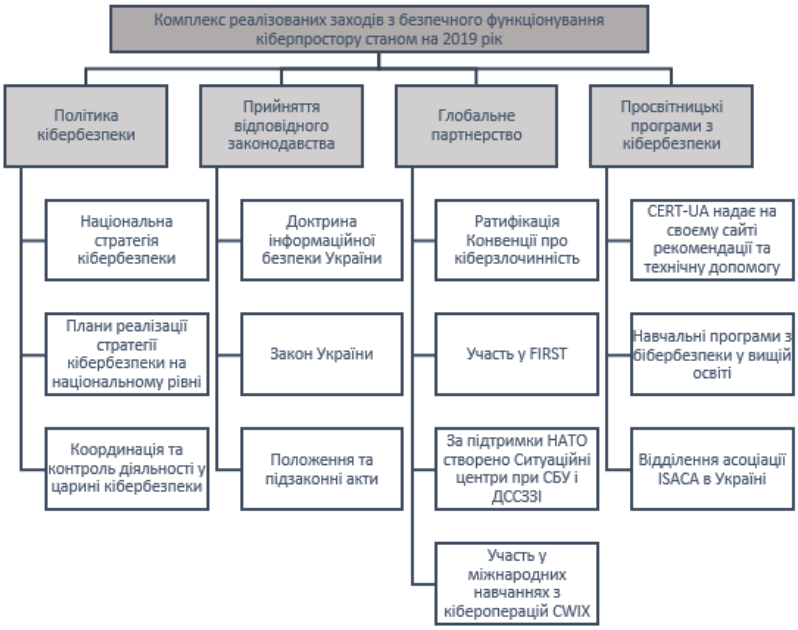

Рисунок 2.1 – Комплекс реалізованих заходів з безпечного функціонування кіберпростору станом на 2019 рік

Після 2014 року в Україні відбулись значні зміни в законодавстві, пов'язаному з кібербезпекою. До 2019 року була створена законодавча основа у цій сфері, включаючи прийняття Доктрини інформаційної безпеки України (з 25.02.2017 р.), а також ряд законів, таких як «Про основні засади забезпечення кібербезпеки України» 2163-VIII (з 09.05.2018 р.), «Про національну безпеку України» 2469-VIII (з 08.07.2018 р.), «Про інформацію» 2657-XII (оновлена версія від 01.01.2017 р.), та інші. Також було внесено зміни до президентських указів, зокрема до «Концепції розвитку сектора безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.), «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.) і «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.).

Для зміцнення міжнародних відносин та уніфікації регуляторних документів в області кібербезпеки, з урахуванням міжнародних та стандартів ЄС і НАТО, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші глобальні угоди.

Для оперативного ухвалення управлінських рішень під час виникнення кризових ситуацій та з метою визначення потенційних або реальних загроз національній безпеці України необхідно створювати відповідні ситуаційні центри. Ухвалена постанова «Питання мережі ситуаційних центрів» визначає склад, завдання та їх функції, вимоги до програмного й апаратного забезпечення ситуаційного центру, його підсистем та мереж. А також дозволить створити правові передумови для подальшого розширення й розвитку мережі ситуаційних центрів.

Ситуаційні центри – інструменти ухвалення оперативних управлінських рішень. Вони надають інформацію та аналітику про діяльність органів державної влади у сферах нацбезпеки і оборони. А також є першоджерелом оперативної інформації щодо важливих національних подій [26].

Ситуаційні центри забезпечують швидке реагування на кризові події у країні, дозволяючи державним органам ефективно виконувати свої обов'язки. Правове

регулювання гарантує стабільну роботу цих центрів у мирний час, а також під час особливих умов, включаючи воєнний або надзвичайний стан та інші кризи, які становлять загрозу національній безпеці України.

Україна активно приймає участь у навчаннях з кібероперацій. У м. Бидгощ проходило щорічне навчання НАТО CWIX – Coalition Warrior Interoperability Exercise. Україна бере участь у CWIX як повноправний учасник та тестує свої спроможності на взаємосумісність з державами-членами НАТО з 2018 року. У цьому році Україну під час навчання представляли Центр інновацій Міноборони та представники Збройних Сил України. Команда Центру інновацій змогла перевірити на взаємосумісність 4 протоколи обміну та частково виконати цілі 12 фокус-груп з 19 наявних на навчанні. Також під час навчань команда Центру інновацій успішно відпрацювала спільні тести на досягнення взаємосумісності із 12 системами з 10 країн та 3 системами, розробленими безпосередньо НАТО, в тому числі в різних комбінаціях передачі між ними даних. Загалом цього року у навчання взяли участь 2200 учасників із 43 країн, було протестовано 406 унікальних спроможностей та проведено 22 тисячі тестів [27, ст. 32].

У рамках взаємодії з міжнародними організаціями з питань реагування на кіберінциденти було організовано участь України у Форумі команд реагування на інциденти інформаційної безпеки FIRST (Forum for Incident Response and Security Teams), що об'єднує різні групи CERT (Computer Emergency Response Team – Команда реагування на надзвичайні ситуації) у країнах Європи [25].

Для координації та нагляду за діяльністю різних учасників у сфері кібербезпеки, уряд України організував роботу відповідних державних органів з певними обов'язками у цій галузі:

- Створено механізм управління та ведення діяльності Національного координаційного центру кібербезпеки під егідою Ради національної безпеки і оборони України. Цей центр забезпечує координацію міжвідомчої взаємодії у разі

кібератак і кіберінцидентів, зокрема в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, для підвищення ефективності у формуванні та реалізації державної політики в області кібербезпеки в рамках Стратегії кібербезпеки України.

- Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) відповідає за державний контроль у боротьбі з кіберзлочинністю, захист об'єктів критичної інформаційної інфраструктури, а також за формування та реалізацію політики в сфері кібербезпеки, зокрема щодо захисту державних інформаційних ресурсів.

- Враховуючи важливість захисту персональних даних громадян, також створено незалежний державний наглядовий орган, як цього вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованим обробленням персональних даних.

- В Україні було організовано діяльність Департаменту кіберполіції Національної поліції, відповідального за запобігання, виявлення, припинення та розслідування кримінальних злочинів, що включають використання електронних обчислювальних систем (комп'ютерів), телекомунікаційних мереж та систем [29].

- Було засновано авторитетний орган у сфері інформаційної безпеки – Державне агентство з електронного врядування України, наділене повноваженнями наглядати за дотриманням операторами основних послуг вимог кібербезпеки [28].

Також необхідно зосередитися на підвищенні обізнаності про кібербезпеку на різних рівнях, від центрів комп'ютерної безпеки до запровадження освітніх програм у цій галузі. Особливу увагу слід приділити розробці та впровадженню навчальних програм з комп'ютерної безпеки не тільки у вищій освіті, але й у початкових та середніх школах.

В умовах сучасних викликів у кіберпросторі, організації мають переглянути своє ставлення до кібербезпеки. Це вимагає підвищення обізнаності про значення

інвестицій у кібербезпеку як ключового елементу будь-якої національної ІКТ-стратегії.

Компаніям важливо стимулювати навчання своїх працівників у сфері кібербезпеки, розвивати власні кіберталанти, сприяти громадському діалогу про необхідність раннього навчання кібернавичкам, враховуючи, що дефіцит кваліфікованих кадрів у цій сфері продовжує зростати.

2.2. Огляд методів аналізу та оцінки кібербезпеки

Аналіз та оцінка кібербезпеки – це критичні процеси, що дозволяють організаціям ідентифікувати, оцінювати та управляти ризиками, пов'язаними з кіберпростором. Аналіз ризиків займає значний час та є складним процесом, процедура якого визначена трьома етапами (рис. 2.2).

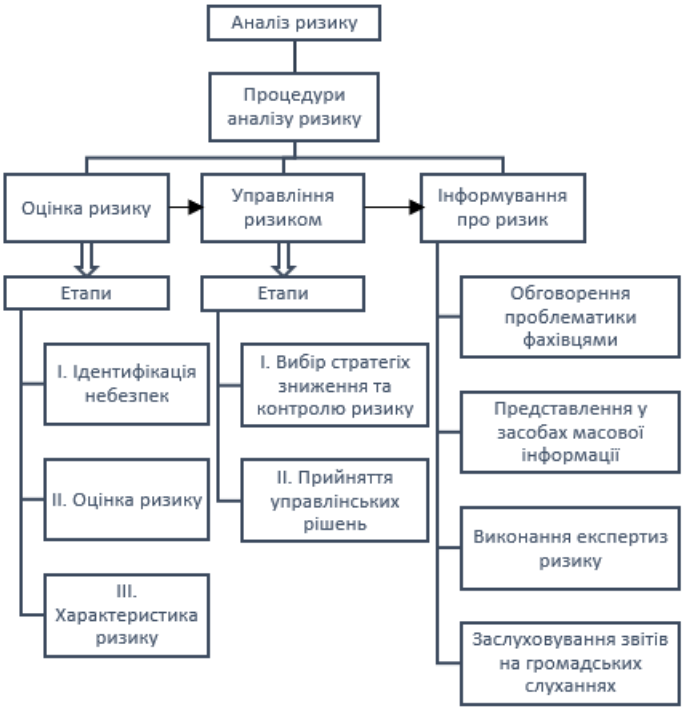

Рисунок 2.2 – Структура аналізу ризику

Кількісний аналіз ризику повинен дати можливість визначити число та розміри окремих ризиків та ризику проекту в цілому. Кількісний аналіз ризиків (Quantitative-RA) застосовується для визначення числових показників ймовірності кожного ризику та його фінансових наслідків. Цей метод може використовуватися

для прогнозування результатів, обчислюючи сумарний вплив ризиків на підставі графіка проекту та його оцінок, надаючи керівникам проектів інформацію про можливість досягнення цілей та потенційні неочікувані обставини.

Кількісний аналіз ризиків, як об'єктивний метод, забезпечує точну оцінку ризиків на основі вимірюваних даних, враховуючи різноманітні ймовірності ризиків та різні можливі наслідки цих ризиків. Однак цей аналіз вимагає значних даних і може бути складним у реалізації, і його точність залежить від наявності усіх ризиків і можливостей у розрахунках.

Кількісний аналіз ризиків не завжди практичний для всіх організацій і частіше використовується в масштабних, глобальних або мегапроектах. Він рідше застосовується у менших або IT/програмних проектах через їх складність і може зустріти опір з боку керівництва організацій.

Моделювання загроз: Методи моделювання, такі як дерева атак та дерева вразливостей, допомагають в ідентифікації потенційних шляхів атаки та вразливостей у системах безпеки.

Стандарти та рамки оцінки: Міжнародні та національні стандарти, такі як група стандартів ISO/IEC 2700 та NIST Cybersecurity Framework, надають організаціям рекомендації щодо встановлення ефективних процесів кібербезпеки.

Використання аудитів та оглядів безпеки: Проведення регулярних аудитів та оцінок безпеки допомагає організаціям виявити слабкі місця та забезпечує дотримання стандартів та політик безпеки.

Інцидентне реагування та аналіз після інциденту: Аналіз інцидентів кібербезпеки, що вже сталися, дає цінну інформацію для вдосконалення стратегій та процедур безпеки.

Використання штучного інтелекту та машинного навчання: Сучасні технології ШІ та машинного навчання здатні аналізувати великі обсяги даних для виявлення потенційних загроз та аномалій у поведінці систем.

2.2.1 Засоби та технології захисту інформації. (Ідентифікація та управління доступом)

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

За концепцією захисту інформації визначають різноманітні джерела загроз інформації, що відрізняються своєю мотивацію. Перелік даних джерел представлено у табл. 2.1.

Таблиця 2.1 – Джерела загроз для інформації.

Джерела	Мотивація
Інші джерела	Одержання переваг у зовнішньополітичній, зовнішньоекономічній, військовій та інших сферах
Політичні партії	Одержання переваг у політичній боротьбі, боротьбі за владу
Злочинні угрупування	Одержання політичних, економічних переваг, нанесення шкоди
Суб’єкти підприємницької діяльності	Одержання переваг у конкурентній боротьбі, економічні переваги
Окремі фізичні особи	Самоствердження, отримання економічних переваг і винагород
Навмисні та ненавмисні дії персоналу	Помилки персоналу, низька кваліфікація працівників, образа, зрада, примушення
Стихійні лиха та техногенні катастрофи	Відсутність мотивації

У галузі захисту інформації вважається, що, якщо захисна система створена з врахуванням усіх новітніх технік та інструментів, а також має добре підготовлений персонал, який не робить помилок, то умисні порушення в такій системі є неможливими. Проте це не зовсім так. З часом захисні системи застарівають, персонал може втратити пильність, а зловмисники знаходять нові методи атак, які

не були відомі при створенні системи. Тому, незважаючи на впевненість у надійності системи захисту інформації, важливо пам’ятати основний принцип: жодна система не може назавжди вистояти проти наполегливих атак кваліфікованих порушників із сучасними технологіями. Це правило, засноване на багаторічному досвіді фахівців, є універсальним і не залежить від рівня системи, відданості користувачів чи якості обладнання та програмного забезпечення. Воно підкреслює, що питання не в тому, чи зловмисники зламають систему, а коли це станеться. Головне завдання захисту інформації – затримати момент злому якнайдовше.

Види інформаційних загроз поділяють на дві основні групи:

1) відмови та порушення працездатності програмних і технічних засобів;
2) навмисні загрози, заздалегідь плановані зловмисниками для нанесення шкоди.

Основним джерелом загроз, які ставлять під ризик цілісність та конфіденційність інформації, є умисні дії, що зловмисники планують заздалегідь для завдання шкоди. Ці загрози поділяються на дві основні категорії:

- Загрози, виконання яких вимагає безперервної участі людини;
- Загрози, які після розробки відповідних комп'ютерних програм зловмисником, втілюються самими цими програмами автономно, без прямої участі людини.

Міри захисту від загроз кожного типу включають:

- Запобігання неавторизованому доступу до ресурсів обчислювальних систем;
- Унеможливлення несанкціонованого використання комп'ютерних ресурсів при отриманні доступу до них;
- Своєчасне виявлення та усунення несанкціонованих дій, а також їх причин та наслідків.

Головним методом запобігання неавторизованому доступу до ресурсів обчислювальних систем є верифікація користувачів та визначення їх прав доступу до інформаційних ресурсів. Цей процес охоплює такі кроки:

- Ідентифікація;
- Підтвердження справжності (автентифікація);
- Встановлення дозволів для подальшого нагляду та обмеження доступу до комп'ютерних ресурсів.

Ідентифікація важлива для надання комп'ютерній системі унікального ідентифікатора користувача, який звертається до неї. Цей ідентифікатор може бути будь-якою комбінацією символів і повинен бути зареєстрований в системі адміністрування безпеки заздалегідь. Під час реєстрації фіксується наступна інформація:

- Прізвище, ім'я та по батькові користувача (та інші потрібні характеристики);
- Унікальний ідентифікатор користувача;
- Назва процедури підтвердження справжності;
- Еталонні дані для верифікації справжності (наприклад, пароль);
- Обмеження на використання еталонних даних (наприклад, термін дії пароля);
- Права доступу користувача до комп'ютерних ресурсів.

Перевірка автентичності (автентифікація) здійснюється шляхом підтвердження достовірності прав користувача.

На рис. 2.3 представлена схема ідентифікації користувача.

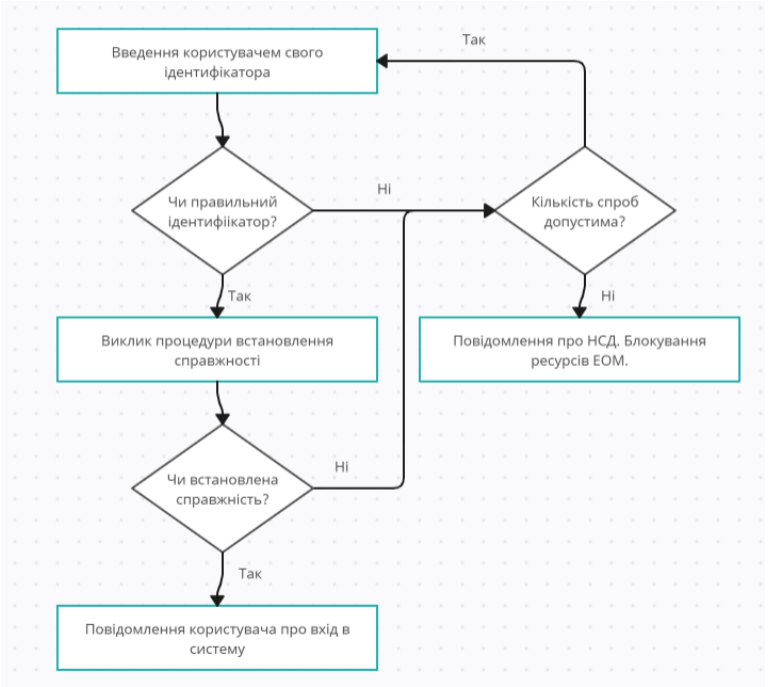

Рисунок 2.3 – Схема ідентифікації користувача

Проте, такі підходи потребують значних витрат, через що їх застосування не є поширеним. Поширеними є методи автентифікації на основі паролів. Існують два види паролів: статичні та динамічні.

Статичний пароль залишається незмінним протягом усього періоду його використання.

Для динамічних паролів використовується метод, який визначає правила їх зміни. Способи адаптації статичних паролів включають, наприклад, вибір випадкових символів пароля для одноразового використання. Метод "питання-відповідь", що ґрунтується на наданні користувачеві випадково вибраних запитань з існуючого набору. Функційні методи, які використовують деяку функцію F з параметрами, що постійно змінюються (такими як дата, час, день тижня тощо), для генерації пароля.

Після того, як користувач пройде процеси ідентифікації та автентифікації, система безпеки має визначити його права для подальшого управління

авторизованим доступом до комп'ютерних ресурсів (обмеження доступу). До комп'ютерних ресурсів належать:

- Програми;
- Зовнішня пам'ять (файли, директорії, логічні диски);
- Категоризована інформація в базах даних;
- Оперативна пам'ять;
- Час (пріоритет) використання процесора;
- Порти введення/виведення;
- Зовнішні пристрої.

Існують такі типи прав доступу користувачів до ресурсів:

- Загальний (повне надання ресурсу);
- Функціональний або частковий;
- Тимчасовий.

Поширені методи обмеження доступу включають:

- Розмежування за списками (користувачів чи ресурсів);
- Використання матриці встановлення прав (рядки матриці – ідентифікатори користувачів, стовпці – ресурси комп'ютерної системи);
- Обмеження за рівнями конфіденційності та категоріями (наприклад, загальний доступ, конфіденційно, таємно);
- Парольне обмеження доступу.

Система управління та контролю доступу (або СКУД/СКД) представляє собою набір програмних та технічних засобів безпеки, які координують доступ та рух людей або транспортних засобів на територіях під наглядом для адміністративного контролю та попередження нелегального доступу.

Система контролю доступу також забезпечує:

- ідентифікацію осіб з правом доступу;
- розділення доступу до різних зон;

- контроль автоматизованих режимів;
- фіксацію часу перебування на об’єкті;
- обработку даних та ведення статистики.

Запровадження СКУД забезпечує безпеку та контроль об’єктів без необхідності залучення значної кількості охоронного персоналу, забезпечуючи стабільну роботу автоматизованих систем цілодобово (наприклад, для банкоматів, розміщених у відокремлених приміщеннях відділень).

2.3 Розробка пропозицій щодо покращення методів забезпечення кібербезпеки.

Стратегія кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [30].

Ухвалення в 2016 році Стратегії кібербезпеки України було значущим етапом у розвитку стратегічного планування в області кібербезпеки, тому сам факт цього рішення можна вважати позитивним досягненням. Протягом останніх років були здійснені зусилля для розбудови та розвитку національної системи кібербезпеки. Ключовим моментом в її структуруванні стало прийняття Закону України "Про основні принципи забезпечення кібербезпеки України", який став основою для формування національної системи кібербезпеки та виконання пов'язаних з цим завдань ключовими учасниками.

У сфері кіберзахисту критичної інформаційної інфраструктури були покращені нормативні акти, затверджені критерії для її визначення та базові вимоги до забезпечення її кіберзахисту.

Засновані центри кібербезпеки та кіберзахисту в таких органах, як Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк України, Міністерство інфраструктури України та Міністерство оборони України (Збройні Сили України).

Розвивається Національна телекомунікаційна мережа, працюють захищені центри обробки даних (дата-центри), створюється Національний центр резервування державних інформаційних ресурсів та започатковано систему виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Для підвищення ефективності координації діяльності учасників забезпечення кібербезпеки був створений робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, чиї рішення сприяють вирішенню складних питань у цій області.

Активно розширюється міжнародне співробітництво, зокрема з ЄС та НАТО, проводяться міжнародні кібернавчання за участю інших країн та міжнародних організацій.

Щорічно проводиться захід, присвячений кібербезпеці. Однак діяльність національної системи кібербезпеки залишається недостатньо узгодженою і зосередженою лише на вирішенні поточних завдань.

Проблеми, що залишаються невирішеними, включають оперативний обмін інформацією про кіберзагрози, розробку ефективної системи підготовки фахівців та створення дієвої моделі державно-приватного партнерства. Також недостатніми вважаються організація та проведення наукових досліджень у сфері кібербезпеки.

2.4 Висновки до розділу 2

Даний розділ присвячений дослідженню передових технологій та методик, що використовуються для захисту критичних інфраструктур від кіберзагроз. Розглянуті сучасні системи виявлення інцидентів, методи шифрування та автентифікації, а також стратегії застосування штучного інтелекту для підвищення

кібербезпеки. Дослідження показало, що на сьогоднішній день існує велика кількість методів та засобів забезпечення кібербезпеки критичної інфраструктури, проте не всі з них є ефективними та відповідають сучасним вимогам.

Особлива увага приділена аналізу практик управління ризиками та реагування на інциденти, що є важливим елементом забезпечення кібербезпеки критичної інфраструктури. Результати дослідження показали, що ефективне управління ризиками та швидке реагування на інциденти можуть значно зменшити наслідки кібератак та інших втручань.

У цілому у розділі було надано важливу інформацію про сучасні методи та засоби забезпечення кібербезпеки критичної інфраструктури, а також про практики управління ризиками та реагування на інциденти. Результати дослідження можуть бути використані для розробки ефективних методів та засобів забезпечення кібербезпеки критичної інфраструктури, що дозволить забезпечити найвищий рівень безпеки критичних систем.

3 ДОСЛІДЖЕННЯ ЗАХОДІВ ПРОТИДІЇ КІБЕРАТАКАМ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

3.1 Типи кібератак та методи їх виявлення

Кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [15].

Однією з відмітних рис кібератак є їх швидке виконання (зазвичай протягом декількох секунд чи хвилин).

Метою кібератаки можуть стати загальні комп'ютерні системи (та їх стабільна робота) або окремі їх елементи: інформаційні ресурси; дані, які передаються через мережі зв'язку; програмне та апаратне забезпечення та інше.

Існують три основні категорії кібератак, класифіковані за їх цілями та впливом на цільові об'єкти:

1) Порушення конфіденційності – мета такої атаки полягає в незаконному доступі до інформації.

2) Порушення цілісності включає несанкціоноване втручання або модифікацію інформації, програмного чи апаратного забезпечення системи.
3) Порушення доступності – метою цього типу атаки є зрив нормальної роботи системи, створюючи перешкоди для законних користувачів у доступі до системи або необхідних для виконання функціональних завдань даних.

Кібератаки можуть бути ініційовані як окремими індивідами, так і організаціями з політичних, кримінальних або особистих мотивів, метою яких є знищення або несанкціонований доступ до конфіденційної інформації.

Ось декілька прикладів різних видів кібератак:

- Віруси та шкідливе програмне забезпечення – це тип кібератак, де шкідливе програмне забезпечення приховане під виглядом надійних вкладень електронної пошти чи програм (наприклад, зашифровані документи або папки з файлами). Вони використовуються для поширення вірусів і дозволяють хакерам отримати доступ до комп'ютерних мереж. Такий вид атаки зазвичай має великий вплив на всю IT-інфраструктуру. До прикладів шкідливого програмного забезпечення належать троянські програми, шпигунське ПЗ, хробаки, комп'ютерні віруси та рекламне ПЗ.

- Розподілена атака на відмову в обслуговуванні (DDoS-атака) – цей вид атаки відбувається, коли група комп'ютерів, контрольованих хакерами, націлюється на веб-сайти або мережеві системи, перевантажуючи їх до такої міри, що вони стають недоступними для звичайних користувачів. Один із прикладів – масове появлення спливаючих рекламних вікон або інші помилки на сайті, які можуть бути використані для запуску розподіленої атаки на відмову в обслуговуванні (DDoS) на цільовому сервері.

- Атаки фішингу – це метод, коли шахраї відправляють фальшиві електронні листи, імітуючи повідомлення від відомих компаній чи інших довірених джерел. Метою фішингу є отримання доступу до особистих або корпоративних даних через обман користувачів.

- SQL-ін’єкції – це техніка незаконного доступу (форма хакерської атаки) до бази даних, яка передбачає виконання шкідливого коду через поля вводу стандартних форм.

У випадку успішного застосування SQL-ін’єкції, несанкціоновані користувачі здатні читати, створювати, оновлювати або навіть видаляти дані в таблицях бази даних. Цей метод часто використовується хакерами, фахівцями з пентестингу та тестувальниками.

- Крос-сайтові скрипти (XSS) – це один з найбільш відомих та небезпечних типів атак, знайомий кожному досвідченому тестувальнику. Вважається однією з найнебезпечніших загроз для веб-додатків, з потенціалом спричинення серйозних проблем.

Атаки XSS часто порівнюють з іншими атаками, які виконуються на стороні користувача, оскільки в основному вони використовують клієнтські мови програмування. Однак, через її здатність наносити шкоду навіть менш чутливим технологіям, атака XSS розглядається як значно більш ризикована.

- Ботнети – це мережа інфікованих шкідливим ПЗ комп'ютерів, яку кіберзлочинці використовують для здійснення незаконних дій, часто без відома власників цих комп'ютерів.

Ботнети часто застосовуються для масової розсилки спаму, встановлення шпигунських програм або крадіжки користувацьких даних. Великомасштабні ботнети можуть бути використані для організації DDoS-атак, направляючи великий обсяг трафіку на певний веб-сайт, що призводить до його сповільнення чи виходу з ладу. Розповсюдження ботнетів здійснюється через шкідливі електронні листи, завантаження файлів або фальшиві програми. Хакери використовують вразливі точки, такі як застаріле ПЗ або відсутність мережевого захисту. Вони також цілять на пристрої, як-от веб-камери, смарт-телевізори та навіть автомобілі.

Для захисту від різноманітних кібератак найчастіше використовують наступні методи виявлення.

Виявлення на основі сигнатур – цей метод дозволяє ідентифікувати конкретні атаки з високим ступенем точності та мінімальною кількістю помилкових спрацьовувань. Втім, він є вразливим до поліморфних вірусів та модифікованих варіантів вже відомих вірусів, а також вимагає постійного та своєчасного оновлення баз даних сигнатур.

Виявлення аномалій. На відміну від сигнатурного методу, виявлення на основі аномалій надає захист від нових, невідомих вірусів і мережевих атак. Однак такі системи можуть викликати велику кількість помилкових тривог, збільшуючи ризик ігнорування справжніх загроз користувачами.

Емуляційне виявлення. В деяких випадках емуляція може ефективно протидіяти таким явищам, як поліморфізм шкідливих програм, аналізуючи дії, а не сам програмний код. Проте значним недоліком є високе навантаження на системні ресурси, що може негативно впливати на продуктивність комп'ютера.

Актуальним є комбінування цих підходів для вдосконалення виявлення шкідливих програм та зниження кількості помилкових спрацьовувань.

3.2 Сценарії реагування на інциденти кібербезпеки

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, національну систему кібербезпеки, повноваження суб’єктів забезпечення кібербезпеки та засади координації [32].

Однією з ключових цілей, визначених законодавством для підтримки національної системи кібербезпеки, є реалізація її організаційно-технічного підходу. Ця організаційно-технічна модель кіберзахисту, створена фахівцями Держспецзв'язку, базується на п'ятирічному досвіді використання законодавства,

розвитку національної кібербезпеки, оцінці сильних та слабких сторін міжнародних моделей, організаційному досвіді та співпраці з іншими учасниками в цій галузі. Визначення моделі включає її структуру, місію, склад, механізми функціонування та цілі. Вона також вперше вводить поняття сил і засобів кіберзахисту, команд швидкого реагування на кіберінциденти та кібергігієни. Модель має багаторівневу архітектуру, що представляє собою структуровану систему з трьох інфраструктур, кожна з яких включає різні сектори, рівні та елементи.

Положенням про організаційно технічну модель кіберзахисту визначено, що її впровадження спрямоване на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості комунікаційних систем. Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки (рис 3.1) [32].

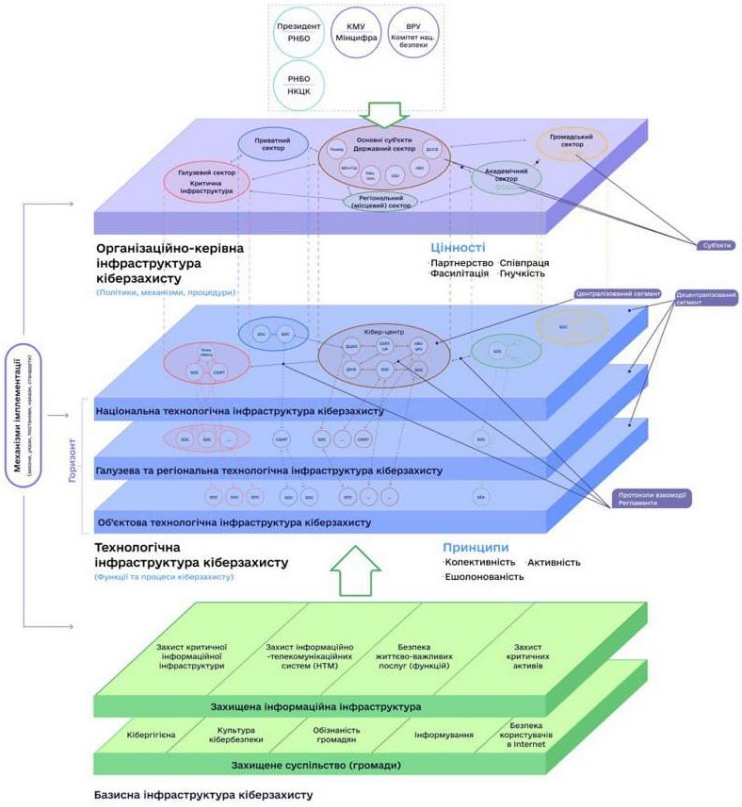

Рисунок 3.1 – Структура ОТМ

У рамках втілення Стратегії кібербезпеки України та на основі урядового рішення, Адміністрація Держспецзв'язку розробила і затвердила методичні рекомендації для реагування на різноманітні події в кіберпросторі. Ці рекомендації, офіційно опубліковані у наказі від 3 липня 2023 року № 570 на сайті служби [22], включають наступні аспекти:

1) Перелік необхідних заходів із кіберзахисту, які мають використовуватися суб'єктами кібербезпеки під час реагування на кіберінциденти або кібератаки. Ці заходи поділяються на різні етапи відповіді.
2) Визначення мети та цілей, яких слід дотримуватися під час виконання цих заходів.
3) Механізм застосування критеріїв для визначення категорії або рівня критичності кіберінциденту чи кібератаки.
4) Принципи, за якими відбувається пріоритезація кіберінцидентів та кібератак.
5) Стандартний перелік заходів для реагування на кіберінциденти та кібератаки, включаючи моніторинг і контроль заходів до їх повного завершення (рис. 3.2).

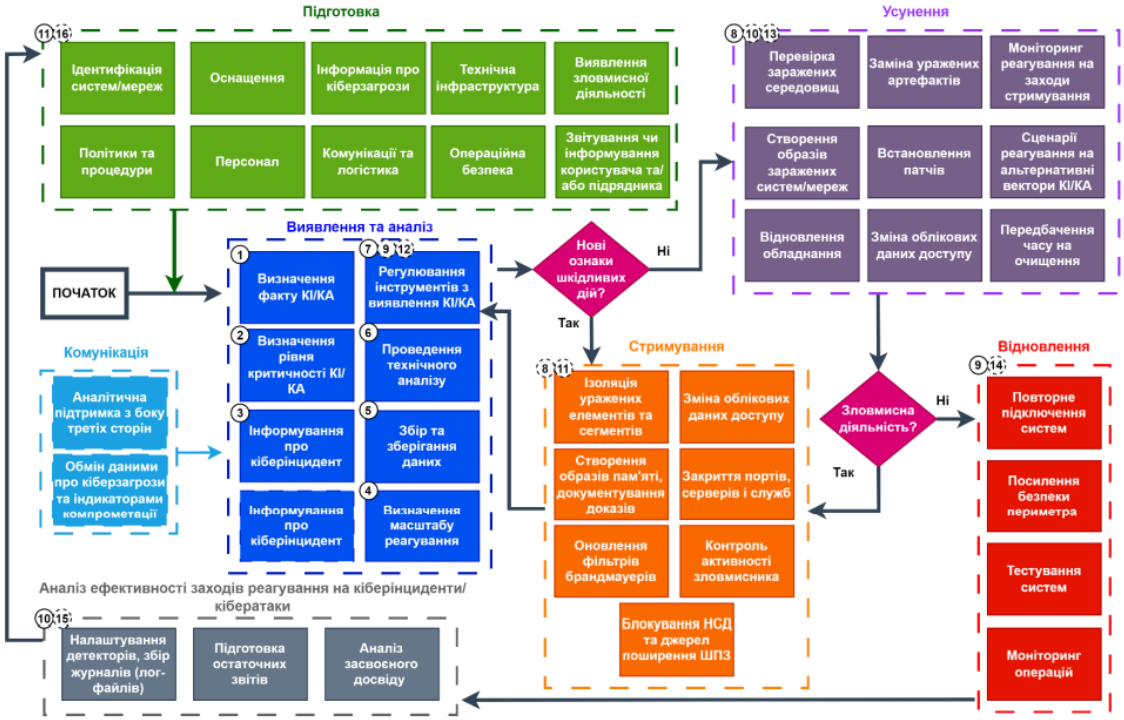

Рисунок 3.2 – Перелік та послідовність заходів реагування на кіберінциденти

Реагування на кіберінциденти або кібератаки розпочинається з етапу підготовки, який передбачає заздалегідні дії, спрямовані на мінімізацію можливого впливу цих інцидентів на суб'єкти кібербезпеки. На цьому етапі основна увага приділяється вивченню та аналізу сучасних видів кіберінцидентів і кібератак, а також розробці методів і механізмів, які можуть запобігати або протидіяти потенційним кіберзагрозам. Це передбачає ретельне планування і розробку стратегій реагування на різні сценарії, що дозволяє ефективно відповідати на кіберінциденти та зменшувати їх наслідки [33].

У процесі реагування на кіберінциденти чи кібератаки, ключову роль відіграє персонал суб'єкта кібербезпеки, який повинен мати підтверджену кваліфікацію та відповідні навички. Для забезпечення високого рівня готовності цих фахівців до реагування на різноманітні кіберзагрози, важливо проводити регулярну перевірку їхніх компетенцій. Це здійснюється через практичні вправи у режимі реального часу, які допомагають підвищувати готовність та вдосконалювати професійні навички.

Особливий акцент робиться на залученні до тренувань тих співробітників, які безпосередньо займатимуться реагуванням на підозрілу поведінку або кіберінциденти в реальних умовах. Це дозволяє зосередити зусилля на розвитку компетенцій та навичок саме тих спеціалістів, котрі це дійсно потребують, оптимізуючи витрати та підвищуючи ефективність цього процесу. Завдяки такому підходу, суб'єкти кібербезпеки можуть не лише підвищувати кваліфікацію своїх співробітників, але й покращувати загальну здатність організації швидко та ефективно реагувати на кіберзагрози.

Найскладнішим аспектом процесу реагування на кіберінциденти або кібератаки є точне виявлення та оцінка потенційних загроз. Це включає визначення чи стався інцидент чи атака, а також уточнення типу і масштабу пошкодження систем або мереж, які були вражені.

Для ефективного виявлення та аналізу таких подій, організації розробляють і впроваджують спеціалізовану політику реагування, обирають відповідні технології, а також засоби для збору інформації, які дозволяють моніторити, виявляти та повідомляти про підозрілу поведінку. Важливо мати чітко затверджені процедури, щоб відрізняти потенційні кіберінциденти від законних дій, таких як звичайні операції адміністратора мережі.

Таким чином, успішне реагування на кіберзагрози вимагає не лише технічних рішень, але й добре продуманих процедур та політик, які дозволяють швидко і точно ідентифікувати та оцінювати кіберінциденти, забезпечуючи належну відповідь на них. Категорії (рівні) критичності кіберінциденту/кібератаки визначаються відповідно до трьох критеріїв критичності кіберінциденту/кібератаки та представленні у табл. 3.1 [33].

Таблиця 3.1 – Категорії та рівні критичності

Критерій	Категорія (рівень)	Опис
А. Загроза порушення сталого, надійного та штатного режиму функціонування систем (системи)	А1	Загрози немає.
	А2	Безпосередня загроза для сталого, надійного та штатного режиму функціонування систем (конкретної системи суб'єкта забезпечення кібербезпеки).
	А3	Безпосередня загроза для сталого, надійного та штатного режиму функціонування декількох систем окремого суб'єкта забезпечення кібербезпеки.
	А4	Безпосередня загроза для сталого, надійного та штатного режиму функціонування значної кількості систем декількох суб'єктів забезпечення кібербезпеки.
	А5	Транскордонний вплив загрози порушення сталого, надійного та штатного режиму функціонування систем.
Б. Загроза порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі)	Б1	Загрози немає
	Б2	Створені передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).
	Б3	Порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).

Продовження табл. 3.1 – Категорії та рівні критичності

В. Загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.	В1	Загрози немає
	В2	Передумови для припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.
	В3	Потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.
	В4	Реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.
	В5	Невідворотна загроза для повноцінного функціонування держави або загроза життю громадян України.

Коли відбувається декілька кіберінцидентів або кібератак одночасно, важливо встановити пріоритети для реагування на кожен з них. Це дозволяє ефективно розподіляти доступні ресурси – часові, людські, технічні та матеріальні – для максимально швидкого та ефективного реагування.

Основними критеріями для визначення пріоритетності реагування є:

1) Серйозність та вплив кіберінциденту: Інциденти, які мають більш серйозні наслідки або створюють значні ризики для критичних операцій або чутливих даних, мають вищий пріоритет.
2) Можливість поширення: Інциденти, які можуть швидко поширюватися або ескалювати, вимагають термінового втручання, щоб запобігти додатковим збиткам.
3) Здатність до відновлення: Якщо кіберінцидент вражає системи, які важко або тривало відновлювати, такі інциденти потребують негайної уваги.

4) Юридичні та репутаційні наслідки: Інциденти, які несуть високі ризики юридичної відповідальності або шкоди репутації, також мають велике значення.

На етапі виявлення та аналізу команда реагування на кіберінциденти/кібератаки може використати інформацію щодо технік та прийомів зловмисника для того, щоб змінити налаштування інструментів та засобів, що використані під час реагування (згідно із пунктом 5 розділу II Рекомендацій) [33]. Ці дії мають дати змогу уповільнити темпи просування шкідливого програмного забезпечення (ШПЗ зловмисника) вглиб периметра систем (внутрішнього та зовнішнього (фізичного)), внутрішньої мережі, мережевих пристроїв, хостів та сховищ даних, збільшити витрати зловмисника (часові, матеріальні, людські), зменшити поточний вплив зловмисника та збільшити ймовірність виявлення наслідків подальших дій зловмисника [33].

При реагуванні на кіберінциденти та кібератаки, необхідно враховувати ризик введення в мережу чи систему нових інструментів або модифікації існуючих засобів з метою обходу встановлених механізмів захисту. Атакуючі часто використовують тактики, які ускладнюють виявлення та реагування на загрози, особливо шляхом зміни характеристик або поведінки відомих інструментів або впровадженням нових.

Мета етапу стримування під час реагування на кіберінцидент або кібератаку полягає в тому, щоб запобігти подальшій ескалації ситуації та зменшити негативний вплив інциденту чи атаки. Це досягається шляхом усунення або обмеження можливостей зловмисника, у тому числі відмовою у доступі до систем або мереж. У процесі кіберзахисту важливо враховувати, що зловмисники можуть активно моніторити заходи реагування та адаптувати свої тактики, техніки та процедури (ТТП), щоб уникнути виявлення і стримування. Це вимагає від оборонних команд забезпечення кібербезпеки розробки глибокого розуміння потенційних здібностей і можливих реакцій зловмисника.

Метою етапу усунення є відновлення штатного режиму функціонування шляхом усунення артефактів інциденту (наприклад, видалення зловмисного коду, створення повторного образу пам’яті елементів «заражених» систем) і пом’якшення наслідків від реалізації кіберзагроз або інших умов, якими скористався зловмисник (зловмисні групи). Перш ніж перейти до ліквідації наслідків, слід переконатися, що було враховано всі засоби постійного доступу до мережі, активність зловмисника стримана достатньою мірою, всі електронні докази було зібрано, а також чи можлива циклічність цих умов. Етап усунення також може передбачати посилення або модифікацію захисту систем/мереж (середовища захисних систем та пристроїв, призначених для захисту систем/мереж від несанкціонованого доступу, впливу ШПЗ (ШПЗ зловмисника)), якщо відома першопричина атаки та/або вектор початкового доступу. Заходи з ліквідації наслідків та відновлення можуть бути виконані одночасно. Перед початком заходів із ліквідації наслідків необхідна координація дій з постачальниками послуг, уповноваженими та правоохоронними органами, суб’єктами національної системи кібербезпеки [33].

Етап відновлення після кіберінциденту або кібератаки зосереджений на пом'якшенні наслідків від реалізованих кіберзагроз та інших дій зловмисника. Цей етап включає ряд ключових завдань та має важливе значення для відновлення нормального функціонування систем та процесів. Основні аспекти етапу відновлення включають:

1) Підтвердження успішного усунення наслідків: Необхідно переконатися, що всі аспекти кіберінциденту або кібератаки були успішно вирішені та що відновлені системи є безпечними для повторного використання.
2) Перебудова систем та мереж: Може включати зміну конфігурації системних та мережевих пристроїв, їх структуру в межах системи або мережі для підвищення їх безпеки та відновлення функціональності.

3) Відновлення нормальної роботи систем та процесів: Необхідно відновити всі операції, що були порушені внаслідок кіберінциденту, та повернутися до звичного режиму роботи.
4) Підвищена пильність та моніторинг: Після відновлення потрібно забезпечити підвищений контроль та моніторинг середовища для переконання у відсутності додаткових ознак зловмисної діяльності.
5) Аналіз та досвід, винесені з інциденту: Важливо проаналізувати інцидент, вивчити отриманий досвід, та внести необхідні зміни у процедури та політики для запобігання майбутнім інцидентам.

Основна мета етапу аналізу ефективності реакції на кіберінциденти або кібератаки полягає у створенні звіту про інцидент, інформуванні керівництва організації забезпечення кібербезпеки, удосконаленні захисних механізмів систем та мереж, перегляді відповідної документації та політик і використанні здобутого досвіду для покращення управління майбутніми інцидентами. Також важливо налаштувати системи виявлення (детектори), процедури оповіщення та методи збору даних, включаючи інформацію з лог-файлів. Після розгляду кіберінциденту необхідно оновити та покращити елементи процедури виявлення в межах організації, визначити потенційно вразливі сегменти систем чи мереж, які можуть бути використані зловмисниками в майбутньому, а також ретельно моніторити середовища для виявлення ознак постійної активності зловмисника.

3.3 Принципи побудови системи виявлення та запобігання вторгненням (IDS/IPS)

IDS/IPS (системи виявлення та запобігання вторгненням) – це комплексні програмні чи апаратні рішення, які забезпечують безпеку мереж та комп'ютерних систем. IDS виступає у ролі пасивної системи виявлення, яка в реальному часі моніторить увесь мережевий трафік і, у разі необхідності, сповіщає про потенційні загрози. Основна особливість IDS полягає в тому, що вона не вносить змін до

мережевих пакетів даних і не впливає на роботу мережі. Натомість IPS є більш активною системою, яка може блокувати доставку підозрілих пакетів, виконуючи функції, аналогічні функціям брандмауера [37].

Загалом, основним принципом систем виявлення вторгнень є аналіз вхідного та вихідного трафіку для виявлення потенційних загроз. Однак, методи аналізу можуть відрізнятися, і можна виділити три основні типи IDS залежно від механізму аналізу:

1) Сигнатурні IDS: Ці системи працюють схоже на традиційні антивіруси, аналізуючи трафік і порівнюючи пакети з базою даних відомих сигнатур. Щоб система працювала ефективно, необхідно регулярно оновлювати базу даних сигнатур. Головним недоліком є те, що в разі відсутності доступу до бази даних, система не зможе ідентифікувати загрози.
2) IDS, засновані на аномаліях: Використовують технологію машинного навчання для аналізу поведінки мережі та порівняння її з попередньою активністю. Система може виявляти статистичні, протокольні аномалії або аномалії на рівні трафіку, за умови достатнього обсягу навчання у минулому.
3) Правилові IDS: Адміністратор може налаштувати конкретні правила для системи, які допомагають виявляти погрози на основі прямих чи непрямих індикаторів. Налаштування такої системи вимагає більше часу та знань, але може забезпечити високий рівень захисту на практиці.

На основі аналізу наявних рішень можна навести перелік компонентів, з яких складається типова система виявлення атак [37].

Модуль стеження забезпечує збір даних з контрольованого простору (журналу реєстрації або мережевого трафіку). Різні виробники дають цьому модулю такі назви: сенсор (sensor), монітор (monitor), зонд (probe) тощо.

Залежно від архітектури побудови системи виявлення атак, модуль стеження може бути фізично відокремлений від інших компонентів, тобто перебувати на іншому комп’ютері.

Підсистема виявлення атак – основний модуль системи виявлення атак. Вона здійснює аналіз інформації, одержуваної від модуля стеження. За результатами цього аналізу ця підсистема може ідентифікувати атаки, ухвалювати рішення щодо варіантів реагування, зберігати відомості про атаку в сховищі даних тощо.

База знань залежно від методів, що використовуються в системі виявлення атак, може містити профілі користувачів і обчислювальної системи, сигнатури атак або підозрілі рядки, що характеризують несанкціоновану діяльність. База знань може поповнюватися виробником системи виявлення атак, користувачем системи або третьою стороною, наприклад, аутсорсинговою компанією, що здійснює підтримку цієї системи [37].

Сховище даних забезпечує зберігання даних, зібраних у процесі функціонування системи виявлення атак.

Графічний інтерфейс. Навіть дуже потужний і ефективний засіб не буде використовуватися, якщо у нього відсутній дружній інтерфейс. Залежно від ОС, під управлінням якої функціонує система виявлення атак, графічний інтерфейс має відповідати стандартам де-факто для Windows і Unix.

Підсистема реагування здійснює реагування на виявлені атаки та інші контрольовані події. Варіанти реагування будуть описані більш детально нижче.

Підсистема управління компонентами призначена для управління різними компонентами системи виявлення атак. Під терміном "управління" розуміється можливість зміни політики безпеки для різних компонентів системи виявлення атак (наприклад, модулів стеження), а також отримання інформації від цих компонентів (наприклад, відомості про зареєстровану атаку). Управління може здійснюватися як

за допомогою внутрішніх протоколів та інтерфейсів, так і за допомогою вже розроблених стандартів, наприклад, SNMP [37].

Системи виявлення атак будуються на основі двох архітектур: "автономний агент" і "агент-менеджер". У першому випадку на кожен вузол або сегмент мережі, що захищається, встановлюються агенти системи, які не можуть обмінюватися інформацією між собою, а також не можуть управлятися централізовано з єдиної консолі. Цих недоліків позбавлена архітектура "агент-менеджер". У цьому разі в розподіленій системі виявлення атак dIDS (distributed IDS), що складається з безлічі IDS, розташованих у різних ділянках великої мережі, сервери збору даних і центральний сервер, що аналізує, здійснюють централізований збір і аналіз реєстрованих даних. Управління модулями dIDS здійснюється з центральної консолі управління. Для великих організацій, у яких філії рознесені по різних територіях і навіть містах, використання такої архітектури має принципове значення.

Розподілена система виявлення атак dIDS складається з таких елементів: консолі управління, серверів, що аналізують, агентів мережі, серверів збору інформації про атаку. Центральний аналізуючий сервер зазвичай складається з БД і Web-сервера, що дає змогу зберігати інформацію про атаки і маніпулювати даними за допомогою зручного Web-інтерфейсу. Агент мережі – один із найважливіших компонентів dIDS. Він являє собою невелику програму, мета якої – повідомляти про атаку на Центральний аналітичний сервер. Сервер збору інформації про атаку – частина системи dIDS, що логічно базується на центральному аналізуючому сервері. Сервер визначає параметри, за якими групуються дані, отримані від агентів мережі. Групування даних може здійснюватися за такими параметрами:

- IP-адресою атакуючого;
- портом одержувача;
- номером агента;
- датою, часом;

- протоколом;
- типу атаки тощо.

3.4. Аналіз та побудова узагальненої моделі порушника, загроз та безпеки для систем критичної інфраструктури

Загрози безпеки інформації важливо класифікувати за різними критеріями, одним з яких є локалізація джерела загрози. Це розділення на внутрішні та зовнішні загрози дозволяє розробити більш точні та ефективні заходи безпеки. Зовнішні загрози походять з-за меж об'єкта критичної інформаційної інфраструктури (ЗВІД) і включають дії сторонніх осіб, відвідувачів, а також представників інших організацій, які не мають авторизованого доступу до системи. Ці порушники можуть впливати на інформацію через зовнішні автоматизовані системи.

Внутрішні загрози, навпаки, виникають всередині контрольованої зони ЗВІД і можуть бути зумовлені діями осіб, які мають доступ до приміщень із засобами обчислювальної техніки. Вони можуть бути як авторизованими користувачами, так і неавторизованими, що включає системних адміністраторів, адміністраторів безпеки, звичайних користувачів та технічний персонал.

Важливість розуміння та розрізнення між цими двома типами загроз полягає у здатності розробляти більш цілеспрямовані стратегії захисту, які враховують унікальні характеристики та потенційні ризики, пов'язані з кожною категорією.

Під час аналізу безпеки інформації в системах критичної інфраструктури важливо враховувати різні типи потенційних порушників. Потенційний порушник може бути особою, яка, навмисно чи випадково, внаслідок незнання або злого наміру, здійснює дії, що можуть порушити конфіденційність, цілісність, або доступність інформації. Ці дії можуть використовувати різні методи та засоби, і це важливо врахувати при розробці заходів безпеки.

Одним з ключових припущень у такому аналізі є високий рівень довіри до адміністратора безпеки, який вважається відповідальним за забезпечення захисту

інформації. Традиційно, така особа не розглядається як потенційний порушник, проте важливо вживати додаткові заходи контролю з боку керівництва, щоб запобігти будь-яким можливостям зловживання.

Модель порушника включає аналіз його практичних та потенційних можливостей, попередніх знань, часу та місця дії. Такий аналіз дозволяє виявити та оцінити різні категорії загроз, що можуть виникнути від різних типів осіб, та розробити відповідні стратегії для їх запобігання та мінімізації можливого впливу на системи критичної інфраструктури.

Під час аналізу безпеки інформації в системах критичної інфраструктури важливо враховувати різні типи потенційних порушників. Потенційний порушник може бути особою, яка, навмисно чи випадково, внаслідок незнання або злого наміру, здійснює дії, що можуть порушити конфіденційність, цілісність, або доступність інформації. Ці дії можуть використовувати різні методи та засоби, і це важливо врахувати при розробці заходів безпеки.

Одним з ключових припущень у такому аналізі є високий рівень довіри до адміністратора безпеки, який вважається відповідальним за забезпечення захисту інформації. Традиційно, така особа не розглядається як потенційний порушник, проте важливо вживати додаткові заходи контролю з боку керівництва, щоб запобігти будь-яким можливостям зловживання. Модель порушника включає аналіз його практичних та потенційних можливостей, попередніх знань, часу та місця дії. Такий аналіз дозволяє виявити та оцінити різні категорії загроз, що можуть виникнути від різних типів осіб, та розробити відповідні стратегії для їх запобігання та мінімізації можливого впливу на системи критичної інфраструктури.

3.4.1. Аналіз моделей потенційних порушників та рекомендації щодо їх побудови

Модель порушника в контексті захисту інформаційних систем є важливим інструментом для аналізу та прогнозування загроз безпеки. Вона є абстрактним і

часто формалізованим описом потенційних дій порушника, включаючи його практичні та теоретичні можливості, апріорні знання, час та місце дії та інші фактори.

Під час побудови такої моделі рекомендується аналізувати та упорядковувати інформацію про потенційних порушників, які можуть намагатися отримати несанкціонований доступ до автоматизованих систем (АС). Варто звернути увагу на привабливість ресурсів АС для різних груп осіб, зокрема з огляду на характер та обсяг інформації, яка в них зберігається та обробляється.

Модель повинна охоплювати такі аспекти:

- Категорії потенційних порушників: Визначення різних груп осіб, які можуть становити загрозу.
- Рівень можливостей порушника: Оцінка потенційних здібностей та ресурсів, які можуть бути використані для здійснення порушень.
- Кваліфікація та рівень знань порушника: Припущення щодо технічних та інших знань, які можуть мати порушники.
- Методи та способи порушень: Огляд потенційних способів, якими порушники можуть діяти.
- Мета порушника: Визначення можливих цілей порушників та оцінка їх небезпечності для системи.
- Можливі місця здійснення порушень: Ідентифікація локацій, де порушення можуть бути найбільш ймовірними.
- Способи реалізації загроз в АС: Оцінка різних технік та засобів, які можуть бути використані для створення загроз.

Класифікація порушників за рівнем можливостей, наданих їм штатними засобами автоматизованої системи (АС), дозволяє ефективно оцінити ризики та визначити потенційні стратегії запобігання порушень. Ця класифікація є

ієрархічною, де кожен наступний рівень включає в себе можливості попереднього [34]:

1) перший рівень визначає найнижчий рівень можливостей проведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
2) другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
3) третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
4) четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Три основні мотиви порушень безпеки інформаційних систем можуть бути визначені як безвідповідальність, самоствердження та корисливий інтерес. Кожен з цих мотивів має свої характеристики та вимагає відмінних підходів до запобігання та виявлення. Класифікація порушників представлена у табл. 3.2 [35].

- Безвідповідальність – цей тип порушень часто є результатом некомпетентності або недбалості. Користувачі можуть випадково або навмисно виконувати дії, що призводять до збоїв у системі або втрати даних, але без злого умислу. Такі дії можуть включати випадкове видалення важливих файлів або неправильне використання системних ресурсів.
- Самоствердження – у цьому випадку порушник намагається довести свої здібності або знання, часто в спробі вразити себе або інших. Такі порушення часто є спробами проникнення або злому системи, сприймаючи це як виклик

або гру. Хоча такі дії можуть не мати корисливого інтересу, вони все одно становлять серйозну загрозу для безпеки системи.

- Корисливий інтерес – тут порушник цілеспрямовано намагається обійти системи безпеки для доступу до конфіденційної інформації або здійснення інших зловмисних дій. Мотивами можуть бути фінансова вигода, шпигунство, саботаж тощо. Незважаючи на заходи безпеки, повністю унеможливити проникнення в систему може бути складно.

Таблиця 3.2 – Класифікація порушників

Класифікація	Характеристика
За рівнем знань про АС	• знає функціональні особливості АС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами; • має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням; • має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем; • знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.
За рівнем можливостей (методам і засобам що використовуються)	• застосовує чисто агентурні методи отримання відомостей; • застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи); • використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

Продовження табл. 3.2 – Класифікація порушників

	• застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).
За часом дії	• у процесі функціонування (під час роботи компонент системи); • у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.); • як у процесі функціонування, так і в період неактивності компонент системи.
За місцем дії	• без доступу на контрольовану територію організації; • з контрольованої території без доступу до будівель та споруджень; • усередині приміщень, але без доступу до технічних засобів; • з робочих місць кінцевих користувачів (операторів); • з доступом у зону даних (баз даних, архівів і т.д.); • з доступом у зону управління засобами забезпечення безпеки.

3.4.2. Аналіз моделей загроз кібербезпеці та рекомендації щодо їх побудови

Загрози для інформаційних систем та процесів можуть мати різноманітні форми і наслідки, тому важливо розуміти їх класифікацію для ефективного аналізу та встановлення відповідних заходів безпеки. Одним із підходів до класифікації загроз є розподіл їх за результатами впливу на інформацію та системи її обробки.

Згідно з документом, розробленим ДССЗІ (Державною службою спеціального зв'язку та інформації), зазіхання або загрози безпеки інформації можуть відбуватися різними шляхами, що включають наступні основні методи [35]:

1) Перехоплення або знімання інформації включає відстежування або перехоплення інформації, яка передається по каналах зв’язку, з метою її копіювання чи поширення. Такі дії можуть суперечити законодавству та використовуватися для незаконних цілей.
2) Неправомірний доступ до баз даних включає отримання доступу до баз даних, в яких зберігаються конфіденційні відомості, такі як номери паспортів, адреси, медичні історії тощо. Доступ може бути використаний не тільки для копіювання або неправомірного поширення відомостей, але й для їх зміни, знищення або внесення спотворень [35].

Для реалізації цих зазіхань зловмисники використовують різні спеціальні програмні та технічні засоби. Оператори систем, часто, не мають готових рішень для відповіді на такі виклики, створені з використанням сучасних технологій.

«Модель загроз» є ключовим інструментом для ідентифікації та аналізу потенційних ризиків, які можуть виникати під час обробки персональних даних. Суб'єкти ринку, які включені до реєстру та підлягають перевірці ДССЗІ, повинні не тільки дотримуватися чинної нормативної документації, але й бути готовими вирішувати нові виклики, які виходять за рамки існуючих регуляцій. Ось деякі з ключових завдань, які включає «Модель загроз»:

- розробка індивідуальних моделей загроз. Кожен суб'єкт повинен створити власну модель загроз, яка була б актуальною та специфічною для його діяльності. Ця модель має враховувати різні види інформації, які обробляються, та потенційних порушників [35].
- аналіз і моніторинг поточної ситуації із захистом баз персональних даних від зовнішнього проникнення [35];

- розробка власної системи захисту баз даних і нейтралізації потенційних загроз, заснованої на пропонованих для кожної окремої системи методах і рекомендаціях [35];
- організація технічної системи захисту засобів обробки даних, яка повинна виключити будь-який вплив на них, що може спричинити їх пошкодження або руйнування [35];
- постійний контроль якості захисту [35];
- систематичне проведення заходів, які повинні виключити несанкціоноване проникнення до баз даних порушників – третіх осіб, яким не оформлений допуск до вивчення і обробці цієї інформації [35].

Під час аналізу потенційних джерел загроз необхідно розглядати різні категорії, такі як загрози, що виникають внаслідок зловживання службовим становищем, а також технічні, програмні та фізичні загрози. Конкретна загроза стає реальною, коли виникає можливість доступу між особою, яка має намір здійснити незаконну дію, та об'єктом, що підлягає захисту. Це створює умови для потенційного несанкціонованого, навмисного або випадкового проникнення до захищеного об'єкта.

Різноманітність загроз, що існують, вимагає ретельного аналізу персоналу, особливо тих співробітників, які мають доступ до конфіденційної інформації. Крім того, важливо звернути особливу увагу на технічну безпеку систем зберігання та обробки даних. Це включає використання високоспеціалізованого програмного забезпечення, такого як системи DLP (Data Loss Prevention), SIEM (Security Information and Event Management), а також інших засобів для захисту інформаційних ресурсів [36].

У моделі загроз безпеки використовується класифікація, яка базується на різних типах технічних засобів, що забезпечують доступ до захищених масивів інформації. Ця класифікація дозволяє розуміти та оцінювати різні потенційні канали

проникнення або вразливі місця, через які може бути здійснений доступ до конфіденційної інформації:

- використання шкідливих програм, вірусів, хробаків і аналогічних, що створюються з свідомо протиправними цілями;
- втрати даних з технічних і фізичних каналах витоку;
- інші спеціальні впливи [36].

У моделі загроз безпеки включена класифікація, яка базується на різних типах використовуваного обладнання. Це дозволяє визначити різні потенційні джерела загроз, залежно від специфіки технічних засобів, що використовуються в інформаційних системах. Різні види обладнання, такі як сервери, мережеві пристрої, комп'ютери користувачів, мобільні пристрої та інші, мають різні рівні вразливості та способи потенційного використання зловмисниками.

Для виявлення точок уразливості в інформаційних системах, регулярний аудит безпеки та систем захисту інформації є ключовим. Цей процес включає аналіз потенційних можливостей доступу передбачуваних порушників до засобів комп’ютерної обробки інформації. Важливо враховувати, що майже будь-яке офісне технічне обладнання може становити потенційне джерело загрози. Модель безпеки, яка класифікує ці загрози, дозволяє глибше зрозуміти та зміцнити захист від різноманітних вразливостей і потенційних атак [36].

Модель безпеки класифікує їх наступним чином [36]:

- АРМ;
- виділені засоби обробки (принтери, копіювальні апарати, звукозаписна апаратура, засоби відеоспостереження;
- мережі зв’язку [36]

3.5 Висновки до розділу 3

Розділ 3 присвячений викликам та перспективам розвитку кібербезпеки критичної інфраструктури. Дослідження показало, що кіберзагрози стають все

більш складними та небезпечними, що ставить під загрозу безпеку критичної інфраструктури. Однак, з іншого боку, розвиток технологій та методів забезпечення кібербезпеки дозволяє ефективно боротися з цими загрозами та забезпечувати безпеку критичних систем.

У цілому, розділ надає важливу інформацію про виклики та перспективи розвитку кібербезпеки критичної інфраструктури. Результати дослідження показують, що розвиток новітніх технологій та методів забезпечення кібербезпеки може допомогти ефективно боротися з кіберзагрозами та забезпечити безпеку критичних систем. Застосування штучного інтелекту та інших інноваційних технологій може значно підвищити ефективність систем забезпечення кібербезпеки та зменшити ризики виникнення інцидентів. Результати дослідження можуть бути використані для розробки ефективних стратегій та методів забезпечення кібербезпеки критичної інфраструктури, що дозволить забезпечити найвищий рівень безпеки критичних систем та зменшити ризики виникнення інцидентів.

4 РЕКОМЕНДАЦІЇ ІЗ РОЗРОБКИ КОМПЛЕКСНОЇ СТРАТЕГІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

4.1 Оцінка ризиків та аудит кібербезпеки

Кібер-ризик – це тип операційного ризику, що виникає, коли економічні суб'єкти зазнають прямих або опосередкованих економічних втрат у результаті їх діяльності в кібернетичному просторі.

Цей термін може бути інтерпретований у двох контекстах:

Вузьке трактування кібер-ризиків: Тут вони асоціюються з операційними загрозами, що стосуються інформаційних та технологічних ресурсів. Такі ризики можуть негативно впливати на конфіденційність, доступність і цілісність інформації чи інформаційних систем.

Широке трактування кібер-ризиків: У цьому контексті вони охоплюють потенційні загрози, що впливають на інтерактивні цифрові мережі, які використовуються для передачі, зміни та зберігання інформації в кіберпросторі.

Кібер-ризик також включає загрози, пов'язані з онлайн-активностями, інтернет-торгівлею, електронними системами і технологічними мережами, а також зберіганням персональних даних (рис. 4.1).

Рисунок 4.1 – Види кібер-ризиків

Аудит кібербезпеки представляє собою ретельну перевірку та оцінку політик безпеки в організації, з метою забезпечення їх відповідності нормативним стандартам та рекомендованим практикам. Цей процес охоплює три основні сфери в рамках інформаційної безпеки: технічну, фізичну та адміністративну.

Через проведення аудитів безпеки, організації отримують можливість виявлення та усунення внутрішніх загроз та уразливих місць. Такі аудити є ключовими для запобігання порушень безпеки та протидії кіберзагрозам і кібератакам, які можуть негативно впливати на безпеку, добре ім'я та фінансову стійкість організації.

Аудит безпеки виконується за встановленою процедурою, що включає наступні кроки:

1) Встановлення критеріїв оцінки: Необхідно визначити цілі аудиту для зрозуміння поточних проблем і загроз. Важливо ідентифікувати основні ризики і вразливості, а також вибрати підходи та методики для проведення аудиту.
2) Аналіз існуючих політик та методів безпеки: На цьому етапі аналізується нинішній стан безпеки, включаючи потенційні загрози, ризики і слабкі місця. Це допомагає визначити, що може бути покращено або змінено для посилення загальної безпеки.
3) Підготовка до аудиту безпеки: На цьому етапі розробляється план аудиту, з акцентом на найбільш проблемні області. Вибираються відповідні інструменти та методи для збору і аналізу даних.
4) Реалізація аудиту безпеки: Виконується аудит з використанням обраних інструментів і методик. Важливо забезпечити документування процесу і результатів для подальшого аналізу та використання.
5) Завершення аудиту та оформлення висновків: По завершенні аудиту складається звіт з результатами та рекомендаціями щодо необхідних змін для

підвищення рівня безпеки. Результати аудиту діляться з відповідними підрозділами для подальших дій [38].

Неперервний процес розробки та оновлення програмного забезпечення змушує організації впроваджувати нове апаратне та програмне забезпечення, що веде до створення нових робочих станцій і може спричинити виникнення нових вразливостей та загроз. Аудит є ключовим для оцінювання рівня безпеки, а регулярне проведення аудитів дозволяє виявляти ці нові загрози та вразливості, сприяючи кращому розумінню організацією своїх політик і стратегій у сфері безпеки. Аудити безпеки можуть бути класифіковані за трьома основними категоріями. Перша категорія – це одноразовий аудит, який виконується при впровадженні нових програм чи у разі виникнення особливих обставин, що змінюють звичайний хід операційної діяльності. Такий аудит націлений на виявлення можливих ризиків та загроз, пов'язаних із цими нововведеннями, для забезпечення безпеки оновлених систем.

Друга категорія – аудит вартості. Цей тип аудиту видає бінарні результати для оцінки нових процесів. Якщо результати показують, що процес безпечний, його можна впроваджувати. У разі виявлення потенційних ризиків чи загроз, такий процес відхиляється.

Третя категорія – портфельний аудит, який проводиться щороку або кожні два роки. Цей тип аудиту зосереджений на перевірці відповідності діяльності організації встановленим стандартам і процедурам безпеки, гарантуючи їх дотримання та виявляючи можливі відхилення для своєчасного виправлення [38].

Рекомендації щодо проведення аудиту безпеки

a. Ретельно задокументуйте всі аспекти аудиту, включаючи інформацію про відповідальних осіб та перелік елементів, які будуть перевірятися.
b. Ведіть записи існуючої політики безпеки, щоб мати можливість порівняти її стан до та після внесених змін та ідентифікувати ключові проблеми.

c. Оцініть чинні заходи безпеки та переконайтеся, що вони дотримуються належним чином.
d. Регулярно оновлюйте програмне забезпечення, щоб уникнути ризиків, пов’язаних із вразливостями в застарілих версіях.
e. Перевіряйте фаєрволи на наявність можливих слабких місць, які можуть створити ризики.
f. Забезпечте, щоб доступ до даних відповідав принципам розділення обов'язків та мінімально необхідних прав.
g. Використовуйте сучасні методи шифрування для забезпечення конфіденційності, цілісності та достовірності даних.
h. Перевірте та уточніть політики безпеки бездротових мереж, впроваджуючи стандартні заходи безпеки.
i. Регулярно скануйте мережу та точки доступу, щоб перевіряти автентичність з'єднань і передачі даних.
j. Слідкуйте за журналами подій для виявлення та аналізу будь-яких несанкціонованих дій чи аномалій у системі.

4.2 Планування заходів захисту інформації

Планування заходів захисту інформації починається з оцінки ризиків, де важливо ідентифікувати потенційні загрози та вразливості, які можуть виникнути в інформаційних системах організації. Це включає аналіз як внутрішніх, так і зовнішніх ризиків, а також оцінку можливих наслідків цих ризиків для бізнесу.

Далі, на етапі розробки політики безпеки, створюються чіткі правила та процедури, яких повинні дотримуватися усі співробітники. Ця політика повинна регулярно оновлюватися, щоб відповідати новим викликам та технологічним змінам, а також забезпечувати залученість та обізнаність персоналу.

На етапі впровадження заходів технічного захисту, організація має встановити відповідне програмне та апаратне забезпечення, які включають фаєрволи,

антивірусні програми, системи виявлення вторгнень та шифрування даних. Разом з цим, забезпечення фізичного захисту є також важливим, оскільки воно включає обмеження фізичного доступу до критичних об'єктів, захист від стихійних лих та моніторинг через системи відеоспостереження.

Навчання персоналу є критично важливим, оскільки співробітники часто є першою лінією оборони проти кіберзагроз. Проведення регулярних тренінгів та освітніх програм, а також симуляції реальних інцидентів, може значно підвищити рівень безпеки.

Регулярний моніторинг та аудит систем забезпечують виявлення нових вразливостей або невідповідностей політикам безпеки, а також дозволяють відслідковувати мережевий трафік для виявлення підозрілої активності.

Розробка плану реагування на інциденти має забезпечити, що організація може швидко і ефективно відповісти на будь-які безпекові порушення. Це включає в себе створення чітких процедур реагування, формування спеціалізованих груп для відновлення роботи після інцидентів, а також регулярне тестування та оновлення плану.

Останнім етапом є оновлення та підтримка систем безпеки. Оновлення охоплює застосування останніх патчів безпеки, оцінку нових технологій, а також збір зворотного зв'язку від співробітників для постійного вдосконалення заходів безпеки.

В Україні існує ряд нормативних документів, які регулюють планування заходів захисту інформації. Ось деякі з них:

1) Закони України:

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII [18].
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [19].
- Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [39].

- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [20].

2) Постанови Кабінету Міністрів України:

- Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373 [40].

- Постанова КМУ «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736 [41].

3) Нормативні документи в галузі технічного захисту інформації та державні стандарти України (ДСТУ):

- НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [42].

- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96 [43].

- НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [44].

- НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу" [45].

Таким чином, комплексний підхід до планування заходів захисту інформації передбачає не тільки технічні рішення, а й активну участь персоналу, постійне оновлення процесів та політик, і готовність до реагування на інциденти.

4.3 Розробка політик та процедур безпеки

Політика інформаційної безпеки є комплексом законодавчих норм, правил, рекомендацій та здобутого практичного досвіду, які формують основу для управлінських та проектних рішень у сфері захисту інформації. Вона визначає, як має бути організовано керування, захист і розподіл критично важливої інформації у

системі, враховуючи всі аспекти процесу обробки інформації та поведінку інформаційної системи в різних умовах.

Згідно з підходами, запропонованими у спеціалізованій літературі, політика інформаційної безпеки реалізується за допомогою структурованого підходу, що базується на нормативно-методичній основі і включає в себе використання програмно-технічних засобів, визначаючи тим самим архітектуру системи захисту.

Політика безпеки для конкретної інформаційної системи повинна бути індивідуалізована, враховуючи технології обробки інформації, використовувані програмні та технічні засоби, а також структуру організації.

Для ефективного опису політики інформаційної безпеки для конкретної системи, адміністратори мають спочатку визначити область обмежень і умов в зрозумілих термінах, вказуючи на причини та цілі розробки цієї політики, що сприяє її дотриманню.

Інформація, яка циркулює в інформаційній системі, часто має критичне значення, а розділення програм та даних серед користувачів збільшує ризики. Тому кожен комп'ютер у мережі потребує ефективного захисту.

Головними цілями політики інформаційної безпеки є підвищення обізнаності співробітників щодо важливості захисту мережі, визначення їх ролі у забезпеченні безпеки, а також розподіл конкретних обов’язків з охорони інформації, що циркулює в мережі.

Стосовно політики безпеки в Інтернеті, організаціям часто необхідно уточнювати, чи ця політика охоплює всі з'єднання, через які ведеться робота з Інтернетом, чи лише безпосередньо з’єднання з Інтернетом. Також ця політика може регламентувати інші аспекти роботи в Інтернеті, які не пов’язані безпосередньо з безпекою, наприклад, персональне використання Інтернет-з'єднань [46].

Політика безпеки визначається як комплекс документованих управлінських рішень, які спрямовані на забезпечення захисту інформації та пов'язаних з нею ресурсів.

У процесі розробки та реалізації цієї політики варто керуватися кількома ключовими принципами:

- Забезпечення неможливості обходу захисних засобів.
- Посилення найслабших місць у системі.
- Недопущення переходу системи у відкритий стан.
- Мінімізація рівня привілеїв користувачів.
- Розподіл обов’язків серед персоналу.
- Використання багаторівневого захисту.
- Різноманітність захисних засобів.
- Забезпечення простоти та керованості системи.
- Гарантування загальної підтримки заходів безпеки.

Зокрема, важливо, щоб усі інформаційні потоки проходили через належні межмережеві екрани, не допускаючи обходу захисних механізмів. Надійність системи безпеки часто залежить від найбільш вразливих елементів, і часто це може бути не комп'ютер чи програма, а людський фактор.

Політика безпеки також має забезпечити, що система захисту інформації не переходить у відкритий стан при будь-яких умовах, а також мінімізувати права доступу, надані користувачам та адміністраторам. Поділ обов'язків допомагає уникнути порушень важливих процесів однією особою.

Застосування багаторівневого захисту, включаючи фізичний захист, програмно-технічні заходи, ідентифікацію та автентифікацію, керування доступом та аудит, дозволяє створити ешелоновану оборону. Різноманітність захисних засобів ускладнює завдання потенційних зловмисників.

Простота і керованість системи сприяють ефективному адмініструванню та контролю захисту. Загальна підтримка заходів безпеки включає створення умов для забезпечення лояльності персоналу, а також постійне навчання і практичне відпрацювання знань [47].

Перед тим, як приступити до реалізації заходів інформаційної безпеки, необхідно переконатися, що користувачі мають достатні навички для їх дотримання. Безпека вимагає не лише знань, але й конкретних дій. Важливо, щоб кожен користувач розумів, що робити у випадку виявлення порушення або підозри на його виникнення, і знав, до кого звертатися за допомогою. Користувачі повинні відчувати, що заходи безпеки приймаються для їхнього блага, а не з інших міркувань.

Розгляньте можливість залучення кваліфікованого консультанта з безпеки, який би надав користувачам відповідні знання. Якщо у вашій організації є можливість, запросіть такого консультанта на наступну зустріч, щоб він виступив як експерт під час розробки правил. Пам'ятайте, що наймання консультанта для самостійної розробки правил може знизити залученість звичайних користувачів і їх інтерес до правил.

Таким чином, ви зможете створити правила безпеки, які будуть важливими для кожного співробітника. Навіть, якщо в результаті ви отримаєте не найідеальніший документ, ефективність правил значно зросте.

Забезпечте користувачів докладними інструкціями, що відповідають прийнятному обсягу інформації. Навіть, якщо користувачі зрозуміли правила, вони можуть мати питання про те, як їх втілити на практиці. Надавайте разом із правилами стандартні процедури їх впровадження та приклади. Фіксуйте запитання від співробітників і ваші відповіді на них у документації до правил, інформуючи про ці доповнення користувачів.

Включайте до правил стандартні процедури та приклади їх застосування, переконайтеся, що ваші правила орієнтовані на захист від реальних загроз, які мають істотну ймовірність виникнення та представляють справжню небезпеку для вашої організації.

У загальному виді сукупність заходів, спрямованих на запобігання погроз, визначається в такий спосіб:

—резервування технічних засобів;

—регулювання доступу до технічних засобів, ПЗ, масивів інформації;

—регулювання використання програмно-апаратних засобів і масивів інформації;

—криптографічний захист інформації;

—контроль елементів ІС;

—реєстрація зведень;

—своєчасне знищення непотрібної інформації;

—сигналізація;

—своєчасне реагування [48].

4.4 Аналіз ефективності впроваджених заходів

Аналіз ефективності заходів забезпечення кібербезпеки стає ключовим елементом управління ризиками та забезпечення надійності інформаційних систем, особливо у галузі критичної інфраструктури. Такий аналіз включає оцінку поточного стану захисту, виявлення слабких місць та розробку стратегій для подальшого покращення та розвитку.

Основним завданням є систематичне виявлення та аналіз потенційних ризиків і загроз, які можуть впливати на критичну інфраструктуру. Це охоплює різноманітні сценарії, включаючи кібератаки, техногенні катастрофи, природні лиха та інші непередбачувані події.

Важливою складовою є розробка та втілення законодавчих норм та організаційних процедур, які забезпечують безпеку критичної інфраструктури. Це включає координацію дій між різними установами та організаціями. Також необхідно розробити та впровадити технічні, технологічні та програмні засоби, що мінімізують або запобігають негативному впливу загроз для критичної інфраструктури. До цього додаються фінансові та наукові механізми, які забезпечують необхідні ресурси та розвиток методів управління ризиками.

Важливою частиною стратегії є військово-оборонні та розвідувально-агентурні підходи для протидії ворожим і зловмисним діям. Також слід акцентувати увагу на інформаційних та освітніх механізмах, що включають розробку інформаційних матеріалів та навчання фахівців у сфері кібербезпеки.

Дипломатичні механізми сприяють міжнародній співпраці та забезпеченню безпеки на глобальному рівні. Важливим є постійний моніторинг і аналіз впроваджених заходів для виявлення прогалин у безпеці та розробки нових методів захисту.

Такий комплексний підхід, який поєднує різноманітні механізми і методики, забезпечує постійний розвиток та адаптацію заходів кібербезпеки до сучасних викликів і змінних умов.

Регламентування захисту інформації є складним завданням через розмаїтість існуючих ІС та типів оброблюваної інформації. Конкретні методи захисту варіюються в залежності від ресурсів підприємства, обсягу конфіденційних даних та їх значення. Загальні правила включають:

- Розробка та експлуатація системи захисту інформації є складною задачею, яка вимагає участі професіоналів.
- Прагнення до абсолютно надійного захисту є марним, адже такого не існує. Замість цього слід прагнути до створення достатньої, надійної, ефективної та

контрольованої системи. Ефективність захисту визначається не витратами на його організацію, а здатністю адекватно реагувати на загрози.

- Заходи захисту інформації мають бути комплексними, поєднувати різні методи та інструменти.
- Система захисту повинна будуватися з урахуванням того, що головна загроза може виходити від співробітників організації.

Залучення кваліфікованих фахівців до організації захисту інформації є необхідним, оскільки вони мають необхідні знання та досвід для ідентифікації загроз та розробки ефективних контрзаходів. Захист інформації стає окремою галуззю, де розробляються спеціальні інструменти для тестування, імітації загроз, аналізу програмного коду, а також створюються експертні системи для встановлення вимог до безпеки IT та оцінки їх дотримання.

Однак, у процесі захисту інформації важливу роль відіграють і звичайні користувачі, оскільки питання захисту не може бути вирішене виключно за допомогою технічних і програмних засобів. Людський фактор є значущим у забезпеченні конфіденційності та безпеки інформації [49].

4.5 Висновки до розділу 4

Розділ 4 присвячений аналізу ефективності впроваджених заходів забезпечення кібербезпеки критичної інфраструктури. Дослідження показало, що впровадження заходів забезпечення кібербезпеки є важливим етапом у забезпеченні безпеки критичних систем. Однак, ефективність цих заходів залежить від багатьох факторів, таких як правильний вибір технологій та методів забезпечення кібербезпеки, відповідність заходів вимогам та потребам критичної інфраструктури, а також відповідальність та компетентність персоналу.

Особлива увага приділена аналізу ефективності впроваджених заходів забезпечення кібербезпеки на прикладі реальних систем критичної інфраструктури. Результати дослідження показали, що впровадження заходів забезпечення

кібербезпеки дозволяє зменшити ризики виникнення інцидентів та забезпечити безпеку критичних систем. Однак, для досягнення максимальної ефективності необхідно постійно вдосконалювати технології та методи забезпечення кібербезпеки, а також проводити регулярні аудити та оцінки ефективності впроваджених заходів.

Крім того, у роботі досліджується вплив новітніх технологій, таких як штучний інтелект та блокчейн, на забезпечення кібербезпеки критичної інфраструктури. Результати дослідження можуть бути корисними для розробки ефективних стратегій та методів забезпечення кібербезпеки критичної інфраструктури, що дозволить забезпечити найвищий рівень безпеки критичних систем та зменшити ризики виникнення інцидентів.

ВИСНОВКИ

Метою цієї магістерської роботи був аналіз існуючих методів та заходів кібербезпеки для захисту критичної інфраструктури, а також створення рекомендацій щодо нових підходів, які відповідають сучасним викликам та загрозам. У ході дослідження було розглянуто системи критичної інфраструктури як об'єкт дослідження та методи та заходи забезпечення їх кібербезпеки як предмет дослідження.

Було проаналізовано поточний стан кіберзахисту систем критичної інфраструктури, вивчено міжнародний досвід у цій сфері, оцінено ризики та виявлено потенційні загрози. Важливим елементом роботи став аналіз рекомендацій, спрямованих на підвищення ефективності існуючих методів кібербезпеки.

У результаті, можна сказати, що ефективний кіберзахист критичної інфраструктури вимагає комплексного підходу, який включає технічні, організаційні та освітні стратегії. Важливо враховувати, що кіберзагрози постійно еволюціонують, тому необхідний постійний моніторинг, аналіз та адаптація заходів безпеки. Також ключовим є залучення кваліфікованих фахівців та розробка стандартів та нормативних документів, які відповідають сучасним вимогам кібербезпеки.

Разом з тим, у роботі було підкреслено необхідність міжнародної співпраці у сфері обміну знаннями та кращими практиками. Це дозволить підвищити загальний рівень безпеки та ефективно протидіяти кіберзагрозам на глобальному рівні.

Висновки з проведеного дослідження підкреслюють необхідність комплексного підходу до забезпечення кібербезпеки, особливо у сфері критичної інфраструктури. Ефективний захист вимагає глибокого розуміння потенційних загроз та розробки відповідних стратегій їх нейтралізації. Важливим є поєднання

технічних рішень з організаційними процедурами та освітніми програмами для залучення та навчання персоналу. Такий підхід забезпечує більш глибоке розуміння ризиків і більш ефективне управління ними.

Оскільки кіберзагрози постійно змінюються, системи кібербезпеки повинні бути гнучкими та адаптивними. Постійний моніторинг і оновлення заходів безпеки є важливими для підтримання їх актуальності. Ключовим є залучення кваліфікованих фахівців, які можуть виявляти складні загрози і розробляти ефективні стратегії протидії.

Міжнародна співпраця відіграє важливу роль у забезпеченні кібербезпеки, оскільки обмін знаннями, ресурсами та кращими практиками може підвищити рівень безпеки на глобальному рівні. Також важливо розробляти та впроваджувати стандарти і нормативні документи, що забезпечують єдині підходи до захисту інформації, підвищуючи ефективність системи кібербезпеки.

У сукупності, проведені дослідження надають основу для розробки та впровадження комплексних стратегій кібербезпеки, які адекватно реагують на загрози і забезпечують надійний захист критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.10.2023).
2. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Каб. Міністрів України від 23.08.2016 р. № 563 : станом на 22 жовт. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/563-2016-п#Text (дата звернення: 02.10.2023)
3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядж. Каб. Міністрів України від 06.12.2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р#Text (дата звернення: 12.10.2023)
4. Теленик С. Критична інфраструктура як об’єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. Т. 15, № 1. С. 179–189. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/3f833b7c-8c50-4334-baeb-55f1976d1dcd/content (дата звернення: 02.10.2023)
5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" : Указ Президента України від 26.05.2015 р. № 287/2015 : станом на 16 верес. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 03.11.2023).
6. Global Risks Report 2023 | World Economic Forum. World Economic Forum. URL: https://www.weforum.org/publications/global-risks-report-2023/ (дата звернення: 02.10.2023)

7. Benner, J. (2007). ISO 27001: Risk management and compliance. Risk Management Magazine, 55, pp. 24-29.
8. Humphreys, T. (2005). State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems, pp. 15-18.
9. Humphreys, T. (2006). State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems, Special report, pp. 9-13.
10. Louderback, J. (1995). Will you be ready when disaster strikes? PC Week, 12, pp. 130-131.
11. Cybersecurity Certificates - ISA. isa.org. URL: https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program (дата звернення: 12.10.2023)
12. DesRuisseaux D. Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System [Електронний ресурс] / Daniel DesRuisseaux // Version 1.0. – 7. URL: https://www.se.com/us/en/download/document/998-20298472/. (Дата звернення: 12.10.2023)
13. ДСТУ IEC 62443-4-1:2019. Безпечність систем промислової автоматизації та керування. Частина 4-1. URL: https://www.twirpx.com/ file/3101466/ (Дата звернення: 12.10.2023)
14. Наказ від 13.08.2019 № 249 Про прийняття національних стандартів та прийняття поправки до національного стандарту. БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=84240 (дата звернення: 01.10.2023)
15. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.11.2023)

16. ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=104399 (дата звернення: 13.11.2023)
17. «Наказ від 17.08.2023 № 210 Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів». БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/document.html?id_doc=104367 (дата звернення: 02.10.2023).
18. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.11.2023)
19. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації : Закон України від 04.06.2020 р. № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text (дата звернення: 13.11.2023)
20. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.11.2023)
21. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації : Закон України від 04.06.2020 р. № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text (дата звернення: 05.11.2023)

22. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.11.2023)
23. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації : Закон України від 04.06.2020 р. № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text (дата звернення: 07.11.2023)
24. Загальний регламент про захист даних (GDPR) - GDPR-Text.com. GDPR-Text.com - GDPR Text, Translation and Commentary. URL: https://gdpr-text.com/uk/ (дата звернення: 07.11.2023).
25. Cybersecurity of Ukraine: analysis of the current situation / О. Г. Трофименко et al. Ukrainian Information Security Research Journal. 2019. Vol. 21, no. 3. URL: https://doi.org/10.18372/2410-7840.21.13951 (дата звернення: 10.10.2023).
26. Підвищення рівня безпеки та захисту українців. Урядовий портал. URL: https://www.kmu.gov.ua/news/pidvyshchennia-rivnia-bezpeky-ta-zakhystu-ukraintsiv-uriad-ukhvalyv-postanovu-iaka-dozvoliaie-stvoryty-pravovi-osnovy-dlia-merezhi-sytuatsiinykh-tsentriv-v-ukraini (дата звернення: 02.10.2023)
27. Рада національної безпеки і оборони України. Cyber digest July 2023. *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/files/НКЦК/2023/Cyber%20digest_July_2023_UA.pdf (дата звернення: 02.10.2023)
28. Державне агентство з питань електронного урядування. *Урядовий контактний центр*. URL: https://www.ukc.gov.ua/derzhavne-agentstvo-z-pytan-elektronnogo-uryaduvannya-rozpochynaye-kampaniyu-trymaj-poradu-vid-susida/ (дата звернення: 05.11.2023)

29. Департамент Кіберполіції. URL: https://cyberpolice.gov.ua/ (дата звернення: 05.11.2023)
30. Проект Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf. (Дата звернення: 05.11.2023)
31. Будько М. МЕТОДИКА ОЦІНКИ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ СИСТЕМ. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2005. № 10. С. 35–46. URL: https://ela.kpi.ua/bitstream/123456789/11427/1/10_p35.pdf (дата звернення: 13.11.2023).
32. НД ТЗІ 1.1-005-07 "Захист інформації на об’єктах інформаційно діяльності. Створення комплексу технічного захисту інформації. Основні положення". *Головна - Приватне акціонерне товариство «Холдінгова компанія «Укрспецтехніка»*. URL: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-1.1-005-07.pdf (дата звернення: 01.11.2023).
33. Модель загроз безпеки персональних даних. *Searchinform*. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/model-ugroz-bezopasnostipersonalnyh-dannyh/ (дата звернення: 10.11.2023)
34. Що таке IPS/IDS і де застосовується - Блог - HostZealot. *HostZealot*. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 10.11.2023)
35. Пост | ISSP Training. *ISSP Training*. URL: https://www.issp.training/post/що-потрібно-знати-про-аудит-кібербезпеки. (дата звернення: 28.10.2023).
36. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 10.11.2023)

37. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 08.02.2021 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-п#Text (дата звернення: 05.11.2023)
38. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : Постанова Каб. Міністрів України від 19.10.2016 р. № 736 : станом на 25 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/736-2016-п#Text (дата звернення: 05.11.2023)
39. Державний стандарт України "НД ТЗІ 3.7-003-2005". *ТЗІ - інформаційна безпека та захист інформації*. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 05.11.2023)
40. Державний стандарт України "ДСТУ 3396.1-96". *ТЗІ - інформаційна безпека та захист інформації*. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf (дата звернення: 05.11.2023)
41. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Вид. офіц. Київ, 2000. 27 с. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf. (Дата звернення: 10.11.2023)
42. Державний стандарт України "НД ТЗІ 2.5-004-99". *ТЗІ - інформаційна безпека та захист інформації - Інформаційна безпека та захист інформації*. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf (дата звернення: 13.11.2023)
43. Кормич Б.А. "Організаційно-правові засади політики інформаційної безпеки України: Монографія". Одеса: Юрид. література, 2003. – 472 с.
44. Медвідь Ф. "Інформаційна безпека України в контексті становлення стратегії національної безпеки держави". Юридичний Вісник України. — 2008. — № 43. — С. 11.

45. Кормич Б.А. "Інформаційна безпека: організаційно-правові основи: навчальний посібник". Рекомендовано МОН України для вищих юридичних навчальних закладів. Київ: Кондор, 2004. – 384 с.
46. *Ужгородський національний університет*. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186 (дата звернення: 02.10.2023).

ДОДАТОК А
СЕКТОРИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Таблиця А.1 – Перелік секторів критичної інфраструктури

Сектор	Підсектор	Тип основної послуги	Секторальний орган у сфері захисту критичної інфраструктури
Паливно-енергетичний сектор	електроенергетика	виробництво електричної енергії	Міненерго
		забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку	
		управління системами передачі та енергопостачання	
		розподіл електричної енергії	
	вугільно-промисловий комплекс	видобуток вугілля для генерації електроенергії на теплоелектростанціях та теплоелектроцентралях	
		зберігання та постачання вугілля	
	торфодобування	розробка родовищ торфу	
		видобування корисних копалин	
	нафтова промисловість	видобуток нафти	
		передача (транзит) нафти та нафтопродуктів	
		очищення, переробка та обробка нафти	
		експлуатація нафтопроводів	
		зберігання та постачання нафти та нафтопродуктів	
	газова промисловість	видобуток газу	
		переробка та очищення газу	
		передача (транзит) газу	
		розподіл газу	
		забезпечення роботи систем зрідження природного газу	
		експлуатація газотранспортної системи	
		зберігання природного газу	
		забезпечення роботи систем зрідження природного газу	
	ядерна енергетика	виробництво ядерного палива	

Продовження табл. А.1– Перелік секторів критичної інфраструктури

		експлуатація ядерних підкритичних установок, ядерних реакторів, які включають критичні та підкритичні збірки дослідницьких реакторів	
		експлуатація атомних електростанцій, підприємств і установок по збагаченню та переробці палива, а також сховищ відпрацьованого палива	
Цифрові технології	електронні довірчі послуги та електронна ідентифікація	надання електронних довірчих послуг, електронної ідентифікації та автентифікації	Мінцифри
		забезпечення функцій центрального засвідчувального органу	
	електронні комунікації	адміністрування адресного простору українського сегмента Інтернету	
	електронне урядування	забезпечення функціонування системи електронної взаємодії органів виконавчої влади	
		забезпечення функціонування системи міжвідомчої взаємодії між органами державної влади, органами місцевого самоврядування та суб'єктами господарювання	
		надання електронних публічних послуг	
		автоматизація процесів надання адміністративних послуг	
		забезпечення функціонування правового режиму Дія Сіті	
Захист інформації		надання послуг (сервісів) кіберзахисту	Держспецзв'язку
Системи життєзабезпечення	комунальні послуги	постачання теплової енергії	Мінрегіон
		постачання гарячої води	
		централізоване питне водопостачання	
		централізоване водовідведення	
		поводження з побутовими відходами	
Харчова промисловість та агропромисловий комплекс		виробництво та переробка сільськогосподарської та/або харчової продукції	Мінагрополітики
		експлуатація зрошувальних систем, каналів	
Державний матеріальний резерв		забезпечення зберігання запасів державного матеріального резерву	Мінекономіки
Охорона здоров'я	медична допомога	забезпечення надання екстреної медичної допомоги	МОЗ

Продовження табл. А.1– Перелік секторів критичної інфраструктури

		забезпечення надання первинної медичної допомоги	
		забезпечення надання вторинної (спеціалізованої) медичної допомоги	
		забезпечення надання третинної (високоспеціалізованої) медичної допомоги	
		забезпечення надання паліативної медичної допомоги	
		забезпечення надання реабілітації у сфері охорони здоров'я	
	громадське здоров'я	заготівля і тестування донорської крові та компонентів крові	
		контроль за інфекційними захворюваннями та/або епідеміями	
	фінансове забезпечення у сфері охорони здоров'я	оплата згідно з тарифом за надані пацієнтам медичні послуги (включаючи медичні вироби) та лікарські засоби за договорами про медичне обслуговування населення за програмою медичних гарантій	
	інформаційні технології у сфері охорони здоров'я	функціонування електронної системи охорони здоров'я	
	фармацевтична промисловість	виробництво та постачання лікарських засобів і медичних виробів	
	медична наука	наукові дослідження в медичній галузі	
Ринки капіталу та організовані товарні ринки		забезпечення функціонування ринків капіталів та організованих товарних ринків	НКЦПФР
Фінансовий сектор		планування, виконання та моніторинг виконання бюджетів	Мінфін
		розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів	
		здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів	
Транспорт і пошта	авіаційний транспорт	управління повітряним рухом	Мінінфраструктури
		авіаперевезення (робота авіаційного транспорту)	
		забезпечення роботи аеропортів та допоміжного обладнання, що розташоване в аеропортах	

Продовження табл. А.1– Перелік секторів критичної інфраструктури

	автомобільний та міський електротранспорт, у тому числі метрополітен	автобусні перевезення (міжміські, міжнародні)	
		міські перевезення (автобуси, трамваї, тролейбуси, метрополітен)	
		технічне обслуговування транспортної інфраструктури (доріг, мостів, тунелів, шляхопроводів)	
		служби контролю трафіку	
		функціонування інтелектуальних транспортних систем (управління рухом, мобільністю, взаємодія з іншими видами транспорту)	
	залізничний транспорт	пасажирські залізничні перевезення	
		вантажні залізничні перевезення	
		експлуатація та технічне обслуговування залізниці	
		забезпечення роботи вокзалів та вузлових станцій	
	морський та річковий транспорт	контроль і управління судноплавством	
		операції на внутрішньому, морському або прибережному пасажирському та вантажному транспорті	
		функціонування керуючих органів портів або суб'єктів експлуатації портового обладнання	
		експлуатація та обслуговування інфраструктури (каналів, дамб, фарватерів тощо)	
		регулювання руху суден	
		лоцманське проведення суден	
	поштовий зв'язок	надання послуг поштового зв'язку	
Промисловість	хімічна промисловість	виробництво промислового газу	Мінстратегпром
		виробництво добрив або азотистих сполук	
		виробництво пестицидів або інших агрохімічних продуктів	
		виробництво вибухових речовин	
		виробництво основних органічних хімічних речовин	
		виробництво основних неорганічних речовин	
	металургійна промисловість	гірничо-металургійний комплекс (металургійне виробництво та добування залізних руд)	

Продовження табл. А.1– Перелік секторів критичної інфраструктури

		виробництво коксу та коксопродуктів	
	оборонна промисловість	розробка, виробництво, модернізація та утилізація продукції військового призначення (оборонно-промисловий комплекс)	
	космічна промисловість	виробництво та постачання космічної техніки	
		космічна діяльність, космічні технології та послуги	
	авіаційна промисловість	виробництво та постачання продукції авіаційної промисловості	
	суднобудівна промисловість	суднобудування та постачання продукції суднобудування	
Сектор громадської безпеки	громадська безпека	охорона публічного (громадського) порядку, фізичний захист критичної інфраструктури	МВС
	екстрена допомога населенню за єдиним телефонним номером 112	надання екстреної допомоги населенню за єдиним телефонним номером 112	
Цивільний захист населення і територій	служби порятунку (атестовані аварійно-рятувальні служби згідно із законодавством)	реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій, надання допомоги постраждалим	
Міграція (імміграція та еміграція)		оформлення документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус	
Охорона навколишнього природного середовища	управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства	забезпечення задоволення потреб населення і галузей економіки у водних ресурсах	Міндовкілля
		проектування, будівництво і реконструкція систем захисту від шкідливої дії вод, групових і локальних водопроводів, систем водопостачання та каналізації у сільській місцевості, гідротехнічних споруд, водогосподарських об'єктів багатоцільового використання	
		захист від підтоплення захисних масивів, протипаводковий і протиповеневий захист	
	поводження з радіоактивними відходами	довгострокове зберігання і захоронення радіоактивних відходів	

Продовження табл. А.1– Перелік секторів критичної інфраструктури

	охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду	охорона, раціональне використання земель та надр	
		охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду	
		ведення лісового і мисливського господарства	
		поводження з відходами, небезпечними хімічними речовинами, пестицидами та агрохімікатами	
		створення, дослідження та практичне використання генетично модифікованих організмів у відкритій системі	
Сектор оборони		оборона	Міноборони
	зберігання боєприпасів	забезпечення зберігання боєприпасів, вибухових речовин	
	виробництво боєприпасів	виробництво ракет, боєприпасів, вибухових речовин	
Національна безпека		захист національної державності	СБУ
		охорона державної таємниці	
		боротьба з тероризмом	
Правосуддя		здійснення правосуддя	ДСА
Тримання під вартою		тримання засуджених та осіб, взятих під варту, в установах виконання покарань та слідчих ізоляторах Державної кримінально-виконавчої служби	Мін'юст
Наукові дослідження та розробки	дослідницька інфраструктура наукових установ та закладів вищої освіти	наукова діяльність	МОН
		надання послуг з використання наукового обладнання (у тому числі інструментів, приладів, інвентарю)	
		дослідницька діяльність	
Фінансовий сектор	банківська система	надання банківських послуг	Національний банк
		зберігання банками запасів готівки Національного банку та проведення операцій із ними	
	ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків)	надання електронних довірчих послуг у банківській системі	
		надання небанківських фінансових послуг	
	ринок платіжних послуг	надання платіжних послуг	
Вибори та референдуми		організація підготовки та проведення виборів та референдумів	Центральна виборча комісія

Продовження табл. А.1– Перелік секторів критичної інфраструктури

Соціальний захист	пенсійне забезпечення	забезпечення пенсійних виплат	Мінсоцполітики
	соціальне страхування	надання матеріального забезпечення і страхових виплат	
	соціальна допомога і соціальні послуги	забезпечення соціальних виплат та надання соціальних послуг	
	інформаційна система соціальної сфери	надання адміністративних послуг соціального характеру в електронній формі	
Інформаційні послуги	засоби масової інформації	надання послуг у сфері телебачення та радіомовлення	МКІП
		надання послуг в інформаційній та видавничій сферах	
Державна влада та місцеве самоврядування		виконання функцій держави	Держспецзв'язку